POSIC

Política de Segurança da Informação e Comunicações

2022

Ministério do Turismo

Fundação Casa de Rui Barbosa

Letícia Dornelles
Presidente

Comitê Gestor de Tecnologia da Informação

Letícia Dornelles – Presidente
Luziana Jordão Lessa – Diretora do Centro de Memória e Informação
Marta Maria Alonso de Siqueira – Diretora do Centro de Pesquisas
Cicilia Leandro Costa Maia – Coordenador Geral de Administração
André Chang Kapp – Chefe do Serviço de Tecnologia da Informação e Comunicação

Comitê Gestor de Segurança da Informação e Comunicação

Amanda Britto Siqueira Ribeiro
Andréa Castelo Branco Magalhães
Eduardo Pinheiro da Costa
Luiz Carlos Baltazar Gonçalves
Ricardo da Silva Fonseca

Sumário

1. **Apresentação da FCRB** 2
2. **Missão da FCRB** 2
3. **Objetivo** 2
4. **Escopo** 3
5. **Conceitos E Definições** 4
6. **Referências Legais e Normativas** 8
7. **Princípio** 10
8. **Diretrizes Gerais** 11
9. **Competências e Responsabilidades** 13
10. **Atualização** 14
11. **Vigência** 14
12. **Normas Internas** 14
13. **Disposição Final** 14

ANEXO 15

1. APRESENTAÇÃO DA FCRB

A Fundação Casa de Rui Barbosa é uma instituição pública federal, vinculada ao Ministério do Turismo, é um espaço reservado ao trabalho intelectual, à consulta de livros e documentos, e à preservação da memória nacional.

As principais atividades da Fundação são:

- Manutenção, preservação e difusão do Museu Casa de Rui Barbosa e seu jardim histórico;
- Formação, preservação e difusão do acervo bibliográfico e documental, com o apoio de laboratórios técnicos;
- Desenvolvimento de estudos e pesquisas em suas áreas de atuação (estudos ruianos, de política cultural, história, direito e filologia) em cultura brasileira em geral;
- Desenvolvimento de estudos e pesquisas nas áreas de documentação e preservação;
- Publicação dessas pesquisas e participação de pesquisadores e tecnologias em eventos acadêmicos e científicos;
- Formação e qualificação de pesquisadores e tecnologias;
- Utilização plena do seu auditório com atividades de dança, música, literatura, teatro e cinema;
- Uso de outras dependências para a realização de exposições de acervo ou relacionadas a trabalhos em andamento e de cursos, congressos e seminários.

2. MISSÃO DA FCRB

Desenvolvimento da cultura, da pesquisa e do ensino, a divulgação e o culto da obra e vida de Rui Barbosa. (Lei 4.693 de 06-04-1966)
Desta forma, a instituição pode contribuir para o conhecimento de diversidade cultural e para o fortalecimento da cidadania, assegurando a implementação das demais políticas do Ministério do Turismo.

3. OBJETIVO

A Política de Segurança da Informação e Comunicações (PoSIC) objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, documentos e conhecimentos produzidos, armazenados ou

transmitidos, por qualquer meio dos sistemas de informação da Fundação Casa de Rui Barbosa(FCRB), contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional. Além disso, objetiva estabelecer o comprometimento da alta direção organizacional da FCRB, com vistas a prover apoio para implementação da Gestão de Segurança da Informação e Comunicações, e estabelecer um ambiente seguro, proporcionando melhor qualidade nos processos de gestão e controle dos sistemas de informação e informática.

Qualquer tipo de dúvida sobre a PoSIC, as Normas Internas (NIs) e demais regulamentações de Segurança da Informação e Comunicações (SIC) devem ser imediatamente esclarecidas com a área de Gestão de Segurança da Informação.

4. ESCOPO

4.1 A PoSIC é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Seu propósito é direcionar a FCRB no que diz respeito à gestão dos riscos e do tratamento dos incidentes de SIC, por meio da adoção de procedimentos e mecanismos, que visam manter os princípios básicos de segurança da informação – confidencialidade, integridade, autenticidade e disponibilidade – para garantir a continuidade das atividades da FCRB, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais e valores éticos.

4.2 Abrangência

4.2.1 A Política de Segurança da Informação e Comunicações (PoSIC) se aplica a todos usuários, as unidades administrativas, servidores, funcionários e colaboradores externos que prestam serviço em razão de contratos administrativos firmados na forma da Lei e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres.

4.3 Responsabilidades do Agente Público

4.3.1 Colaborar com a difusão da POSIC dentro da Fundação.

4.3.2 Evitar realizar conversas em locais públicos ou sem a reserva adequada sobre assuntos sensíveis da Instituição, restringindo-se a tratá-los somente em locais que ofereçam a proteção adequada.

4.3.3 Colaborar ativamente na solução de problemas e no aprimoramento dos processos de segurança da informação da FCRB.

5. CONCEITOS E DEFINIÇÕES

5.1 Agente público: todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente à FCRB.

5.2 Ameaça: Conjunto de fatores externos ou causa potencial de um incidente.

5.3 Ativo de informação: qualquer pessoa, tecnologia, processo ou ambiente que processe, armazene, transporte ou descarte informação institucional.

5.4 Autenticidade: - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

5.5 Assinatura digital: Um conjunto de dados criptografados, associados a um documento no qual são função é garantir a integridade e autenticidade do documento associado, mas não a sua confidencialidade.

5.6 Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura que a suporta.

5.7 Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal-intencionado.

5.8 Irretratabilidade ou não repúdio - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita

5.9 Mecanismos de certificação: Atesta a validade de um documento.

5.10 Mecanismos de cifração ou encriptação: Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

5.11 Mecanismos de controle de acesso: Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

5.12 Comitê Gestor de Tecnologia de Informação – Delibera sobre o planejamento, a coordenação e a gestão dos sistemas de informação e informática. O comitê é constituído pelos seguintes membros: Presidente, Diretor Executivo, Coordenador Geral de Planejamento e Administração, Diretor do CMI, Diretor do CP e Chefe do Serviço de Informática.

5.13 Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da FCRB.

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

5.15 Credenciais de Acesso: Permissões concedidas por autoridade competente da FCRB após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, biometria, cartão, *token*, ou lógica para identificação de usuários.

5.16 CPD (Centro de Processamento de Dados): Sala onde se localizam parte dos servidores da FCRB responsáveis pelo processamento e armazenamento de dados. Sua nomenclatura obsoleta deve-se ao não cumprimento de requisitos que a definam como *DataCenter*, o qual possui uma série de especificações de infraestrutura e contingência que o CPD não possui. O CPD em questão possui infraestrutura diferenciada da maioria dos setores da FCRB, contendo: com controle de acesso físico e lógico, monitoramento por câmera, medidor de temperatura e umidade ambiente, com configuração de alerta para temperatura acima da estipulada, e contingência para ar-condicionado.

5.17 Diretriz: Conjunto de instruções ou indicações que orientam o que deve ser feito para se alcançar os objetivos estabelecidos na política.

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

5.19 Dispositivos móveis: Consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: *notebooks*, *netbooks*, *smartphones*, *tablets*, *pendrives*, USB *drives* HDs externos e cartões de memória.

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

5.21 Governança de TI: Está relacionada ao desenvolvimento de um conjunto estruturado de competências e habilidades estratégicas para profissionais de TI responsáveis pelo planejamento, implantação, controle e monitoramento de programas e projetos de governança, requisito fundamental para as organizações, seja sob os aspectos operacionais, seja sob suas implicações legais.

5.22 Incidente: qualquer evento indesejado ou inesperado, relacionado ou não com segurança, que comprometa ou ameace as operações e/ou a segurança da informação. Este é identificado rapidamente pela equipe de TI.

5.23 Problema: Pode ser a causa que gere os incidentes, tendo sua origem desconhecida e requer maior tempo de análise pela equipe de TI a fim de solucionar o mesmo.

5.24 Informação: Entende-se por informação todo e qualquer conteúdo informacional, podendo ser digital, que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

5.25 Política de Segurança da Informação: 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.

5.26 Quebra de segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC da FCRB.

5.27 Redes Sociais: Estruturas sociais, disponíveis na rede mundial de computadores (Internet), compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, quepartilham valores e objetivos comuns.

5.28 Segurança da Informação e Comunicações: Ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações, abrangendo não só aspectos tecnológicos, mas também recursos humanos e processos.

5.29 Senha forte: Deve ter no mínimo 8 caracteres e conter letras (preferencialmente combinar maiúsculas e minúsculas), números e caracteres especiais.

5.30 Severidade: índice ou grau que se refere à medição do impacto de um evento ou incidente de segurança da informação.

5.31 Usuário(s): Visitantes, Servidores, agentes públicos, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada de acesso aos Ativos de Informação da FCRB

5.32 Vulnerabilidade: Qualquer fragilidade dos sistemas computacionais e redes de computadores que permita a exploração maliciosa e acessos indesejáveis ou não autorizados. Também definida como conjunto de fatores internos ou causa potencial de um incidente indesejado, que pode resultar em risco para um ativo ou sistema e pode ser evitado por uma ação interna de SIC.

5.33 Recursos de TI: É composto por todos os ativos de TI, tangíveis e intangíveis, que são utilizados sob demanda dos usuários ou dos sistemas computacionais que o requisitarem. Exemplos de ativo de TI tangível: Computador ou estação de trabalho e servidores de rede.

5.34 Exemplos de ativo de TI intangível: Software utilizado para produção de textos e planilhas, aplicações web, etc.

5.35 Proxies Externos: Qualquer proxy que não pertença a configuração realizada pela STIC. Por definição, para esclarecer sua funcionalidade e de acordo com o Wikipedia, “Em redes de computadores, um

proxy (em português 'procurador', 'representante') é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores".https://pt.wikipedia.org/wiki/Proxy

5.36 Um tipo de proxy externo que pode afetar a segurança de TIC é denominado "proxy anônimo", segundo o Wikipedia, "Um proxy anônimo é uma ferramenta que se esforça para fazer atividades na Internet sem vestígios: acessa a Internet a favor do usuário, protegendo as informações pessoais ao ocultar a informação de identificação do computador de origem. " https://pt.wikipedia.org/wiki/Proxy#Proxy_an%C3%B4nimo

"O operador do proxy ainda pode relacionar as informações dos usuários com as páginas vistas e as informações enviadas ou recebidas. "

5.37 Biometria: método automático de reconhecimento individual baseado em medidas biológicas - anatômicas e fisiológicas. Na FCRB, refere-se à impressão digital previamente cadastrada em aplicação proprietária para controle e segurança de acesso.

5.38 Sistema Integrado de Comando e Controle: conjunto de sistemas inter-relacionados necessários para o apoio dos vigilantes de segurança de empresa contratada, controle e monitoramento dos acessos à Instituição, segurança e integridade das pessoas nas dependências da FCRB. É composto por: Sistema de Controle de Acessos, Circuito Fechado de Televisão (CFTV), Sistema de Alarme deIncêndio, Sistema de Detecção de Intrusão e Centro de Comando e Controle e de Operações.

5.39 Sistema de controle de acessos: sistema de identificação pessoal, responsável pelo registro e liberações de acessos nas dependências da instituição.

5.40 Circuito Fechado de TV (CFTV): sistema de monitoramento de ambientes por câmeras, responsável pela filmagem, pela visualização em tempo real e pelo registro de imagens dos locais monitorados.

5.41 Sistema de Alarme de Incêndios: Sistema responsável pela detecção e disparo de alarme de incêndio.

5.42 Sistema de Detecção de Intrusão: sistema responsável por detectar e registrar eventos de entrada ou permanência de pessoas indesejadas em locais monitorados.

5.43 Centro de Comando e Controle: local destinado a abrigar 01(um) posto de vigilância e as centrais controladoras dos sistemas envolvidos. O agente de vigilância neste local é responsável por monitorar, controlar e supervisionar os eventos e incidentes relacionados a todo o Sistema de Comando e Controle, agindo em conformidade com as normas de segurança da FCRB estabelecidas por seu Comitê Gestor de Tecnologia da Informação.

5.44 Recesso: refere-se às interrupções normais ou eventuais na jornada de trabalho - finais de semana, feriados, ou qualquer suspensão ou dispensa temporária das atividades totais ou parciais da FCRB.

5.45 Ocorrência: episódio, evento, fenômeno considerado anormal ou incomum dentro dos procedimentos amparados pelo Sistema Integrado de Comando e Controle.

5.46 Problema: episódio, evento, fenômeno considerado anormal ou incomum. Sua principal característica é a dificuldade em identificar a causa de origem, pode ser a fonte para a ocorrência de incidentes.

5.47 Incidente: fato anormal que pode ser identificado, relacionado a uma ocorrência ou a um problema.

6. REFERÊNCIAS LEGAIS E NORMATIVAS

6.1 Decreto nº 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética do Servidor Público Civil do Poder Executivo Federal.

6.2 Decreto 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.

6.3 Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados e informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

6.4 Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores (Internet)

6.5 Decreto Nº 7.845, de 14 de novembro de 2012 - os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, Gestão de Segurança da Informação e Comunicações.

6.6 Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação

6.7 Instrução Normativa GSI Nº 2, de 5 de fevereiro de 2013 - Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 32, de 18 Fev 2013- Seção 1).

6.8 Instrução Normativa GSI Nº 3, de 6 de março de 2013 - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 50, de 14 Mar 2013- Seção 1)

6.9 Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta.

6.10 Instrução Normativa nº 01/IN01/DSIC/GSIPR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e suas normas complementares.

6.11 Lei n° 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.

6.12 Lei Nº 12.527, DE 18 DE NOVEMBRO DE 2011 - de acesso a informações.

6.13 Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

6.14 Norma ISO/IEC 27001:2006 –Tecnologia da Informação –Técnicas de segurança –Sistemas de Gestão de Segurança da Informação –Requisitos, segundo a obra: FERNANDES, A.A.; ABREU, V.F. Implantando a Governança de TI: da estratégia à gestão dos processos e serviços: 4.ed. Rio de Janeiro: Brasport, 2014.

6.15 Normas ISO/IEC 27001 e 27002:2005, que institui o código de melhores práticas para práticas para Gestão de Segurança da Informação e Comunicações, segundo a obra: FERNANDES, A.A.; ABREU, V.F. Implantando a Governança de TI: da estratégia à gestão dos processos e serviços: 4.ed. Rio de Janeiro: Brasport, 2014.

6.16 Norma ISO/IEC 31000:2009, que institui o código de melhores práticas para práticas para Gestão de Riscos, segundo a obra: FERNANDES, A.A.; ABREU, V.F. Implantando a Governança de TI: da estratégia à gestão dos processos e serviços: 4.ed. Rio de Janeiro: Brasport, 2014.

6.17 Portaria Interministerial MCT/MPOG nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores (Internet) e dá outras providências.

6.18 Portaria Nº 36, de 02 de agosto de 2012 – Institui o Comitê Gestor de Tecnologia da Informação da Fundação Casa de Rui Barbosa.

6.19 Portaria Nº 55, de 04 de dezembro de 2013 – Aprova o Plano Diretor de Tecnologia da Informação – PDTI 2013/2015 da Fundação Casa de Rui Barbosa.

6.20 Portaria Nº 3, de 09 de janeiro de 2015 – Institui o Comitê Gestor de Segurança da Informação da Fundação Casa de Rui Barbosa.

7. PRINCÍPIOS

As ações de Segurança da Informação e Comunicações na FCRB são norteadas pelos seguintes princípios (sem prejuízo aos princípios da Administração Pública Federal, definidos no art. 37 da Constituição Federal):

7.1 Autenticidade: Garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos, por pessoa física, ou por sistema, órgão ou entidade vinculado a FCRB.

7.2 Celeridade: As ações de SIC devem oferecer respostas a incidentes e falhas de segurança.

7.3 Confidencialidade: Garantia de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada pela FCRB.

7.4 Conhecimento: Os usuários devem conhecer e respeitar a PoSIC, NIs e demais regulamentações SIC da FCRB.

7.5 Clareza: As regras de SIC, documentação e comunicações devem ser precisas, concisas e de fácil entendimento.

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

7.7 Ética: Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento da SIC.

7.8 Integridade: Garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino.

7.9 Legalidade: As ações de segurança devem levar em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais da FCRB.

7.10 Privacidade: Garantia ao direito pessoal e coletivo, à intimidade e ao sigilo da correspondência e das comunicações individuais.

7.11 Publicidade: Transparência no trato da informação, observados os critérios legais.

7.12 Responsabilidade: As responsabilidades primárias e finais pela segurança dos ativos da FCRB e pelo cumprimento de processos de segurança devem ser claramente definidas.

8. DIRETRIZES GERAIS

Para fins desta Portaria ficam estabelecidas as seguintes diretrizes gerais:

8.1 Tratamento das informações

8.1.1 Os ativos de informação da instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados.

8.1.2 Todo ativo de informação deve possuir um responsável explicitamente identificado.

8.1.3 Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas.

8.1.4 Eliminação de ativos da informação devem seguir as normas do CONARQ

8.2 Tratamento de incidentes de redes

8.2.1 Os incidentes de segurança da rede devem ser registrados e gerenciados.

8.2.2 Deve ser definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, segundo critérios a serem definidos pela área de Segurança da Informação do Comitê Gestor, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais no órgão.

8.3 Gestão de risco

8.3.1 Deve ser adotada a gestão de riscos de segurança da informação, segundo critérios a serem definidos pela área de Segurança da Informação do Comitê Gestor, para a identificação e implementação das medidas de proteção necessárias para a mitigação ou eliminação dos riscos.

8.3.2 Informações confidenciais da FCRB não podem ser transportadas em qualquer meio sem as devidas autorizações e proteções.

8.4 Gestão de continuidade

8.4.1 Deve ser adotada a gestão de continuidade das atividades em segurança da informação, segundo critérios a serem definidos pela área de Segurança da Informação do Comitê Gestor, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, através de ações de prevenção, resposta e recuperação dos ativos que sustentam os processos críticos da Instituição.

8.5 Conformidade

8.5.1 Deve-se manter a conformidade com as legislações vigentes.

8.6 Controles e monitoramento de acesso.

8.6.1 Todo acesso à informação sigilosa se dará através de mecanismos de identificação e controle de acesso.

8.6.2 Todos os usuários da FCRB devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violações da PoSIC e demais regulamentações em vigor.

8.6.3 Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação.

8.6.4 A identificação do usuário deverá ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o reconhecimento do envolvido.

8.7 Segurança de recursos humanos

8.7.1 Todo agente público deverá ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de informação, inclusive por ocasião da mudança de atividades.

8.8 Segurança física e do ambiente

8.8.1 Todo ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade.

8.9 Gerenciamento de operações e comunicações

8.9.1 Deve-se garantir a operação segura e correta dos recursos de processamento da informação.

8.9.2 Aquisição, desenvolvimento e manutenção de sistemas

8.9.3 Todos os sistemas de informação adquiridos ou desenvolvidos para uso da Instituição devem ter sua continuidade garantida, independentemente de eventuais mudanças na relação FCRB – fornecedor.

8.10 Ativos de TIC

8.10.1 Os recursos de tecnologia da informação e comunicações de propriedade da FCRB são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração. É considerada imprópria a utilização desses recursos para propósitos não profissionais ou não autorizados. Os usuários e visitantes que tomarem conhecimento dessa prática devem levá-la ao conhecimento do superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

9. COMPETÊNCIAS E RESPONSABILIDADES

O Gestor de Segurança da Informação e Comunicações foi designado pela então Presidente, Marta de Senna, como sendo o Coordenador Geral de Administração, através da Portaria 66 de 26 de junho de 2018;

9.1 São competências do Gestor de Segurança da Informação e Comunicações:

9.1.1 Submeter esta POSIC à autoridade máxima desta Fundação para aprovação e sua posterior publicação.

9.1.2 Disseminar as regras e orientações de segurança aplicadas aos usuários através de campanhas internas permanentes, disponibilização integral e contínua na Intranet, como forma de ser criada uma cultura de segurança dentro da FCRB.

9.1.3 Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

9.1.4 Propor recursos necessários às ações de segurança da informação e comunicações;

9.1.5 Coordenar o Comitê de Segurança da Informação e Comunicações

9.1.6 Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

9.1.7 Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

9.1.8 Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito da FCRB.

9.2 São competências do Comitê de Segurança da Informação e Comunicações:

9.2.1 Assessorar na implementação das ações de segurança da informação e comunicações;

9.2.2 Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações, quando cabível;

9.2.3 Propor alterações na PoSIC;

10.ATUALIZAÇÃO

A Política de Segurança da Informação e Comunicações, bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

11. VIGÊNCIA

A presente Portaria entra em vigor na data de sua publicação no Boletim Interno.

12.NORMAS INTERNAS

Todo usuário deve conhecer e cumprir a Política de Segurança da Informação e Comunicações (POSIC) e as legislações em vigor referenciadas no anexo deste documento – Normas Internas Relativas à Política de Segurança da Informação e Comunicações.

13. DISPOSIÇÃO FINAL

Os incidentes de segurança e denúncias de descumprimento à Política de Segurança da Informação e Comunicações e suas normas devem ser notificados ao Comitê Gestor de Segurança da Informação e Comunicações e poderão resultar na aplicação das sanções previstas e descritas no item 6.

ANEXO

NORMAS INTERNAS RELATIVAS À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC 2022

1. Sobre o uso de recursos de TI

1.1. Os usuários devem proteger os recursos de TI da FCRB contra acesso, modificação, destruição ou divulgação não autorizada.

1.2. Utilizar os recursos de TI disponibilizados pela FCRB preferencialmente para os fins institucionais.

1.3. Não abrir o gabinete das estações de trabalho ou computador portátil, nem modificar qualquer configuração, seja de hardware ou software. Essas configurações são padronizadas, conforme definições da área de TI. Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada à área de TI para análise.

1.4. Não instalar ou executar software de sua propriedade ou de terceiros sem prévia homologação e autorização da área de TI.

1.5. Desligar a estação de trabalho ou computador portátil corretamente e diariamente ao final do expediente, seguindo os procedimentos do sistema operacional.

1.6. Devem-se armazenar os arquivos com informações institucionais nos servidores disponibilizados na rede local da Unidade, levando-se em consideração que cópias de segurança são realizadas periodicamente. Deve-se evitar o armazenamento nas estações de trabalho.

1.7. Todo recurso de TI deve ter seu uso restrito ao local de trabalho, salvo, para os casos de necessárias tramitações externas autorizadas.

2. Sobre o uso de dispositivos portáteis

2.1. Os dispositivos portáteis da FCRB, sempre que não estiverem sendo utilizados,devem ser guardados em local seguro, onde o responsável, por estes, possa garantirque os mesmos não serão utilizados por outras pessoas.

3. Sobre o uso de credenciais

3.1. O Usuário somente terá acesso às informações e aos recursos de TI após a conclusão do processo de credenciamento/concessão de acesso, que se dará através de solicitação formal da chefia imediata do usuário ao Setor de Informática.

3.2. A cada usuário devem ser disponibilizadas as credenciais de acesso – usuário e senha - aos recursos de TI. Estas credenciais são pessoais e intransferíveis não podendo ser compartilhadas com outros usuários sem nenhuma hipótese.

3.3. A senha de acesso ao recurso de TI qualifica o usuário como responsável por todos os acessos realizados. A definição e a utilização de senhas estão condicionadas às regras definidas pela área de TI.

3.4. Os direitos e perfis de acesso seguem as definições do responsável pelo usuário em concordância com os padrões estabelecidos pela área de TI.

3.5. O usuário deve trocar sua senha de acesso aos recursos de TI periodicamente, seguindo as orientações da área de TI.

3.6. Recomenda-se a utilização de senhas com no mínimo 8(oito) caracteres contendo letras e números.

3.7. Bloquear o acesso à estação de trabalho ou computador portátil que lhe foi confiado sempre que dela se ausentar.

4. Sobre impressão e digitalização de documentos

4.1. Os documentos impressos devem ser encaminhados para o Serviço de Arquivo Histórico e Institucional com o objetivo de serem classificados em conformidade com a legislação vigente.

4.2. Os documentos sigilosos não devem ser deixados sobre as mesas na ausência do usuário, e devem ser guardados em local seguro e com controle de acesso.

4.3. Documentos enviados a impressoras compartilhadas devem ser recolhidos tão logo impressos.

5. Sobre descarte de informações

5.1. Os ativos, considerados como documento de arquivo, deverão ser submetidos à análise do Serviço de Arquivo Histórico e Institucional quanto à sua permanência ou descarte de acordo com a legislação vigente.

5.2. Os ativos em meio eletrônico não mais utilizados pelos usuários, devem ser submetidos à chefia imediata para análise quanto à permanência ou descarte.

6. Sobre a Propriedade da Informação

6.1. É restrito o uso da informação (pertencente à Casa) às dependências da FCRB salvo quando necessárias tramitações externas com a devida autorização.

6.2. As informações institucionais produzidas por usuários no exercício de suas funções são patrimônio da FCRB e não cabe a seus produtores qualquer forma de exploração sobre essas informações.

7. Sobre Movimentação e Acesso aos acervos

7.1. Da utilização da Sala de Consulta

7.1.1. Não é permitida a entrada na Sala de Consulta com nenhum tipo de bolsa, pasta, caderno, livro, caneta, celular e arquivo fechado.

7.1.2. Não é permitido o acesso à Sala de Consulta com alimentos e bebidas.

7.1.3. A quantidade máxima permitida de material bibliográfico por usuário é de dez itens, sendo permitida a entrada de cinco por vez.

7.1.4. Para manuseio de documentos e obras raras ou em condições físicas fragilizadas, o usuário deve usar material apropriado (cedido pela Fundação) para conservação da obra.

7.1.5. Não é permitido dobrar, riscar, escrever ou marcar páginas de livros, revistas ou qualquer outro tipo de documento, ficando o usuário responsável pela sua integridade, respondendo por eventuais danos ao patrimônio público.

7.1.6. Todas as obras consultadas, após uso, devem ser devolvidas no balcão de atendimento.

7.2. Serviço de Arquivo Histórico e Institucional (SAHI)

7.2.1. Do acesso ao acervo

7.2.1.1. O acesso ao acervo se dá mediante agendamento através do endereço eletrônico consulta.acervo@rb.gov.br, arquivo@rb.gov.br ou diretamente na Sala de Consultas.

7.2.1.2. O usuário deverá preencher formulário específico de cadastramento.

7.2.1.3. No caso dos documentos que já estejam digitalizados, o usuário terá acesso à cópia digital, e não ao original.

7.2.1.4. Para manusear os documentos do SAHI, o usuário deverá utilizar luvas, que serão disponibilizadas na sala de consulta.

7.2.2. Do empréstimo do acervo

7.2.2.1. Os arquivos pessoais não poderão ser emprestados. O fundo institucional, no entanto, pode ser emprestado internamente para o processo de tomada de decisões.

7.2.3. Da reprodução do acervo

7.2.3.1. O usuário deverá solicitar seu pedido de reprodução através dos endereços eletrônicos consulta.acervo@rb.gov.br ou arquivo@rb.gov.br.

7.2.3.2. O usuário deverá assinar o “Termo de Licença para reprodução de acervo arquivístico da Fundação Casa de Rui Barbosa”. Com esse instrumento o usuário declara que se responsabiliza por qualquer dano material ou moral decorrente da violação das obrigações estabelecidas no instrumento, sem prejuízo das providências penal e administrativa, isentando a FCRB por qualquer dano causado a terceiros com a utilização irregular dos direitos autorais pertinentes ao acervo.

7.3. Serviço de Biblioteca (BIB)

7.3.1. Do cadastramento

7.3.1.1. Ocadastro do usuário externo será realizado mediante o preenchimento do "Formulário de Atendimento – Biblioteca".

7.3.2. Do empréstimo

7.3.2.1. Aos bolsistas, estagiários e usuários externos é vedado o empréstimo, sendo permitido fazer consulta e pesquisa ao acervo somente nas dependências da Sala de Consulta.

7.3.2.2. O empréstimo do acervo é exclusivo aos usuários internos, de acordo com as normas para cada coleção e/ou obra específica.

7.3.2.3. É permitido o empréstimo de até dez obras, pelo prazo de quinze dias úteis.

7.3.2.4. Ressalta-se que é vedado o empréstimo domiciliar das obras da Biblioteca de Rui Barbosa e da Coleção Plínio Doyle. As obras referentes a esses acervos apenas poderão ser levadas para as dependências de trabalho dos servidores, na FCRB, na condição de empréstimo durante o expediente, mediante assinatura do termo de empréstimo,sendo obrigatória sua devolução até o horário máximo das 17h30 do mesmo dia.

7.3.2.5. O usuário interno é responsável pelo material emprestado, respondendo administrativamente por dano ou perda.

7.3.3. Do empréstimo permanente ou por prazo indeterminado

7.3.3.1. O empréstimo permanente é concedido com prazo até 29 de dezembro, sendo facultado aos setores da FCRB no caso somente de obras da Biblioteca São Clemente, podendo ser renovado a cada ano. Esse empréstimo está assim sujeito à apresentação, no mês de dezembro, para inventário patrimonial do Serviço de Biblioteca.

7.3.4. Das perdas e danos

7.3.4.1. Qualquer obra danificada ou extraviada pelo usuário deverá ser substituída por exemplar idêntico; caso a publicação esteja esgotada, por outra da mesma natureza e valor, a ser indicada pela biblioteca.

7.3.5. Da devolução

7.3.5.1. A devolução dos materiais bibliográficos deverá ser feita única e exclusivamente no balcão de atendimento e posteriormente aguardar o processo de baixa no material.

7.3.6. Da reprodução

7.3.6.1. Toda reprodução de documentos fica condicionada à Lei de Direitos Autorais (Lei nº9.610/1998).

7.3.6.2. Tendo em vista a preservação dos materiais bibliográficos originais, os pedidos de reprodução devem ser atendidos mediante as restrições de uso e estado de conservação da obra, segundo avaliação do Serviço de Preservação.

7.3.6.3. Para solicitar o serviço de reprodução é necessário o cadastro do usuário na Sala de Consulta. Assim, o usuário receberá orientações sobre direitos autorais e obrigatoriedade de atribuição de crédito à FCRB nos casos de publicação ou divulgação de qualquer material bibliográfico. Também deverá preencher formulário específico de "Termo de responsabilidade − Biblioteca − Licença para reprodução" e o "Termo de responsabilidade de uso do acervo do Serviço de Biblioteca da Fundação Casa de Rui Barbosa".

7.3.6.4. Toda reprodução deverá ocorrer em local específico para essa finalidade sob supervisão de um servidor.

7.3.6.5. Obras que não estejam em domínio público não poderão ser reproduzidas.

7.4. Serviço de Preservação (SEP)

7.4.1. Do traslado do acervo

7.4.1.1. O traslado do acervo para o SEP é de responsabilidade do detentor do acervo a ser tratado ou da unidade de origem nos casos em que pertençam à FCRB.

7.4.1.2. Nos casos em que as características físicas e o estado de conservação exijam, e mediante acordo prévio com o proprietário, o traslado dos objetos deverá ser acompanhado por um técnico do SEP.

7.4.1.3. O traslado do acervo para fora da instituição deverá, em todas as situações, ser acompanhado por um técnico do SEP.

7.4.1.4. A todo acervo cedido deverá ser preenchido um termo de "Responsabilidade de Cessão".

7.4.2. Da entrada do acervo

7.4.2.1. No momento da entrada do acervo no SEP, todos os objetos deverão ser registrados com o preenchimento da "Ficha de Entrada", "Ficha Técnica" e, sempre que necessário(danos muito graves, objetos de outras instituições, etc.), ser fotografados.

7.4.2.2. Nos casos em que o acervo entregue ao SEP pertença a outras instituições, o proprietário, ou seu representante, deverá, no momento da entrega, assinar o correspondente "Termo de Compromisso" constante da "Ficha de Entrada de Obra" e receber o "Recibo e Obra" subscrito e datado por técnico do SEP.

7.4.3. Da segurança do acervo

7.4.3.1. É de responsabilidade do SEP zelar pela integridade e segurança do acervo que se encontre sob sua guarda.

7.4.3.2. Em casos em que o acervo saia da instituição, será exigido seguro contra danos, furtos e/ ou destruição/descaracterização ocasionadas por sinistros ou falha técnica.

7.4.4. Da responsabilidade do corpo técnico do SEP

7.4.4.1. Zelar pela preservação dos acervos documentais, artísticos e históricos que estiverem sob sua guarda e tratamento;

7.4.4.2. Não fumar nem consumir bebidas e alimentos nas dependências do SEP.

7.5. Divisão Museu Casa de Rui Barbosa (MCRB)

7.5.1. Do acesso ao acervo

7.5.1.1. O visitante recebe as seguintes orientações, necessárias para sua entrada:

7.5.1.1.1. Preenchimento da planilha de visitação e pagamento do ingresso, quando for o caso;

7.5.1.1.2. Programar câmeras para fotografias sem flash;

7.5.1.1.3. Proibição de comer, beber e mascar chiclete durante a visita;

7.5.1.1.4. Uso dos guarda-volumes para a guarda de seus pertences pessoais antes de iniciar a visita, tendo em vista ser proibido entrar no museu com bolsas e mochilas;

7.5.1.1.5. Aguardar o vigilante que acompanhará a visita.

7.5.2. Do empréstimo do acervo

7.5.2.1. O acervo solicitado para empréstimo será previamente avaliado, considerando-se O estado de conservação do documento ou objeto, O período do empréstimo O acondicionamento e o transporte.

7.5.2.2. O empréstimo deverá ser feito mediante assinatura do termo de comodato e acompanhado do *condition report*.

7.5.2.3. Em caso de empréstimo para exposição, deverão ser considerados o local, a segurança e a montagem, com garantia de condições ambientais favoráveis, de acordo com as normas da Associação Brasileira de Normas Técnicas (ABNT).

7.5.2.4. O empréstimo do acervo para exposição será acompanhado de um técnico da FCRB, que fiscalizará toda a operação de acondicionamento, transporte, montagem e desmontagem, cabendo ao solicitante as despesas daí decorrentes.

7.5.2.5. Os documentos só poderão ser retirados mediante aprovação da apólice de seguro pela FCRB, sendo o ônus do seguro dos documentos de responsabilidade do solicitante.

7.5.3. Reprodução do acervo

7.5.3.1. Toda solicitação para a reprodução de imagens, modelos tridimensionais, digitais, fotografias e filmagens deverão ser encaminhadas à chefia do museu, informando sua finalidade.

7.5.3.2. Após a aprovação, o solicitante deverá preencher e assinar o "Termo de Licença para Reprodução de Acervo Museológico da Fundação Casa de Rui Barbosa". Por meio desse instrumento, o usuário declara que se responsabiliza por qualquer dano material ou moral decorrente da violação das obrigações estabelecidas no instrumento, sem prejuízo das providências penal e administrativa, isentando a FCRB por qualquer dano causado a terceiros com a utilização irregular dos direitos autorais pertinentes ao acervo. Em toda a reprodução e/ou filmagem deverá constar o crédito da instituição assim descrito: "Acervo Museu Casa de Rui Barbosa/Fundação Casa de Rui Barbosa".

7.5.3.3. Nenhum item do acervo poderá ser utilizado ou transferido de lugar sem a autorização e presença de um técnico do museu.

7.6. Divisão Arquivo-Museu de Literatura Brasileira (AMLB)

7.6.1. Do acesso ao acervo

7.6.1.1. A consulta presencial será feita mediante agendamento através do e-mail consulta.acervo@rb.gov.br, sendo o atendimento feito por um técnico de arquivo.

7.6.2. Do empréstimo do acervo

7.6.2.1. A solicitação de empréstimo de acervo deverá ser feita com três meses de antecedência e será previamente avaliada, considerando-se:

7.6.2.1.1. Estado de conservação do documento arquivístico ou museológico;

7.6.2.1.2. Tempo de empréstimo (prazo de três meses, podendo ser prorrogado por igual período);

7.6.2.1.3. Acondicionamento para transporte e tipo de transporte.

7.6.2.2. Documentos únicos e raros do acervo não são passíveis de empréstimo.

7.6.2.3. O empréstimo deverá ser feito mediante contratação de seguro pelo solicitante do empréstimo e assinatura de termo de comodato.

7.6.2.4. O empréstimo do acervo para exposição será acompanhado de um técnico da FCRB, que fiscalizará toda a operação de acondicionamento, transporte, montagem, condições de exibição (ambiente climatizado e dotado de controle de umidade e de luz) e desmontagem, cabendo ao solicitante as despesas daí decorrentes.

7.6.3. Da reprodução do acervo

7.6.3.1. A reprodução de documentos arquivísticos se dará mediante autorização dos herdeiros caso os documentos em questão não estejam em domínio público.

7.6.3.2. A reprodução deverá ser realizada com equipamento fornecido pelo usuário e na presença de um técnico da FCRB. Não é permitida a reprodução por fotocópia.

7.6.3.3. No caso de publicação do material reproduzido, será obrigatória a atribuição de crédito à FCRB/AMLB.

8. Sobre o PenSei Digital – Processo Eletrônico Nacional

8.1. O SEI, no âmbito da FCRB, será utilizado exclusivamente para a produção de processo eletrônico, de natureza administrativa, preconizado conforme Lei nº 9.784, de 29 de janeiro de 1999.

8.2. O Sistema Eletrônico de Informações não será utilizado para produzir e tramitar documentos avulsos.

8.3. A abertura dos processos continuará a ser realizada pelo Serviço de Arquivo Histórico e Institucional - SAHI, mediante solicitação via formulário eletrônico disponível na intranet desta Fundação.

8.4. Os documentos eletrônicos produzidos e geridos no âmbito do SEI terão garantia de integridade, autoria e autenticidade asseguradas pela utilização de Assinatura Eletrônica emitida pelo próprio sistema, mediante *login* e senha de acesso do usuário.

8.5. A assinatura eletrônica é de uso pessoal e intransferível, sendo de responsabilidade do titular sua guarda e sigilo.

8.6. Os usuários externos, mediante credenciamento prévio, poderão*:*

8.6.1. Visualizar os processos em trâmite na FCRB*;*

8.6.2. Assinar eletronicamente contratos, convênios, acordos e outros instrumentos congêneres celebrados com a FCRB*;*

8.7. O credenciamento de usuário externo é ato pessoal e intransferível e dar-se-á a partir do preenchimento de cadastro disponibilizado no sítio eletrônico da FCRB.

8.8. Documentos que possuam restrições de acesso em conformidade com a Lei 12.527, de 18 de novembro de 2011, não serão produzidos e tramitados no SEI.

8.9. Deverá existir um ambiente de teste para futuras atualizações e modificações no SEI.

8.10. As cópias de segurança deverão ser realizadas diariamente.

8.11. Deverá haver um plano de contingência para possível interrupção do serviço.

9. Sobre o uso da Internet

9.1. O acesso à Internet disponibilizado aos usuários de rede pela FCRB deve ser realizado somente para os interesses de negócio da Instituição.

9.2. É atribuição exclusiva da área de TI definir os softwares para uso da Internet na Fundação.

9.3. O uso dos recursos computacionais da FCRB para acesso à Internet nas instalações da Instituição, somente será permitido quando realizado através de redes de dados homologadas pela área de TIC.

9.4. O acesso à Internet por meio da rede local não pode ser realizado por equipamentos particulares, tais como laptops, smartphones, etc. Casos excepcionais devem ser tratados pela área de TI através de solicitação formal.

9.5. É recomendado que quando o acesso à Internet for realizado por meio de dispositivos móveis da FCRB fora de suas dependências, este seja feito por meio de uma rede de dados móvel fornecida pela própria Instituição.

9.6. A todo usuário da rede local da FCRB é facultado o acesso à Internet em conformidade com os termos estabelecidos nesta norma.

9.7. O acesso à Internet dependerá do processo de credenciamento do usuário junto ao SARH ou STIC, ambos serviços ligados à CGA.

9.8. O acesso à Internet pelo usuário da rede será obrigatoriamente desativado quando ocorrer o desligamento do usuário.

9.9. O acesso à Internet concedido ao usuário de rede da FCRB é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à Instituição por meio de seu uso.

9.10. O uso da Internet através da rede corporativa não poderá ser feito via proxies externos.

9.11. O usuário da rede deverá utilizar a Internet de forma a não causar tráfego desnecessário na rede corporativa e demais redes de outras Instituições.

9.12. Todo serviço disponibilizado na Internet, antes de ser implantado na rede corporativa, deve ser avaliado pela área de TI através de avaliação e relatório técnico, considerando os aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

9.13. Uso vedado à utilização da Internet para:

9.13.1. Acessar sites com códigos maliciosos. Caso tenha dúvida em relação a esse acesso, consulte o STIC;

9.13.2. Não utilizar links recebidos por outras pessoas, sem se certificar de sua procedência;

9.13.3. Acessar sites com materiais atentatórios à moral e aos bons costumes ou ofensivos;

9.13.4. Acessar sites ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;

9.13.5. Acessar sites ou arquivos com conteúdo de incitação à violência;

9.13.6. Realizar download de arquivos que não estejam relacionados às necessidades de trabalho da FCRB;

9.13.7. Realizar atividades relacionadas a jogos eletrônicos pela Internet;

9.13.8. Acessar sites para transferência de arquivos, escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho na FCRB;

9.13.9. Utilizar serviços de compartilhamento de arquivos online, salvo aqueles homologados pela área de TI.

9.13.10. A utilização de equipamentos pessoais no ambiente da FCRB não poderá ser realizada por meio da rede corporativa. Para tal, a FCRB disponibiliza uma rede WIFI, isolada, específica para este fim, mediante prévio cadastro e concordância do termo de responsabilidade pelo usuário.

9.14. O acesso à Internet é monitorado e pode ser restringido pela área de TI quanto a endereço de sites, quantidade de acessos, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que estes controles sejam feitos por parâmetros gerais.

9.15. O SARH ou chefias hierarquicamente superiores podem solicitar formalmente um relatório com as informações de acesso à Internet de um de seus usuários da rede, para si ou para outros, nas seguintes situações:

9.16. Suspeita de infração à Política de Segurança da Informação e Comunicações.

9.16.1. Necessidade de visualizar os sites acessados e o tempo gasto nos mesmos por seus usuários de rede.

9.16.2. Outros casos previstos em Lei.

10. Sobre o uso do E-MAIL

10.1. A conta de correio eletrônico institucional, disponibilizada aos usuários da rede de dados pela FCRB é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências e deve ser utilizada somente para os interesses de trabalho. Vale ressaltar que o cadastro em sites de comercio eletrônico pode trazer prejuízo para a instituição.

10.2. É atribuição exclusiva da área de TI definir os softwares homologados para o uso do correio eletrônico institucional.

10.3. O uso do correio particular, quando utilizado através de rede corporativa, não deverá exceder os limites da ética, bom senso e razoabilidade, sendo o usuário responsável pelo conteúdo trafegado e seus eventuais riscos.

10.4. É proibido o uso de provedores de e-mail externos para o encaminhamento das mensagens de uma caixa postal da FCRB.

10.5. O usuário terá direito a uma única conta de e-mail após avaliação de sua chefia imediata.

10.6. A caixa postal compartilhada deve ter um responsável e um substituto formalizados.

10.7. A lista de distribuição deve ter um responsável designado para qualquer solicitação relacionada à lista.

10.8. Cabe ao SARH comunicar à área de TI o desligamento do servidor e/ou colaborador para devidas providências.

10.9. O uso do correio eletrônico institucional é uma concessão da FCRB e será desativado:

10.10. Em até seis meses no caso de aposentadoria do servidor público;

10.10.1. Imediatamente ao desligamento, em caso de demissão (servidor) ou encerramento de contrato (terceirizado);

10.10.2. Em até dois meses, nos demais casos.

10.11. As caixas postais do correio eletrônico institucional possuem tamanho limitado, definido conforme a capacidade e disponibilidade constante em contrato com a empresa provedora do serviço.

10.12. Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar o limite de tamanho estabelecido.

10.13. É vedada a utilização do correio eletrônico institucional para:

10.13.1. Realizar Spam;

10.13.2. Contribuir com a continuidade de correntes de mensagens eletrônicas;

10.13.3. Utilizá-lo com objetivos político-partidários, religiosos, entre outros;

10.13.4. Receber de forma consentida, armazenar ou enviar mensagens com:

10.13.4.1. Vírus de computador e outros códigos maliciosos;

10.13.4.2. Material pornográfico, atentatório à moral e aos bons costumes ou ofensivos;

10.13.4.3. Conteúdo criminoso, ilegal, ou que façam sua apologia;

10.13.4.4. Conteúdo discriminatório (racial, religioso, etc.) ou de incitação à violência;

10.13.4.5. Conteúdo que desrespeitem os direitos autorais.

10.14. De forma a preservaro funcionamento do serviço de correio eletrônico institucional, o usuário deve:

10.14.1. Eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive as existentes nas pastas personalizadas, na lixeira, rascunho e enviados, de forma a não exceder o limite de tamanho da caixa postal;

10.14.2. Evitar clicar em links de acesso a páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem iniciar a instalação de

softwares maliciosos ou direcionar o usuário da rede de dados para um site falso, possibilitando a captura de informações;

10.14.3. Evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência. No caso de suspeita de irregularidade na mensagem, o usuário deve solicitar ajuda à área de TI;

10.15. O uso da conta de correio eletrônico institucional em listas de discussão ou distribuição deve se limitar aos casos de necessidade do trabalho ou atividade desempenhada na FCRB.

10.16. O correio eletrônico particular não deve ser utilizado para o envio ou recebimento de informações da FCRB.

10.17. O correio eletrônico institucional não deve ser utilizado para fim particular, como cadastro de comércio eletrônico, por exemplo.

10.18. A FCRB não se responsabiliza em fornecer suporte técnico ao correio eletrônico particular.

10.19. O correio eletrônico institucional pode ser monitorado e restringido pela área de TI, quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados).

10.20. Nos casos de suspeita de infração à Política de Segurança da Informação e Comunicações, a área de TI poderá acessar a caixa postal institucional do respectivo usuário através de ato administrativo ou judicial;

11. Sobre a segurança física no CPD

11.1. Somente será permitido o acesso ao CPD nos seguintes casos:

11.1.1. Aos servidores do setor de Informática da FCRB com a liberação da porta de acesso por meio da identificação biométrica ou em caso de exceção, somente o cartão (crachá).

11.1.2. Aos demais servidores da FCRB, quando for necessário, acompanhados, por pelo menos uma pessoa do Serviço de Tecnologia da Informação e Comunicação.

11.1.3. Todos os demais casos, onde seja preciso o acesso de alguma pessoa ao CPD, este deverá ser autorizado pelo STIC seguindo as regras de identificação de visitantes da FCRB.

11.1.4. O acesso ao CPD fora do horário de expediente deve ser autorizado pelo STIC e seguir as regras de identificação da FCRB.

11.2. A localização do CPD deve ser ocultada às pessoas que transitam em áreas públicas;

11.3. O CPD deve estar posicionado em local seguro, protegido por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso de acordo com criticidade associada aos seus ativos e informações;

11.4. A edificação do CPD deve ser protegida contra descargas elétricas atmosféricas;

11.5. A edificação do CPD deve ser livre de sistemas de tubulação de drenagem pluvial, tubulação pressurizada de gases, exceto para a finalidade de combate a incêndio;

11.6. As portas e janelas do CPD devem ser mantidas fechadas;

11.7. Equipamentos de contingência e mídias com cópias de segurança devem ser armazenados a uma distância segura da instalação principal;

11.8. As instalações elétricas, de cabeamento lógico e dos equipamentos de detecção e combate a incêndio devem ser feitas de acordo com o especificado nas normas da ABNT;

11.9. É proibido o manuseio de alimentos, bebidas e cigarros, bem como o consumo no CPD.

11.10. Preferencialmente não ligar mais de um equipamento em uma mesma tomada;

11.11. Os equipamentos de TI do CPD devem ser instalados em racks, sempre que possível;

11.12. Todos os racks do CPD devem ser seguros, possuírem, preferencialmente, portas dotadas de chaves em todos os seus lados e permitirem trancamentos, de maneira que as tomadas de energia permaneçam no seu interior e os fios e cabos sejam acondicionados sem contato com a parte externa, diretamente do piso para o interior do rack;

11.13. Os equipamentos cuja dimensão impeça a instalação dentro de racks devem ter seus botões de ligar/desligar devidamente protegidos contra acessos ou internamente desconectados, de forma a evitar seu acionamento local;

11.14. As chaves dos racks e dos quadros de força devem receber identificação e serem guardadas em um claviculário em local adequado, protegido contra acesso indevido;

11.15. Todos os cabos existentes no CPD devem ser identificados;

11.16. Quando possível, os pontos de rede inoperantes devem ficar inativos;

11.17. O cabeamento deve ser implementado de acordo com a ABNT NBR 14.565:2007 - Cabeamento de telecomunicações para edifícios comerciais;

11.18. Os cabos de dados devem ser lançados em bandejas ou dutos rígidos, separados dos cabos e fios elétricos, de forma a evitar interferências eletromagnéticas;

11.19. Os circuitos específicos (elétrico, telefônico, sinalização, controle, sonorização e dados) devem ser identificados e instalados em eletrodutos ou bandejas separados dos demais circuitos de fornecimento de energia.

11.20. O circuito de energia que alimenta os recursos de tecnologia no interior do CPD, deve ser estabilizado e separado dos demais circuitos.

11.21. Devem ser implementados estabilizadores centrais ou individuais equipados com filtros contra variação de tensão.

11.22. Nobreaks e geradores de energia devem ser instalados, a fim de garantir a continuidade no fornecimento de energia aos equipamentos críticos para os serviços alocados no CPD.

11.23. Os circuitos elétricos devem ser divididos e protegidos por disjuntores, dimensionados de acordo com normas específicas.

11.24. Os disjuntores dos quadros de distribuição de energia devem identificar claramente cada circuito elétrico.

11.25. O quadro de distribuição de energia, painéis de controle e caixas de passagem do cabeamento lógico devem ser protegidos contra acesso indevido.

11.26. Os acessos ao CPD devem ser monitorados por circuito fechado de TV (CFTV). Câmeras de monitoramento devem ser instaladas em locais estratégicos do ambiente, seja ele interno ou externo.

11.27. Os circuitos das câmeras de monitoramento devem ser protegidos por conduítes de metal e ficar fora do alcance manual, evitando-se desativação intencional ou acidental.

11.28. As imagens captadas pelas câmeras do circuito interno de TV devem ser gravadas de forma contínua, visando embasar futuras investigações em caso de suspeitas ou incidentes de segurança.

11.29. Os arquivos das imagens gravadas devem ser guardados pelo período mínimo de 20(vinte) dias, sendo tratados com os mesmos critérios das mídias de cópia de segurança.

11.30. O sistema de circuito fechado de TV deve ser monitorado, alertando a equipe em caso de indisponibilidade no funcionamento.

11.31. As portas de acesso devem possuir dispositivo de controle de acesso, tais como crachá por aproximação e biometria.

11.32. Somente pessoas autorizadas pelo STIC podem portar equipamentos eletrônicos portáteis (celular, *pen drive*, *palms*, etc.) no interior do CPD.

11.33. O sistema de ar-condicionado deve ser redundante.

12. Sobre cópias de segurança

12.1. As cópias de segurança das informações e de software serão efetuadas e testadas pela área de TI.

12.2. A infraestrutura para a geração de cópias de segurança deverá ser adequada para garantir que toda informação essencial possa ser recuperada.

12.3. A área de TI é a responsável pelo processo de cópias de segurança no âmbito da FCRB.

12.4. As cópias de segurança devem ser realizadas em horário de baixa utilização das informações, preferencialmente fora do horário de expediente.

12.5. Sendo inevitável a realização de cópias de segurança no horário do expediente deverá ser justificada antecipadamente, caso haja necessidade de parada do serviço ou queda no desempenho dos recursos de TI.

12.6. A área de TI, junto com o responsável pela informação, deve definir e regulamentar os critérios necessários das cópias de segurança, a frequência, a extensão (completa, diferencial e incremental) e o seu período de retenção.

12.7. Cabe à área de TI definir procedimentos para a geração e restauração das cópias de segurança, mantendo os registros completos e fidedignos.

12.8. Os mecanismos de cópias de segurança devem ser automatizados, a fim de facilitar os processos de geração e recuperação.

12.9. As mídias devem ser devidamente identificadas de forma a permitir sua rápida localização e recuperação.

12.10. O usuário deve solicitar formalmente a restauração de uma cópia de segurança, de acordo com procedimento definido e tempo estimado pela área de TI.

13. Sobre aquisição, desenvolvimento e manutenção de sistemas de informação

13.1. Todos os requisitos de segurança devem ser identificados e justificados na fase de definição de um projeto, acordados e documentados.

13.2. Todos os usuários que utilizarão um sistema devem ser treinados e capacitados.

13.3. Devem ser documentados os procedimentos para a instalação e atualização de softwares.

13.4. O suporte dos sistemas somente poderá ser realizado após abertura de chamado (para registro dos eventos).

13.5. No caso de desenvolvimento interno de sistemas, a preservação e a documentação do código fonte deverão ficar sob a responsabilidade do STIC.

14. Sobre acesso remoto

14.1. O acesso remoto a uma rede de dados da FCRB será permitido em caráter excepcional e somente para fins de trabalho.

14.2. Deve ser formalizado junto à área de TI o pedido de acesso remoto, justificando a necessidade de acesso e período de uso.

14.3. A área de TI deve registrar e monitorar o acesso remoto do usuário.

14.4. O acesso remoto a uma rede de dados da FCRB deve ser realizado por meio de canal criptografado e solicitação de autenticação do usuário.

14.5. A área de TI deve prover mecanismos de proteção adequados às redes de dados sob sua responsabilidade, bem como aos serviços a elas conectados.

14.6. O usuário é responsável por toda e qualquer operação (acesso, processamento, comunicação, etc.) realizada através de um acesso remoto.

15. Sobre o uso de redes sociais

15.1. As redes sociais na FCRB podem ser utilizadas para a comunicação entre pessoas, empresas, órgãos e entidades públicas e privadas, desde que seu uso não comprometa a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação da instituição;

15.2. O uso das redes sociais deve respeitar a legislação vigente, a Política de Segurança da Informação e Comunicações (POSIC) da FCRB e quaisquer outros atos normativos complementares;

15.3. A área de comunicação deve designar um servidor público, para responder por um ou mais perfis institucionais nas redes sociais e ser responsável pela equipe e sua coordenação.

15.4. A área responsável por uma conta com perfil institucional em uma rede social deve utilizar o e-mail institucional (Ex: @rb.gov.br) da área responsável;

15.5. É vedada a utilização de e-mail institucional em redes sociais por usuários que não tenham o papel de produzir ou disseminar conteúdo de caráter institucional;

15.6. Todo usuário ao acessar uma rede social (independentemente de seu perfil de acesso) é responsável pelas informações veiculadas ou que de alguma forma tenham relação com a instituição;

15.7. O usuário deve se certificar sobre a autenticidade de uma informação antes de divulgá-la em uma rede social, quando utilizando a rede institucional;

15.8. O usuário responsável por uma conta institucional em uma rede social deve adotar comportamentos que protejam esta conta. Alguns exemplos são:

15.8.1. Criar senhas fortes;

15.8.2. Manter a senha em sigilo;

15.8.3. Trocar a senha periodicamente;

15.8.4. Evitar salvar senhas no navegador;

15.8.5. Não deixar o computador desbloqueado quando se afastar dele;

15.8.6. Desconectar-se da rede social ao acabar o trabalho.

16. Sobre segurança física – Sistema Integrado De Comando E Controle Patrimonial

16.1. Para acesso de usuários externos nas instalações prediais da FCRB, a recepção do edifício sede deverá efetivar um cadastro no sistema de segurança a partir de um documento de identificação pessoal e entregará um crachá provisório com as específicas autorizações de acessos.

16.2. A recepção do edifício deverá atentar-se quanto à obrigatoriedade da devolução de crachás, quando da saída do usuário externo.

16.3. A recepção do edifício deverá, sempre, comunicar os eventos de desaparecimento de crachás ao gestor de segurança;

16.4. O desaparecimento de crachás indicado pela recepção deverá ser objeto de comunicação ao gestor do sistema para o seu bloqueio imediato, para análises da ocorrência e para outras providências que se julgarem necessárias.

16.5. Para acesso às instalações prediais da FCRB, todo usuário interno (servidores, terceirizados, estagiários ou bolsistas) deverá ter o seu cadastro no sistema de acessos efetivado pelos setores Serviço de Administração de Recursos Humanos (SARH) e pelo Serviço de Informática (STIC). Um formulário para cadastro de usuários e suas permissões de acessos, devidamente preenchido e autorizado pelas diretorias, deverá ser o instrumento de liberação no sistema para o trânsito de usuários internos nas dependências da FCRB.

16.6. Para desempenho das atividades dos usuários em geral somente deverão ser cadastradas as áreas com acessos autorizados aos seus deslocamentos.

16.7. Para o acesso em locais sensíveis, relativos ao uso de biometria, os usuários internos autorizados, com deficiências em suas impressões digitais, terão autorização excepcional para o uso somente de crachás, mediante a assinatura de um termo de responsabilidade.

16.8. Os crachás de identificação e acesso às dependências da FCRB são de uso obrigatório, responsabilizando-se, o usuário, pela comunicação imediata ao gestor do sistema no caso de perda, extravio, furto ou desaparecimento, mesmo que momentâneo.

16.9. Quando da comunicação de perda, extravio, furto ou desaparecimento de crachás, caberá ao gestor do sistema o seu imediato bloqueio.

16.10. Para o caso de todo e qualquer usuário interno (servidores, terceirizados, estagiários ou bolsistas), ser efetivamente desligado de suas atividades de trabalho, deverão ser executados os bloqueios de acessos e deverão ser recolhidas as suas identificações funcionais, crachás, etc. Caberá SARH a retenção de identificações e a responsabilidade pela comunicação dos desligamentos e os referidos bloqueios de crachás.

16.11. As informações geradas pelo CFTV deverão ser gravadas e estar disponíveis para visualizações.

16.12. As solicitações para visualizações das imagens deverão ser solicitadas ao CGA, podendo este, permitir ou não.

16.13. Os backups, ou seja, o registro referente ao CFTV, deverão ser armazenados em local seguro pelo prazo de 20(vinte) dias.

16.14. A percepção visual de ocorrências (acessos, intrusão, incêndio) através do CFTV, ou aquelas registradas via sistema, deverão ser comunicadas ao gestor de20 segurança da FCRB, e ainda, deverão ser apontadas em livro de ocorrências e em relatórios impressos.

16.15. A impressão de relatórios de ocorrências do sistema (acessos, intrusão, incêndio) deverá ser efetivada, impreterivelmente, no primeiro (1º) dia útil subsequente a qualquer recesso. Em caso de ocorrência excepcional, independentemente de recesso, também deverá ser impresso o relatório, em momento subsequente à ocorrência ou no próximo dia útil.

16.16. Todos os documentos gerados a partir de ocorrências deverão ser encaminhados ao gestor de segurança para análise e providências adicionais.

16.17. Os registros de ocorrências do sistema deverão ser objeto de backup, obedecerão às normas de segurança desta POSIC e terão armazenamento pelo prazo de 180 (cento e oitenta) dias.