1 SUMÁRIO

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749

www.agerio.com.br

2 PREFÁCIO

TÍTULO

SEGURANÇA CIBERNÉTICA

UNIDADE GESTORA

SUTEC

UNIDADES CORRESPONSÁVEIS

GEITI, GEATI, GEINF, Gestores da Informação e Gestores de Sistemas

CLASSIFICAÇÃO

Norma de Política de Atuação

PÚBLICO-ALVO

Toda AGÊNCIA

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

Não se aplica.

RELAÇÕES COM OUTRAS NORMAS

POL.023 – Segurança da Informação

ORG.002 – Classificação e Tratamento da Informação

ORG.003 – Comunicação Administrativa

ORG.009 – Uso da Intranet e Internet

ORG.007 – Uso do Correio Eletrônico

REGULAMENTAÇÃO E DOCUMENTAÇÃO UTILIZADA

BACEN Resolução 4.658 Banco Central do Brasil

NBR ISO/27.000: Família de Normas de Segurança da Informação.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749

www.agerio.com.br

Lei n° 9.610 de 19/02/1998 - Lei de Direitos Autorais.

Lei n° 9.609 de 19/02/1998 - Lei de Software.

RES 463/2019

DEL 104/2019

NORMAS REVOGADAS

Não se aplica.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749

www.agerio.com.br

3 OBJETIVO

3.1 Orientar os empregados, estagiários, parceiros ou prestadores de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio quanto às diretrizes de segurança cibernética visando garantir a aplicação dos princípios e diretrizes de proteção do ambiente computacional, da propriedade intelectual, das informações da organização e dos clientes residentes neste ambiente.

4 DEFINIÇÕES

ABNT: Sigla da Associação Brasileira de Normas Técnicas que editas as Normas Brasileiras (NB).

Gestor: É todo empregado que detém função gratificada/cargo de livre provimento em comissão de gestão, podendo exercer o papel de gestor de unidade e/ou de gestor imediato de uma equipe.

Gestor da informação: Empregado da AGÊNCIA responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade e pela definição do nível de confidencialidade a ela atribuída.

Gestor de Segurança Cibernética – Diretor responsável pela matéria registrado devidamente no UNICAD do BACEN.

Gestor do sistema: pessoa responsável pela definição das funcionalidades, perfis de acesso, autorização de acesso aos sistemas de informação, nível de disponibilidade e integridade. Em sistemas corporativos podem ser definidos Gestores para módulos específicos.

Login Name ou Nome de Usuário ou Identificação Pessoal de Sistema: identificação pessoal para acesso aos recursos computacionais da AGÊNCIA, podendo ser utilizado o Login Name de rede, caso recomendável tecnicamente.

Parceiros: pessoa física ou jurídica, sem vínculo contratual que participa de um determinado processo da AGÊNCIA.

Prestadores de serviço: É toda empresa contratada pela AGÊNCIA para prestar serviços à população em seu nome, com critérios por ela estabelecidos.

Rede Corporativa Local: conjunto de servidores de rede e equipamentos de interconexão locais, interligados com o objetivo de disponibilizar serviços aos usuários da AGÊNCIA.

Recursos computacionais ou Dispositivos Cibernéticos: todo recurso utilizado na geração, processamento, armazenamento, transmissão, descarte e recuperação da informação em meio eletrônico, tais como;

Hardware:

a) Estações de Trabalho (computadores, notebooks, tablets, celulares e similares);

b) Servidores e equipamento de CPD;

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

c) Impressoras e similares;

d) Mídias ópticas e magnéticas;

e) Equipamentos de Rede LAN e WAN.

Software:

a) Sistemas de informação (Sistemas prontos, parametrizados, customizados ou desenvolvidos sob encomenda, interna ou externamente);

b) Softwares básicos (Sistemas Operacionais, Bancos de Dados, Pacotes de Automação de Escritório, Navegadores de Internet, programas de Correio Eletrônico e produtos adquiridos em "prateleira" e similares).

Sessão de trabalho: período em que o empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio, utilizando seu Login Name, encontra-se conectado à rede corporativa local da AGÊNCIA ou a seus servidores ligados à Internet/Extranet.

Unidades Gestoras (UG): As UGs são os componentes organizacionais que possuem gestor, equipe, atividades e responsabilidades, entendendo-se por superintendências, gerências e coordenadorias.

5 NORMAS

5.1 PRINCÍPIOS

5.1.1 Confidencialidade – Disponibilidade da informação ou dispositivo cibernético somente para a usuários, entidades ou processos autorizados.

5.1.2 Disponibilidade – Garantia de que usuários autorizados obtenham acesso à informação e dispositivos cibernéticos sempre que necessários.

5.1.3 Integridade – Exatidão, higidez e autenticidade da informação e dos métodos de processamento, visando à integralidade da informação e dos dispositivos cibernéticos.

5.1.4 Rastreabilidade – Existência de rastros que permitam esclarecer incidentes de segurança cibernética, coletados de forma proporcional aos riscos existentes.

5.1.5 Controles – Existência de controles para a implementação das normas.

5.1.6 Responsabilidade – Gestor de Segurança Cibernética em nível de diretoria.

5.1.7 Incidentes – Existência de Plano de Ação e de Resposta a Incidentes com aprovação pelo Conselho de Administração.

5.1.8 Serviços em Nuvem – Controles internos e do BACEN para contratação.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749

www.agerio.com.br

5.2 DIRETRIZES

5.2.1 Preservar a confidencialidade, integridade e disponibilidade das informações no ambiente cibernético da AgeRio conforme graus de sensibilidade pré-determinados;

5.2.2 Compatibilizar as medidas de segurança cibernética ao porte, produtos, acessos e modelo de negócios da AgeRio, em uma abordagem de medidas adequadas aos riscos assim como na sensibilidade quanto aos aspectos de confidencialidade, disponibilidade e integridade das informações;

5.2.3 Dar ciência a todos os envolvidos no ambiente cibernético da AgeRio das questões relacionadas a segurança cibernética, atribuindo responsabilidades também aos Gestores da Informação, Gestores de Sistemas e fornecedores de serviços cibernéticos.

5.2.4 Continuidade de TI – Designação de um Diretor responsável pela Política de Segurança Cibernética e pelo Plano de Ação e Resposta a Incidentes, que pode desempenhar outras funções na AgeRio, desde que não haja conflito de interesses. Este Diretor deve ser responsável pelo reconhecimento da necessidade dos serviços de TI para operação do negócio e planejamento de sua continuidade, defendendo sua relevância e investimentos adequados.

5.2.5 Reduzir os riscos de vazamento de dados e buscar rastreabilidade para garantia das informações sensíveis;

5.2.6 Cultura de Segurança Cibernética – Deve ser um compromisso de todos, patrocinada pela Diretoria quanto à sua melhoria contínua, cultivada junto a usuários e clientes, sendo amplamente divulgada. Usuários devem ser capacitados e avaliados sobre o tema e estar alerta para riscos e ameaças através de programas periódicos de treinamento. Clientes devem receber informações sobre a cultura de segurança e suas responsabilidades.

5.2.7 Os Gestores de Informação e Gestores de Sistemas serão designados pela DIREX.

5.3 CLASSIFICAÇÕES DO NÍVEL DE SENSIBILIDADE

5.3.1 Todo componente (informação ou dispositivo cibernético) da AGÊNCIA deverá ser classificado quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explicita ou implícita.

5.3.1.1 Quanto à confidencialidade: Os graus de confidencialidade estão descritos na Norma ORG.002 Classificação e Tratamento da Informação como Graus de Sigilo

5.3.1.2 Quanto à Disponibilidade:

a) **Alta** - Componente relacionado aos negócios e políticas administrativas da AGÊNCIA, cuja indisponibilidade poderá ter consequências incontornáveis nos seus processos, requerendo cuidados especiais para garantir sua disponibilidade.

b) **Normal** - Componente relacionado aos negócios e políticas administrativas da AGÊNCIA, cuja indisponibilidade não terá consequências incontornáveis, mas, caso persista, poderá

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

comprometer seus processos, requerendo cuidados moderados para garantir sua disponibilidade.

c) **Baixa** - Componente relacionado aos negócios e políticas administrativas da AGÊNCIA, cuja indisponibilidade não trará consequências para seus processos, requerendo cuidados mínimos para garantir sua disponibilidade.

5.3.1.3 Quanto à Integridade:

a) **Alta -** Componente relacionado aos negócios e políticas administrativas da AGÊNCIA, cuja falta de integridade poderá comprometer seriamente seus processos, requerendo cuidados especiais para garantir sua integridade.

b) **Normal** - Componente relacionado aos negócios e políticas administrativas da AGÊNCIA, cuja falta de integridade não terá consequências incontornáveis, mas, caso persista, poderá comprometer seus processos, requerendo cuidados moderados para garantir sua integridade.

c) **Baixa** - Componente relacionado aos negócios e políticas administrativas da AGÊNCIA, cuja falta de integridade não trará consequências para seus processos, requerendo cuidados mínimos para garantir sua integridade.

5.3.2 A informação armazenada ou transportada nos recursos computacionais da AGÊNCIA, que não possuir uma classificação explícita será considerada de uso interno (G10) quanto à confidencialidade e de nível normal quanto à disponibilidade e integridade, exceto material de propaganda e marketing, claramente de uso externo, em que não é aconselhável estampar a classificação.

5.3.3 A informação eletrônica armazenada ou transportada fora do ambiente cibernético da AgeRio será tratada pela SUTEC como de baixa disponibilidade e baixa integridade, e deverá receber de seu portador os cuidados inerentes à sua confidencialidade. São exemplos: Dispositivos móveis que contenham informação da Agência, Pen-drives, discos externos e outros.

5.4 RESPONSABILIDADES - SEGURANÇA ADEQUADA AO RISCO

5.4.1 Toda informação, gerada ou transformada pelos empregados, no exercício de suas atividades, é de propriedade da AGÊNCIA, e deverá ser protegida segundo as diretrizes descritas na Política de Segurança da Informação e nesta norma, no que tange às informações residentes em recursos computacionais.

5.4.2 Toda informação utilizada na AGÊNCIA deverá receber o tratamento adequado no momento da sua geração, atualização, acesso, guarda, proteção, controle e descarte, segundo a sua classificação.

5.4.3 A classificação da informação é atribuição do Gestor da informação, devendo este considerar o balanceamento entre a classificação da informação e o custo das medidas de segurança necessárias à sua proteção, podendo, para tanto, recorrer à SUTEC.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

5.4.4 No descarte de informações da AGÊNCIA deverão ser observados: a temporalidade prevista na legislação, as políticas, as normas, procedimentos internos e a classificação quanto à confidencialidade. O descarte de informações classificadas como confidenciais deverá ser realizado de forma a impossibilitar sua recuperação total ou parcial. O Gestor da Informação definirá essas questões junto à SUTEC.

5.4.5 Todos os sistemas deverão ter seus perfis de acessos e grau de sensibilidade definidos pelo Gestor do Sistema.

5.4.6 A SUTEC ao definir as medidas de segurança aplicáveis aos recursos físicos ou computacionais da AGÊNCIA deverá considerar o balanceamento entre os custos inerentes ao grau de segurança e a classificação da informação a proteger, obtendo aprovação do Gestor de Segurança Cibernética no nível de Diretoria às propostas formuladas com objetivo de prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com o ambiente cibernético.

5.5 CONTROLES TÉCNICOS ESPECÍFICOS DE SEGURANÇA E RASTREABILIDADE

5.5.1 Autenticação - Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários locais e remotos aos serviços de TI.

5.5.2 Criptografia - Deve ser desenvolvida e implementada uma norma para o uso de controles criptográficos para a proteção da informação onde isso seja requerido.

5.5.3 Prevenção e detecção de intrusão – Devem ser implementados métodos e ferramentas tecnológicas adequadas para prevenção de invasão no ambiente cibernético, detectar as ameaças em tempo hábil e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

5.5.4 Prevenção de vazamento de informações - Oportunidades para vazamento de informações devem ser prevenidas através de dispositivos e técnicas adequadas.

5.5.5 Realização periódica de testes e varreduras - Deve ser obtida informação em tempo hábil sobre vulnerabilidades técnicas do ambiente cibernético em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.

5.5.6 Proteção contra software malicioso – Deve-se implementar recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais.

5.5.7 Mecanismos de rastreabilidade – Devem ser compostos mecanismos adequados ao monitoramento da atuação dos componentes do ambiente cibernético da AgeRio, como logs de acesso, por exemplo. Os mecanismos devem balancear os riscos com os custos associados ao nível de controle.

5.5.8 Segmentação de redes de computadores - Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes conforme sua necessidade de acesso.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

5.5.9 Cópias de segurança de informações – Além de realizar cópias internas e externas nas frequências e prazos de retenção ajustados com as áreas de negócio, deve-se monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

5.5.10 Desenvolvimento de sistemas de informação seguros - Devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes, que podem ser traduzidos em requisitos não funcionais ou funcionais.

5.6 CONTROLE DE ACESSO

5.6.1 O acesso à informação e aos recursos físicos ou computacionais, pelo empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio, deverá ser relacionado às atividades profissionais do mesmo e aos interesses de negócios da AGÊNCIA.

5.6.2 O perfil de acesso a sistemas deverá ser apontado pelo Gestor da UG à qual o empregado, estagiários, parceiro ou prestador de serviço da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio está vinculado e confirmado pelo Gestor do Sistema ao qual ele terá acesso.

5.6.3 Todo empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio que utiliza qualquer recurso computacional deverá ter um Login Name, único e intransferível.

5.6.4 Quando do desligamento do empregado, estagiário, parceiro ou prestadores de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio das suas atribuições junto às AGÊNCIA, este deverá ter seu acesso aos recursos computacionais bloqueado imediatamente.

5.6.5 Após o bloqueio, o empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio que necessitar retirar suas informações particulares deverá solicitar a autorização de acesso ao seu superior imediato.

5.6.6 O acesso do empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio ao ambiente físico, que contenha informações da AGÊNCIA, deverá se restringir aos necessários e indispensáveis à realização de suas atividades, especialmente ao Datacenter.

5.6.7 O acesso de visitante ao ambiente físico da AGÊNCIA deve receber cuidados como acompanhamento e supervisão, de modo a assegurar a proteção das informações e componentes cibernéticos.

5.6.8 O acesso de prestadores de serviço ou visitante à internet será feito por rede apartada da Rede Local Corporativa.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

5.6.9 Casos em que o trabalho de prestadores de serviço requeira acesso à Rede Local Corporativa são excepcionais e devem ser ajustados junto à SUTEC, que concederá recursos apenas necessários às funções a serem desempenhadas e por tempo determinado.

5.7 AVALIAÇÃO DE VULNERABILIDADES

5.7.1 As vulnerabilidades do ambiente cibernético devem ser avaliadas, identificando-se as possíveis ameaças e o grau de exposição dos ativos a cada uma delas.

5.7.2 Devem ser considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de evento de segurança, assim como a expectativa de tal evento ocorrer, compondo cenários de incidentes para testes futuros.

5.7.3 Uma vez definidos os riscos, ações de prevenção e proteção devem ser tomadas.

5.8 MONITORAMENTO

5.8.1 Os acessos e uso dos recursos computacionais da AGÊNCIA devem ser monitorados por controles com parâmetros gerais, não personalizados.

5.8.2 Os procedimentos de monitoramento dos recursos físicos ou computacionais da AGÊNCIA devem ser compatíveis com os riscos, gerando registros que permitam a verificação de acesso e identificação de possíveis causas de quebras de segurança.

5.8.3 A periodicidade, detalhamento e período de guarda dos registros do monitoramento devem ser definidos pela área de compliance (GECIC) levando em conta o equilíbrio entre risco e custo do controle;

5.8.4 Os relatórios com os registros de controle podem ser solicitados pelas áreas competentes, com o propósito de apurar indícios do não cumprimento desta ou outras normas da AGÊNCIA.

5.8.5 São consideradas as áreas competentes: GECIC, Gestor do Sistema ou a Auditoria interna.

5.8.6 A saída dos recursos computacionais, que contenham informações de propriedade e/ou de interesse da AGÊNCIA, de suas instalações, deverá ser registrada e autorizada pelo Gestor da UG à qual o recurso pertence ou por pessoa designada por este, sendo proibido o seu transporte sem as medidas de proteção correspondentes.

5.8.7 A inserção de recursos computacionais no ambiente da AGÊNCIA traz riscos que deverão ser controlados, observando-se quanto a software, a necessidade de terem o adequado licenciamento para uso neste ambiente.

5.8.8 De forma a preservar a segurança das informações, os empregados da AGÊNCIA deverão, sempre que necessário, ser orientados para a correta utilização dos recursos físicos e computacionais.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

5.9 REGISTRO E AVALIAÇÃO DE RELEVÂNCIA DE INCIDENTES

5.9.1 Devem ser estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados, inclusive de serviços cibernéticos contratados.

5.9.2 Os incidentes devem ser avaliados de forma a prover inteligência de ameaças com o objetivo de identificar ameaças e reduzir incidentes futuros.

5.9.3 Deve ser avaliada a possibilidade de compartilhamento do incidente com outras instituições financeiras que possam estar submetidas aos mesmos riscos, preservadas as questões de sigilo e livre concorrência.

5.9.4 Comunicação ao BACEN em caso de incidentes que configurem uma situação de crise para a AgeRio, por paralização de serviços essenciais.

5.10 PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES CIBERNÉTICOS

5.10.1 O Plano de Ação e de Resposta a Incidentes Cibernéticos deve ser apresentado e aprovado pelo Conselho de Administração e revisado anualmente, sempre em consonância com os princípios de segurança adequada aos riscos.

5.10.2 O **Plano de Ação de Implementação de Segurança Cibernética** deve elencar todas as ações a serem desenvolvidas pela instituição para adequar sua estrutura organizacional e operacional ao disposto nesta Política.

5.10.3 Deve ainda elencar as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção de incidentes.

5.10.4 Os processos críticos deverão ser suportados por um **Plano de Resposta a Incidentes Cibernéticos** que responda a situações de anormalidade. Este plano deve ser documentado e, periodicamente, testado e revisado pela SUTEC.

5.10.5 O plano deve elencar as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na resposta de incidentes e prever também o processo de retorno às configurações originais, após o término do incidente.

5.10.6 Deve designar área específica para registro e controle de incidentes relevantes.

5.10.7 Os Gestores das UGs, de forma a garantir a integridade das informações, deverão assegurar que não haja um único empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio com a domínio e compreensão exclusivos de processos críticos.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

5.11 CULTURA DE SEGURANÇA E RESPONSABILIDADES

5.11.1 Os empregados, estagiários, parceiros ou prestadores de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio têm por obrigação cumprir esta Política de Segurança Cibernética e demais normas que a complementarem.

5.11.2 O empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio é responsável pelas ações efetuadas por meio da utilização de seu Login Name.

5.11.3 O empregado, estagiário, parceiro ou prestador de serviços da AGÊNCIA ou qualquer pessoa contratada direta ou indiretamente para prestar serviços à AgeRio é responsável pelos danos que, por sua ação ou omissão, possam ser causados às informações ou aos recursos computacionais da AGÊNCIA, em especial por meio da utilização de seu Login Name.

5.11.4 Ao receber a guarda de recurso computacional portátil disponibilizado pela AGÊNCIA, o usuário deverá assinar um Termo de Custódia e Utilização, o qual conterá as regras de utilização e preservação do mesmo.

5.11.5 O Gestor da Informação deve definir, em comum acordo com o Gestor do Sistema, o período de retenção, guarda ou preservação da informação nas cópias de segurança.

5.11.6 As áreas responsáveis pela administração dos recursos computacionais em parceria com a área de recursos humanos e/ou comunicação devem, periodicamente, promover a disseminação e aplicação dos conceitos de segurança da informação.

5.11.7 Deve ser divulgado publicamente um resumo desta política, com suas informações em linhas gerais.

5.12 SERVIÇOS EM NUVEM

5.12.1 Os serviços em nuvem devem ser considerados nas políticas, estratégias e estruturas para o gerenciamento de riscos.

5.12.2 Como condição para a contratação de serviços relevantes deverá ser verificar a capacidade da empresa prestadora de serviço (competência, recursos) de aderência às exigências da legislação em vigor e desta Política, inclusive através de relatórios de auditoria adequados.

5.12.3 A contratação de serviços em nuvem deve ser monitorada com os mesmos cuidados de serviços internos, no que tange aos quesitos de confidencialidade, integridade e disponibilidade.

5.12.4 Garantir contratualmente e por diligências prévias que a contratada é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

5.12.5 Garantir contratualmente que haja ferramental adequado ao monitoramento dos serviços a serem prestados e que a qualidade dos controles de acesso seja compatível com a sensibilidade dos dados.

5.12.6 Segregação física ou lógica dos dados em relação aos demais clientes do fornecedor.

5.12.7 Deve ser comunicada com sessenta dias de antecedência ao Banco Central do Brasil, indicando a empresa, os serviços, os países e regiões onde os dados serão processados e armazenados. Alterações contratuais também devem ser comunicadas.

5.12.8 A contratação dos serviços prestados no exterior deve ter como requisitos:

- **a)** definição país e região onde os dados serão processados e armazenados,
- **b)** existência de convênio BACEN com autoridades dos países,
- **c)** autorização do BACEN caso não exista convênio com os países,
- **d)** legislação dos países não restrinjam acesso da AgeRio e do BACEN,
- **e)** continuidade de negócio em caso de impossibilidade da prestação de serviço,
- **f)** medidas para garantir a segurança da transmissão e armazenamento da informação.

5.12.9 Quando da extinção do contrato, obrigatoriedade de transferência de dados para o novo prestador de serviço de maneira a garantir a continuidade do serviço, com posterior exclusão dos dados.

5.12.10 Devem ser observados todos os demais requisitos da Resolução 4.568 do BACEN para este tipo de contratação.

5.12.11 Toda informação depositada em recursos computacionais, se relacionada aos negócios e políticas administrativas da AGÊNCIA, deverá ser armazenada nos servidores da sua Rede Corporativa Local ou em ambientes de nuvem contratados pela SUTEC para este fim, que compõem o ambiente cibernético da AgeRio. As UGs não podem utilizar recursos de armazenamento em nuvem contratados diretamente, sejam gratuitos ou pagos, para armazenamento de informações da AgeRio.

5.13 CONTROLE DE CUMPRIMENTO DESTA POLÍTICA

5.13.1 Deve ser encaminhado ao Conselho de Administração, pelo Gestor da Segurança Cibernética, Relatório Anual de Segurança Cibernética (data–base 31/12), até o dia 31 de março de cada ano.

5.13.2 Este relatório deverá conter:

- **a.** Efetividade da Implementação do Plano de Ação de Implementação de Segurança Cibernética;
- **b.** Resumo dos resultados obtidos nas ações de prevenção e resposta a incidentes;
- **c.** Incidentes relevantes no período,

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br

d. Resultado dos testes de continuidade considerando os cenários de incidentes;

5.14 DISPOSIÇÕES GERAIS

5.14.1 As infrações a esta Norma e normas correlatas deverão ser comunicadas ao Gestor da Informação, do Sistema e ao superior imediato do infrator.

5.14.2 Em casos de quebra de segurança da informação nos recursos cibernéticos, a SUTEC deverá ser imediatamente acionada para tomar as providências necessárias para sanar as causas, podendo inclusive restringir temporariamente o acesso às informações e/ou ao uso dos recursos computacionais da AGÊNCIA.

5.14.3 Ao autor de infração a esta norma será aplicado processo de apuração de responsabilidades.

5.14.4 Os casos omissos serão resolvidos pelo Gestor de Segurança Cibernética.

6 PROCEDIMENTOS

Não se aplica

7 ARQUIVAMENTO DE DOCUMENTOS

Não se aplica

8 ANEXOS

8.1 Anexo I - Plano de Ação e de Resposta a Incidentes

Avenida Rio Branco, 245 – 3° andar – Centro - 20040-917 - Rio de Janeiro, RJ – Tel:(21)2333-1212
Ouvidoria: 0800-282-2749
www.agerio.com.br