PoSIC

Política de Segurança da Informação e Comunicações



# Ministério da Cultura

# Fundação Casa de Rui Barbosa

### Manolo Garcia Florentino

### **Presidente**

### **Comitê Gestor de Tecnologia da Informação**

### Manolo Garcia Florentino - Presidente

### Carlos Renato Marinho – Diretor Executivo

### Ana Maria Pessoa dos Santos – Diretora do Centro de Memória e Informação

### José Almino de Alencar e Silva Neto – Diretor do Centro de Pesquisas

### Sérgio Paulo Futer – Coordenador Geral de Planejamento e Administração

### Andréa Castelo Branco Magalhães – Chefe do Serviço de Informática

### **Equipe de Elaboração**

### Amanda Britto Siqueira

### Andréa Castelo Branco Magalhães

### Eduardo Pinheiro da Costa

### Luiz Carlos Baltazar Gonçalves

### Ricardo da Silva Fonseca

Sumário

1. Apresentação da FCRB ........................................................................................................... 4
2. Missão da FCRB ...................................................................................................................... 4
3. Objetivo .................................................................................................................................. 4
4. Escopo .................................................................................................................................... 5
5. Conceitos e Definições ........................................................................................................... 6
6. Referências Legais e Normativas ........................................................................................... 10
7. Princípios .............................................................................................................................. 12
8. Diretrizes Gerais …….............................................................................................................. 13
9. Penalidades............................................................................................................................ 15
10. Competências e Responsabilidades ...................................................................................... 15
11. Atualização ............................................................................................................................ 17
12. Vigência ……............................................................................................................................ 17
13. Normas Internas……................................................................................................................ 17
14. Disposições Finais ................................................................................................................... 45

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**

1. Apresentação da FCRB

 A Fundação Casa de Rui Barbosa é uma instituição pública federal, vinculada ao Ministério da Cultura, e oferece 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.
1. 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 da Cultura.

1. 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) deve ser imediatamente esclarecido com a área de Gestão de Segurança da Informação.

1. ESCOPO
	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 dos negócios da FCRB, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais e valores éticos.
	2. Abrangência e vigência
		1. A Política de Segurança da Informação e Comunicações (PoSIC) se aplica a todos 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.
		2. A PoSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.
2. CONCEITOS E DEFINIÇÕES
	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.
	2. Ameaça: Conjunto de fatores externos ou causa potencial de um incidente.
	3. Ativo de informação: qualquer pessoa, tecnologia, processo ou ambiente que processe, armazene, transporte ou descarte informação institucional.
	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. 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.
	6. Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura que a suporta.
	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.
	8. Irretratabilidade ou não repúdio - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita
	9. Mecanismos de certificação: Atesta a validade de um documento.
	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.
	11. Mecanismos de controle de acesso: Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
	12. Mecanismos de garantia da integridade da informação: Usando funções de "Hashing" ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.
	13. 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.
	14. 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.
	15. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
	16. Contas 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.
	17. CPD (Centro de Processamento de Dados): local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização. Pode ser interno ou externo(CPD contratado).
	18. Diretriz: Conjunto de instruções ou indicações que orientam o que deve ser feito para se alcançar os objetivos estabelecidos na política.
	19. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
	20. 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.
	21. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.
	22. Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medias de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.
	23. Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão.
	24. 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.
	25. Incidente de segurança: qualquer evento indesejado ou inesperado, que comprometa as operações ou ameace a segurança da informação;
	26. Informação: - Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.
	27. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
	28. Metodologia de Desenvolvimento de Sistemas: conjunto de práticas que define o processo de desenvolvimento de sistemas de informação.
	29. Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.
	30. Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.
	31. Plano de Recuperação de Desastres: documentação dos procedimentos e informações necessárias para que o órgão ou entidade da Administração Pública Federal operacionalize o retorno das atividades críticas a normalidade.
	32. 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.
	33. Quebra de segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC da FCRB.
	34. Redes Sociais: Estruturas sociais, disponíveis na rede mundial de computadores (Internet), compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.
	35. 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.
	36. Senha forte: Deve ter no mínimo 8 caracteres e conter letras, números e caracteres especiais.
	37. Severidade: índice ou grau que se refere à medição do impacto de um evento ou incidente de segurança da informação.
	38. Usuário(s): 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, formalizada por meio da assinatura de um Termo de Responsabilidade.
	39. 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.
3. REFERÊNCIAS LEGAIS E NORMATIVAS

• 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.

• 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.

• 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.

• 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)

• 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.

• 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).

• 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)

• 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.

• 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.

• 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.

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

• 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.

• NBR ISO/IEC 27001:2006 –Tecnologia da Informação –Técnicas de segurança –Sistemas de Gestão de Segurança da Informação –Requisitos.

• NBR ISO/IEC 27002:2005 –Tecnologia da Informação –Técnicas de segurança –Código de prática para a Gestão da Segurança da Informação.

• Norma ABNT NBR ISO/IEC 27005:2008, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação e Comunicações.

• Norma ABNT NBR/ISO/IEC 15999:2007, que institui o código de melhores práticas para Gestão de continuidade de negócios.

• Norma ABNT NBR/ISO/IEC 27001:2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações.

• Norma ABNT NBR/ISO/IEC 27002:2005, que institui o código de melhores práticas para práticas para

• Gestão de Segurança da Informação e Comunicações.

• 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.

* Portaria Nº 36, de 02 de Agosto de 2012 – Institui o Comitê Gestor de Tecnologia da Informação – da Fundação Casa de Rui Barbosa
* 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
* Portaria Nº 3, de 09 de Janeiro de 2015 – Institui o Comitê Gestor de Segurança da Informação – da Fundação Casa de Rui Barbosa
1. 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):

a) 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.

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

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

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

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

f) 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.

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

h) 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.

i) 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.

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

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

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

1. **DIRETRIZES GERAIS**

Para fins desta Portaria ficam estabelecidas as seguintes diretrizes gerais:

* 1. Tratamento das informações
		1. Os ativos de informação da instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados.
		2. Todo ativo de informação deve possuir um responsável explicitamente identificado.
		3. Informações confidenciais da FCRB não podem ser transportadas em qualquer meio sem as devidas autorizações e proteções.
		4. Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas.
	2. Tratamento de incidentes de redes
		1. Os incidentes de segurança da informação devem ser registrados e gerenciados.
		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.
	3. Gestão de risco
		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.
	4. Gestão de continuidade
		1. Deve ser adotada a gestão de continuidade de negócios 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.
	5. Conformidade
		1. Deve-se manter a conformidade com as legislações vigentes.
	6. Controles e monitoramento de acesso.
		1. Todo acesso à informação sigilosa se dará através de mecanismos de identificação e controle de acesso.
		2. Todos os usuários da FCRB devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da PoSIC e demais regulamentações em vigor.
		3. Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação.
		4. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o reconhecimento do envolvido.
	7. Segurança de recursos humanos
		1. Todo agente público deve ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de informação, inclusive por ocasião da mudança de atividades.
	8. Segurança física e do ambiente
		1. Todo ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade.
	9. Gerenciamento de operações e comunicações
		1. Deve-se garantir a operação segura e correta dos recursos de processamento da informação.
		2. Aquisição, desenvolvimento e manutenção de sistemas
		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.
		4. Todo desenvolvimento de sistemas de informação para a FCRB deve ser realizado com base em uma Metodologia de Desenvolvimento de Sistemas publicada.
	10. Ativos de TI
		1. Os recursos de tecnologia da informação 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.
1. **PENALIDADES**

O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (PoSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

1. **COMPETÊNCIAS E RESPONSABILIDADES**

Instituir, no âmbito da Fundação, a seguinte estrutura para Gestão da Segurança da Informação e Comunicações:

I. O Gestor de Segurança da Informação e Comunicações, que será designado pela autoridade máxima desta Fundação e deverá ser um representante da alta administração;

 São competências do Gestor de Segurança da Informação e Comunicações:

1. Submeter esta POSIC à autoridade máxima desta Fundação para aprovação e sua posterior publicação.
2. Promover cultura de segurança da informação e comunicações;
3. 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.
4. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
5. Propor recursos necessários às ações de segurança da informação e comunicações;
6. Coordenar o Comitê de Segurança da Informação e Comunicações
7. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
8. 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;

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

 São competências do Comitê de Segurança da Informação e Comunicações:

1. Assessorar na implementação das ações de segurança da informação e comunicações;
2. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
3. Propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;
4. Propor alterações na PoSIC;
5. **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 três anos.

1. **VIGÊNCIA**

A presente Portaria entra em vigor na data de sua publicação.

1. **NORMAS INTERNAS**
	1. **NORMA INTERNA DE RESPONSABILIDADES DO USUÁRIO**

13.1.1 OBJETIVO

Esta norma dispõe sobre as responsabilidades do usuário quanto ao uso de senhas e equipamentos, mesa limpa e tela limpa.

13.1.2 REGRAS

13.1.2.1 Disposições gerais

13.1.2.1.1 Todo usuário deve conhecer e cumprir a Política de Segurança da Informação e Comunicações (POSIC) e as legislações em vigor referenciadas nesta norma.

13.1.2.1.2 Colaborar com a difusão da POSIC dentro da Fundação.

13.1.2.1.3 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.

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

13.1.2.2 Uso de recursos de TI

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

13.1.2.2.2 Utilizar os recursos de TI colocados à sua disposição somente para os fins institucionais aos quais se destinam.

13.1.2.2.3 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.

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

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

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

13.1.2.2.7 Todo ativo de informação deve ter seu uso restrito ao local de trabalho, salvo, para os casos de necessárias tramitações externas autorizadas.

13.1.2.3 Uso de dispositivos portáteis

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

13.1.2.4 Uso da identificação e senhas de acesso

13.1.2.4.1 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.

13.1.2.4.2 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 em nenhuma hipótese.

13.1.2.4.3 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.

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

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

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

13.1.2.5 Política de mesa e tela limpas

13.1.2.5.1 Os documentos impressos devem ser classificados em conformidade com a legislação vigente.

13.1.2.5.2 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.

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

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

13.1.2.6 Descarte de informações

13.1.2.6.1 Os ativos não mais utilizados pelos usuários, em meio eletrônico ou não, devem ser apagados ou destruídos conforme regras da legislação vigente.

 13.1.2.7 Propriedade da Informação

13.1.2.7.1            As informações produzidas por usuários no exercício de suas funções são patrimônio intelectual da FCRB e não cabe a seus criadores qualquer forma de exploração  sobre essas informações, preservando-se sempre o direito autoral moral.

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

* 1. **NORMA INTERNA DE USO DA INTERNET**

13.2.1 OBJETIVO

Esta norma dispõe sobre as regras de segurança relativas ao uso do serviço da Internet.

13.2.2 REGRAS

13.2.2.1 Disposições gerais

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

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

13.2.2.1.3 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.

13.2.2.1.4 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.

13.2.2.1.5 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.

13.2.2.2 Permissão de acesso

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

13.2.2.2.2 O acesso à Internet dependerá do processo de credenciamento do usuário junto ao SARH/CGPA.

13.2.2.3 Cancelamento e bloqueio do acesso à Internet

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

13.2.2.4 Uso da Internet

13.2.2.4.1 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.

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

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

13.2.2.4.4 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.

13.2.2.4.5 É vedada a utilização da Internet para:

• Acessar sites com códigos maliciosos;

• Acessar sites com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

• 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;

• Acessar sites ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares;

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

• Realizar atividades relacionadas a jogos eletrônicos pela Internet;

• Escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho na FCRB;

• Acessar sites para transferência de arquivos, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho da FCRB;

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

13.2.2.4.6 O usuário deve sempre se certificar da procedência do site, verificando, quando cabível, o certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do site diretamente no navegador.

13.2.2.4.7 É vedado aos usuários disponibilizar informações de propriedade da FCRB em sites da Internet sem observar sua classificação e o público a que se destina.

13.2.2.4.8 A utilização de equipamentos pessoais no ambiente da FCRB não poderá ser realizada por meio da rede corporativa, salvo quando a Unidade dispuser de uma rede isolada específica para este fim e mediante a concordância do termo de responsabilidade pelo usuário.

13.2.2.5 Monitoramento

13.2.2.5.1 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.

13.2.2.5.2 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:

* Suspeita de infração à Política de Segurança da Informação e Comunicações.
* Necessidade de visualizar os sites acessados e o tempo gasto nos mesmos por seus usuários de rede.
* Outros casos previstos em Lei.
	1. **NORMA INTERNA DE USO DO E-MAIL**

13.3.1 OBJETIVO

Esta norma dispõe sobre as regras de segurança relativas ao uso do serviço de correio eletrônico.

13.3.2 REGRAS

13.3.2.1 Disposições gerais

13.3.2.1.1 A conta de correio eletrônico institucional, disponibilizada aos usuários da rede de dados pela FCRB, deve ser utilizada somente para os interesses de trabalho.

13.3.2.1.2 A conta de correio eletrônico institucional disponibilizada ao usuário da rede de dados pela FCRB é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências.

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

13.3.2.1.4 Quando a área de TI permitir o uso do correio particular, o usuário não deverá exceder os limites da ética, bom senso e razoabilidade, sendo o responsável pelo conteúdo trafegado e seus eventuais riscos.

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

13.3.2.2 Permissão de acesso e criação de contas

 13.3.2.2.1 O usuário terá direito a uma única conta de e-mail que o identificará univocamente em toda FCRB.

13.3.2.2.2 O responsável pelo usuário da rede de dados da Unidade deve avaliar a necessidade de utilização do correio eletrônico institucional, indicando tal necessidade quando da solicitação da criação da conta de acesso aos recursos de TI.

13.3.2.2.3 A caixa postal compartilhada ou lista de discussão deve ter um responsável e um substituto formalizados.

13.3.2.3 Cancelamento, bloqueio, suspensão ou desbloqueio do correio eletrônico.

13.3.2.3.1 Cabe ao SARH comunicar à área de TI o cancelamento, bloqueio, suspensão ou desbloqueio da conta de correio do usuário.

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

a) Em até seis meses no caso de aposentadoria do servidor público;

b) Imediatamente ao desligamento, nos demais casos.

13.3.2.4 Uso do correio eletrônico

13.3.2.4.1 As caixas postais do correio eletrônico institucional possuem tamanho limitado, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo da área de TI provedora do serviço definir esses limites.

13.3.2.4.2 Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar o limite de tamanho estabelecido pela área de TI provedora do serviço.

13.3.2.4.3 É vedada a utilização do correio eletrônico institucional para:

• Realizar Spam;

• Contribuir com a continuidade de correntes de mensagens eletrônicas;

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

• Receber de forma consentida, armazenar ou enviar mensagens com:

a) Vírus de computador e outros códigos maliciosos;

b) Material pornográfico, atentatório à moral e aos bons costumes ou ofensivos;

c) Conteúdo criminoso, ilegal, ou que façam sua apologia;

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

 e) Conteúdo que desrespeitem os direitos autorais.

13.3.2.4.4 De forma a preservar o funcionamento do serviço de correio eletrônico institucional, o Usuário da rede de dados deve:

• 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;

• 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;

• 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 a área de TI;

13.3.2.4.5 Todo usuário da rede de dados da FCRB, antes de enviar mensagens pelo correio eletrônico institucional, deve levar em conta a classificação da informação, conforme legislação vigente.

13.3.2.4.6 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.

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

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

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

13.3.2.5 Monitoramento

13.3.2.5.1 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).

13.3.2.5.2 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;

* 1. **NORMA INTERNA DE SEGURANÇA FÍSICA NO CPD**

13.4.1 OBJETIVO

Esta norma dispõe sobre as regras para prevenção de acesso não autorizado, dano ou interferência às informações, recursos tecnológicos e instalações físicas em CPDs na FCRB.

13.4.2 REGRAS

13.4.2.1 Disposições Gerais

13.4.2.1.1 Somente será permitido o acesso ao CPD nos seguintes casos:

 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).

 Aos demais servidores da FCRB, quando for necessário, acompanhados, por pelo menos um servidor do Setor de Informática.

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

 O acesso ao CPD fora do horário de expediente(9h as 18h de segunda a sexta-feira) deve ser autorizado pelo SINF e seguir as regras de identificação da FCRB.

13.4.2.1.2 Os agentes públicos devem utilizar a identificação física em local de fácil visualização;

13.4.2.1.3 Os agentes públicos devem comunicar imediatamente a perda, furto ou desaparecimento da sua identificação física à área de segurança da informação;

13.4.2.2 Segurança ambiental

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

13.4.2.2.2 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;

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

13.4.2.2.4 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;

13.4.2.2.5 As portas e janelas do CPD devem ser mantidas fechadas;

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

13.4.2.2.7 Todo trabalho realizado por terceiros no CPD deve ser registrado e supervisionado;

13.4.2.2.8 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;

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

13.4.2.3 Instalação e proteção dos equipamentos

13.4.2.3.1 É proibida a ligação de mais de um equipamento em uma mesma tomada;

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

13.4.2.3.3 Todos os racks do CPD devem ser seguros, possuírem 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;

13.4.2.3.4 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;

13.4.2.3.5 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;

13.4.2.3.6 A identificação adotada deve ser de difícil dedução para pessoas estranhas ao ambiente;

13.4.2.3 Segurança do cabeamento

13.4.2.3.1 Todos os cabos existentes no CPD devem ser identificados;

13.4.2.3.2 Os pontos de rede excedentes devem ficar inativos;

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

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

13.4.2.4 Fornecimento de energia

13.4.2.4.1 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.

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

13.4.2.4.3 Devem ser implementados estabilizadores centrais ou individuais equipados com filtros contra variação de tensão e com monitoramento por voltímetro.

13.4.2.4.4 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.

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

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

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

13.4.2.5 Controles de segurança do CPD

13.4.2.5.1 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.

 13.4.2.5.2 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.

13.4.2.5.3 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.

13.4.2.5.4 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.

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

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

 13.4.2.5.7 É proibido comer, fumar ou beber no interior do CPD.

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

13.4.2.6 Sistema de ar condicionado

13.4.2.6.1 O sistema de ar-condicionado deve ser redundante.

* 1. **NORMA INTERNA PARA CÓPIAS DE SEGURANÇA**

13.5.1 OBJETIVO

Esta norma estabelece as diretrizes para a geração de cópias de segurança das informações e sua recuperação em um tempo aceitável.

 13.5.2 REGRAS

13.5.2.1 Disposições Gerais

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

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

13.5.2.2 Cópias de segurança da informação

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

13.5.2.2.2 Os equipamentos envolvidos no processo de cópias de segurança devem garantir que os dados selecionados sejam gravados na sua totalidade.

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

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

13.5.2.2.5 Cada área de TI 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.

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

13.5.2.2.7 Deve ser implementado um controle de acesso físico e lógico para as informações das cópias de segurança.

13.5.2.2.8 As cópias de segurança devem ser testadas regularmente e os registros das evidências dos testes devem ser devidamente documentados.

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

13.5.2.3 Armazenamento de mídias

13.5.2.3.1 As mídias devem ser armazenadas em local seguro com acesso restrito e controlado somente a usuários autorizados.

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

13.5.2.4 Restauração de cópias de segurança

13.5.2.4.1 A área de TI deve realizar regularmente testes de restauração das cópias de segurança em ambiente distinto ao de produção e suas evidências dos testes devem ser devidamente documentados.

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

**13.6 NORMA INTERNA DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO**

13.6.1 OBJETIVO

Esta norma estabelece as diretrizes de segurança para aquisição, desenvolvimento e manutenção de sistemas da informação no âmbito da FCRB.

13.6.2 REGRAS

13.6.2.1 Disposições gerais

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

13.6.2.1.2 Todo projeto de sistema de informação antes da sua concepção, inclusive aquele desenvolvido pelo usuário, deve ser submetido à área de TI para avaliação/homologação dos aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

13.6.2.1.3 Todos os usuários que utilizarão um sistema devem ser treinados e capacitados para exercer suas atividades.

13.6.2.2 Requisitos de segurança de sistemas de informação

13.6.2.2.1 Devem ser considerados requisitos de segurança na definição e aquisição dos novos sistemas.

13.6.2.2.2 Devem ser considerados requisitos de segurança em todas as fases de criação dos sistemas, ou seja, definição, projeto, desenvolvimento, implantação e manutenção.

13.6.2.3 Segurança dos arquivos do sistema

13.6.2.3.1 Devem ser documentos os procedimentos para a instalação e atualização de softwares.

13.6.2.3.2 A massa de dados utilizados nos testes da fábrica de software deve ser diferente da utilizada no ambiente de produção.

13.6.2.3.3 O acesso aos códigos fontes dos sistemas deve ser controlado e autorizado pela área de TI.

13.6.2.4 Segurança em processo de desenvolvimento e de suporte

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

13.6.2.5 Gestão de Vulnerabilidades técnicas

13.6.2.5.1 Devem ser avaliada e implementada medidas apropriadas para lidar com os riscos associados a uma eventual vulnerabilidade.

**13.7 NORMA INTERNA DE ACESSO REMOTO**

13.7.1 OBJETIVO

Esta norma estabelece as diretrizes para a realização de acesso à rede de dados da FCRB a partir de um local externo.

13.7.2 REGRAS

13.7.2.1 Disposições gerais

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

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

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

13.7.2.1.4 O acesso remoto deve ser concedido por um período de tempo pré-definido.

13.7.2.2 Do Acesso

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

13.7.2.2.2 A área de TI deve informar aos usuários os requisitos mínimos de segurança estabelecidos para realização de acesso remoto.

 13.7.2.2.3 Os recursos de Tecnologia da Informação –TI utilizados no ambiente de trabalho remoto, tal como residências, devem conter mecanismos de proteção contra vírus, software malicioso e controle de acesso.

13.7.2.2.4 O acesso a uma rede de dados da FCRB deve ser permitido somente a partir de recursos de TI que foram previamente cadastrados e homologados pela área de TI.

13.7.2.2.5 Quando os recursos de informática forem de propriedade de terceiros, a área de TI deve solicitar a estes que os referidos recursos atendam aos requisitos mínimos de segurança estipulados.

13.7.2.3 Responsabilidades

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

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

* 1. **NORMA INTERNA DE USO DE REDES SOCIAIS**

13.8.1 OBJETIVO

Esta norma estabelece diretrizes para o uso das redes sociais nos aspectos relativos à Segurança da Informação e Comunicações no âmbito da FCRB.

13.8.2 REGRAS

13.8.2.1 Disposições gerais

13.8.2.1.1 Entende-se como redes sociais as estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

13.8.2.1.2 As redes sociais na FCRB podem ser utilizadas para a comunicação institucional 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;

13.8.2.2 Diretrizes

13.8.2.2.1 As redes sociais ao serem utilizadas na FCRB por suas unidades devem ter como finalidade a aproximação da instituição com o cidadão, sendo entendidas como ferramentas para a prestação de serviços públicos de forma ágil e transparente, em consonância com os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência;

13.8.2.2.2 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;

13.8.2.3 Critérios

13.8.2.3.1 As áreas de comunicação devem designar um servidor público, ocupante de cargo efetivo, para responder por um ou mais perfis institucionais nas redes sociais e ser responsável pela equipe e sua coordenação. As equipes devem ser compostas exclusivamente por profissionais ocupantes de cargo efetivo da FCRB. No entanto, caso não seja possível, admite-se uma equipe mista;

13.8.2.3.2 É vedada a terceirização da administração e gestão dos perfis institucionais da FCRB nas redes sociais;

13.8.2.3.3 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;

13.8.2.3.4 As contas com perfil institucional devem ser associadas ao e-mail da área responsável pela conta em detrimento ao e-mail pessoal;

13.8.2.3.5 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;

13.8.2.4 Responsabilidades

13.8.2.4.1 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;

 13.8.2.4.2 O usuário deve se certificar sobre a autenticidade de uma informação antes de divulgá-la em uma rede social;

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

a) Criar senhas fortes;

b) Manter a senha em sigilo;

c) Trocar a senha periodicamente;

d) Não salvar senhas no navegador;

e) Não deixar o computador desbloqueado quando se afastar dele;

f) Manter antivírus instalado e atualizado;

g) Sair do serviço usando logout”link(ousimilar),“etc.

h) Tomar as devidas precauções ao acessar um link encurtado;

**13.9 NORMA INTERNA DE SEGURANÇA FÍSICA – SISTEMA INTEGRADO DE COMANDO E CONTROLE PATRIMONIAL**

13.9.1 OBJETIVO

Esta norma dispõe sobre as regras relativas ao Sistema Integrado de Comando e Controle de Segurança Patrimonial.

13.9.2 DEFINIÇÕES

13.9.2.1 Acesso: Ato de ingressar e transitar nas dependências da FCRB.

13.9.2.2 Biometria: método automático de reconhecimento individual baseado em medidas biológicas - anatômicas e fisiológicas. Na FCRB, refere-se à impressão digital.

13.9.2.3 Sistema Integrado de Comando e Controle de Segurança Patrimonial: conjunto de sistemas inter-relacionados necessários para o apoio à segurança física da instituição, entre eles: Sistema de Controle de Acessos, Circuito Fechado de Televisão (CFTV), Sistema de Alarme de Incêndio, Sistema de Detecção de Intrusão e o Centro de Comando e Controle e de Operações.

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

13.9.2.5 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.

13.9.2.6 Sistema de Alarme de Incêndios: Sistema responsável pela detecção e disparo de alarme de incêndios.

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

13.9.2.8 Centro de Comando e Controle: local destinado a abrigar um (1) posto de vigilância e as centrais controladoras dos sistemas envolvidos. É responsável pelo monitoramento, supervisão e registros de eventos, e por comandar ações necessárias ao controle da segurança patrimonial.

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

13.9.2.10 Ocorrência: episódio, evento, fenômeno considerado anormal ou incomum dentro dos procedimentos de segurança patrimonial ou aquele apontado e registrado pelo Sistema Integrado de Comando e Controle de Segurança Patrimonial;

13.9.3 REGRAS

13.9.3.1 Disposições gerais

13.9.3.1.1 O sistema de segurança patrimonial implantado na FCRB tem por finalidade colaborar com a segurança da informação na instituição.

13.9.3.1.2 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.

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

13.9.3.1.4 A recepção do edifício deverá, sempre, comunicar os eventos de desaparecimento de crachás ao Gestor de segurança;

13.9.3.1.5 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.

13.9.3.1.6 Para acesso as 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 (SINF). 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.

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

13.9.3.1.8 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.

13.9.3.1.9 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.

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

13.9.3.1.11 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.

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

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

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

13.9.3.1.15 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 subseqüente à ocorrência ou no próximo dia útil.

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

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

1. DISPOSIÇÕES FINAIS

14.1 Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações do Comitê Gestor ao Comitê de Segurança da Informação e Comunicações.

14.2 Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações do Comitê Gestor deve ser imediatamente notificado a fim de adotar as providências necessárias.

14.3 As notificações ao Serviço de Segurança da Informação e Comunicações devem ser comunicadas ao Comitê de Segurança da Informação e Comunicações.

14.4 Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo 7. PENALIDADES deste documento.

14.5 Os incidentes de segurança, quebra de segurança e denúncias de descumprimento à Política de Segurança da Informação e Comunicações e suas normas devem ser notificados ao Comitê de Segurança da Informação e Comunicações.