DIÁRIO OFICIAL DA UNIÃO

Publicado em: 24/06/2019 | Edição: 119 | Seção: 1 | Página: 9

Órgão: Ministério da Cidadania/Agência Nacional do Cinema/Diretoria Colegiada

RESOLUÇÃO Nº 87, DE 18 DE JUNHO DE 2019

Altera a Política de Segurança da Informação e Comunicações da Agência Nacional do Cinema - ANCINE.

A DIRETORIA COLEGIADA DA AGÊNCIA NACIONAL DO CINEMA-ANCINE, no uso das atribuições que lhe conferem os Incisos II e IV do Artigo 6º do Anexo I do Decreto nº 8.283, de 3 de julho de 2014, tendo em vista a Resolução de Diretoria Colegiada ANCINE nº 63, de 23 de setembro de 2014; a Instrução Normativa nº 01 (GSI/PR), do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República, bem como suas Normas Complementares, e conforme decidido na 727ª Reunião de Diretoria Colegiada, de 18 de junho de 2019, assim resolve:

Art. 1º. Alterar o Anexo da Resolução de Diretoria Colegiada nº 63, de 23 de setembro de 2014, revisando a Política de Segurança da Informação e Comunicações da Agência Nacional do Cinema - ANCINE de acordo com a dispositivo que prevê sua revisão periódica.

Art. 2º. Esta Resolução entra em vigor na data de sua publicação.

CHRISTIAN DE CASTRO
Diretor-Presidente

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA ANCINE

1.OBJETIVO

Prover a AGÊNCIA NACIONAL DO CINEMA - ANCINE de norma de Segurança da Informação e Comunicações, estabelecendo responsabilidades e diretrizes para tratamento, controle e proteção, com o objetivo de preservar a confidencialidade, integridade, disponibilidade e autenticidade de informações e dados.

Visa, também, a orientar a construção de mecanismos quantitativos de avaliação de riscos, procedimentos preventivos para sua minimização, além de rotinas de tratamento de incidentes de segurança da informação, objetivando neutralizar seus efeitos.

2.ABRANGÊNCIA

Esta política é aplicável, no que couber, a todos os ambientes físicos e computacionais, ativos de informação, e às atividades de todos os servidores e colaboradores que atuam no âmbito da AGÊNCIA NACIONAL DO CINEMA - ANCINE, ou quem porventura tenha acesso a dados ou informações protegidos por essa Política.

3.CONCEITOS E DEFINIÇÕES

3.1.Ativo: qualquer coisa que tenha valor para a organização.

3.2.Ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso [1].

3.3.Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema [2].

3.4.Colaborador: todas as pessoas envolvidas com o desenvolvimento de atividades na organização, de caráter permanente, continuado ou eventual, incluindo prestadores de serviço, bolsistas, consultores e estagiários.

3.5.Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado [3].

3.6.Dado: qualquer elemento identificado em sua forma bruta que, por si só, não conduz a uma compreensão de determinado fato ou situação.

3.7.Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [4].

3.8.Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

3.9.Incidente de segurança de informação: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

3.10.Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato [5].

3.11.Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo [6].

3.12.Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [7].

3.13.Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal (APF) mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes [8].

3.14.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 [9].

3.15.Plano de Recuperação de Negócios: documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas à normalidade [10].

3.16.Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações [11].

3.17.Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações [12].

3.18.Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [13].

3.19.Servidor: pessoa legalmente investida em cargo público [14].

3.20.Sistema de Informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção.

3.21.Sistema de Segurança da Informação: sistema destinado à proteção contra a quebra de confidencialidade, de integridade ou de disponibilidade de dados ou informações, armazenados, em processamento ou em trânsito, podendo abranger a segurança dos recursos humanos, da documentação e do material, das áreas e instalações de comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

3.22.Tratamento da Informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas [15].

3.23.Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade.

4.REFERÊNCIAS LEGAIS E NORMATIVAS

4.1.Lei nº. 12.527, de 18 de novembro de 2011, que regula o acesso à informação (Lei de Acesso à Informação).

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

4.3.Decreto nº3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

4.4.Decreto nº. 7.724, de 16 de maio de 2012, que regulamenta a Lei nº. 12.527, de 18 de novembro de 2011.

4.5.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, e dá outras providências.

4.6.Normas Complementares DSIC/GSI/PR nº. 1 à nº 20.

4.7.Resolução de Diretoria Colegiada ANCINE nº. 57, de 09 de outubro de 2013.

4.8.Norma ABNT NBR ISO/IEC 16167:2013 - Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação.

4.9.Norma ABNT NBR ISO/IEC 27000 - Tecnologia da Informação - Técnicas de Segurança.

4.10.Norma ABNT NBR ISO/IEC 22301:2013 - Segurança da Sociedade - Sistema de gestão de continuidade de negócios - Requisitos.

4.11.Norma ABNT NBR ISO/IEC 27001:2013 - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos.

4.12.Norma ABNT NBR ISO/IEC 27005:2011, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação.

5.PRINCÍPIOS

A Política de Segurança da Informação e Comunicações da AGÊNCIA NACIONAL DO CINEMA - ANCINE é guiada pelos seguintes princípios:

5.1.Responsabilidade: as responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.

5.2.Conhecimento: para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários.

5.3.Ética: todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados ao prover um sistema de informação e ao estabelecer um sistema de segurança.

5.4.Legalidade: os processos de segurança devem levar em consideração os objetivos e a missão da AGÊNCIA NACIONAL DO CINEMA - ANCINE; bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais.

5.5.Proporcionalidade: o nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos sistemas de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.

5.6.Integração: os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente.

5.7.Celeridade: as ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível.

5.8.Revisão: os sistemas de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo.

5.9.Liberdade: um sistema de segurança da informação deve ser compatível com o legítimo uso e fluxo de informações/dados devendo ser observadas as normas de privacidade e de direito de realização de auditorias.

6.DIRETRIZES

São diretrizes da Política de Segurança da Informação e Comunicações da

ANCINE:

6.1.Tratamento da Informação

O tratamento da informação será regido por norma complementar, e devem ser estabelecidos procedimentos que abranjam as informações em quaisquer formatos. Deve-se assegurar a toda informação, produzida ou sob custódia da ANCINE, a proteção durante todo seu ciclo de vida.

6.2.Segurança em Recursos Humanos

Servidores e colaboradores da ANCINE devem ser treinados e capacitados, desde a fase de admissão, nos procedimentos e no uso correto das informações e ativos sob sua responsabilidade, a fim de minimizar possíveis riscos de segurança.

A ANCINE deve capacitar seus servidores em matéria de Segurança da Informação e Comunicações.

6.3.Auditoria e Conformidade

Deve-se proceder ao exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação e comunicações com as legislações e normas vigentes. A análise de conformidade em segurança da informação e comunicações deve ser efetuada criticamente, em intervalos regulares.

As normas e procedimentos complementares de Auditoria e Conformidade devem ser especificados de acordo com requisitos legais, observando-se a prevenção contra uso indevido de recursos de processamento da informação, monitoramento de uso e política de acesso.

6.4.Gestão de Riscos

A ANCINE deve estabelecer o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC. Esse processo deve abordar: a definição do contexto para identificação dos riscos; a análise e avaliação dos riscos; o tratamento, aceitação e comunicação às partes interessadas; além da realização contínua do monitoramento e da análise crítica dos riscos.

O processo de GRSIC deve considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e o Regimento Interno da Agência, além de estar alinhado à Política de Segurança da Informação e Comunicações.

O escopo, as diretrizes e a metodologia do processo da Gestão de Riscos de Segurança da Informação e Comunicações serão estabelecidos em norma complementar.

6.5.Tratamento de Incidentes

É dever dos servidores e colaboradores da ANCINE reportar imediatamente eventos ou incidentes de segurança da informação à Equipe de Tratamento de Resposta a Incidentes em Redes Computacionais (ETIR). Os incidentes de segurança devem ser registrados, avaliados e tratados.

A ANCINE deve estabelecer contato com autoridades legais, organismos reguladores, e provedores de serviço de informação, a fim de garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança da informação. Também deve ser providenciada a filiação a grupos de segurança da informação e a fóruns setoriais. Nas trocas de informações, deve-se observar a restrição de acesso a informações sigilosas.

6.6.Controle de Acesso

O acesso aos ambientes físicos e computacionais da ANCINE deve ser controlado e concedido somente a pessoas identificadas e autorizadas. As autorizações de acesso devem ser concedidas com base na necessidade do conhecimento da informação, condição inerente ao efetivo exercício de cargo, função ou atividade.

O acesso a informações e recursos de Tecnologia da Informação será provido via perfis de trabalho, ou por solicitação especial ao Gestor de Segurança da Informação e Comunicações.

O acesso de colaboradores à informação e aos recursos de processamento da informação não deve ser permitido até que os controles sejam implementados e o contrato que define os termos para a conexão ou acesso seja assinado. Esta política deve ser observada no que concerne à assinatura de tais contratos e na contratação externa para processamento da informação.

6.7.Acesso à Intranet, Internet e Uso de Mensageria

As comunicações por meio eletrônico, o armazenamento de mensagens, ou qualquer informação produzida no ambiente corporativo, são de propriedade da ANCINE, e seu conteúdo deve ter tratamento adequado à preservação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade das informações.

Os serviços corporativos de correio eletrônico, mensagens instantâneas, Intranet e Internet devem ter seu uso orientado para o interesse da ANCINE.

O uso dos serviços de Internet e mensageria devem estar em conformidade com perfis funcionais definidos em norma e procedimento complementar.

6.8.Desenvolvimento Seguro de Sistemas

Os processos de desenvolvimento de Sistemas de Informação devem observar as melhores práticas e padrões de desenvolvimento seguro visando à Gestão de Riscos de Segurança da Informação e Comunicações.

6.9.Gestão da Continuidade de Negócios em Segurança da Informação e Comunicações

A ANCINE deve desenvolver o Programa de Gestão da Continuidade de Negócios. O Programa deve buscar minimizar os impactos decorrentes de incidentes de Segurança da Informação e Comunicações sobre as atividades da Agência, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

O Programa de Gestão da Continuidade de Negócios envolve a elaboração do Plano de Gerenciamento de Incidentes, do Plano de Continuidade de Negócios e do Plano de Recuperação de Negócios, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas [16].

7.COMPETÊNCIAS E RESPONSABILIDADES

7.1.Gerenciamento da Segurança da Informação

O controle, a implementação e a manutenção da Segurança da Informação e Comunicações são de responsabilidade da seguinte infraestrutura de gerenciamento:

a)Autoridade máxima: responsável pela aprovação da Política de Segurança da Informação.

b)Agente responsável: servidor público ocupante de cargo efetivo, formalmente designado, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR [17].

c)Comitê de Segurança da Informação e Comunicações (CSIC): grupo de pessoas com a responsabilidade de assessorar a implementação das atividades de Segurança da Informação e Comunicações no âmbito da ANCINE [18].

d)Gestor de Segurança da Informação e Comunicações: responsável pelas ações de Segurança da Informação e Comunicações [19].

e)Equipe de Tratamento de Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes computacionais [20]. A equipe será criada por norma complementar e terá como missão prioritária a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais.

7.2.Atribuição da Responsabilidade em Segurança da Informação

As responsabilidades pela proteção das informações, dos ativos de informação e cumprimento das normas de Segurança da Informação e Comunicações devem ser definidas em normas específicas. Na atribuição das responsabilidades, deve-se observar o mapeamento e inventário dos ativos de informação.

8.PENALIDADES

Os recursos de Tecnologia da Informação e Comunicações são de propriedade da AGÊNCIA NACIONAL DO CINEMA - ANCINE e fornecidos para uso corporativo, para os fins a que se destinam, e no interesse da administração.

É considerada imprópria a utilização destes recursos, assim como das informações de propriedade da ANCINE, para fins não profissionais ou não autorizados. Quando do conhecimento desta prática, servidores e colaboradores devem informá-la ao superior imediato, para que sejam aplicadas as ações disciplinares cabíveis.

A violação das normas de Segurança da Informação e Comunicações pode ensejar a suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais, e será apurada em processo administrativo disciplinar, podendo haver responsabilização penal, civil e administrativa, na forma da legislação em vigor.

Os casos omissos desta política serão tratados pelo Comitê de Segurança da Informação e Comunicações.

9.ATUALIZAÇÃO

A POSIC e todos os instrumentos normativos dela derivados devem ser revisados sempre que necessário, não excedendo o período máximo de 36 (trinta e seis) meses.

As alterações serão propostas pelo Comitê de Segurança da Informação e Comunicações, conforme o artigo 3º, I, da Resolução de Diretoria Colegiada ANCINE nº 57, de 09 de outubro de 2013.

10.DISPOSIÇÕES FINAIS

As diretrizes de Segurança da Informação e Comunicações estabelecidas neste documento são aplicáveis às informações produzidas ou sob guarda da ANCINE, armazenadas ou em trânsito, e devem ser seguidas por todos os servidores e colaboradores, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

As matérias relativas à Segurança da Informação e Comunicações serão disciplinadas por normas complementares.

[1]DSIC/GSIPR. NC 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012.

[2]Lei nº 12.527, de 18 de novembro de 2011.

[3]Instrução Normativa GSI/PR nº. 1, de 13 de junho de 2008.

[4]Instrução Normativa GSI/PR nº. 1, de 13 de junho de 2008.

[5]Lei nº 12.527, de 18 de novembro de 2011.

[6]Decreto nº 7.724, de 16 de maio de 2012.

[7]Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

[8]DSIC/GSIPR. NC 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009.

SIC/GSIPR. NC 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009.

[10]DSIC/GSIPR. NC 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009.

[11]Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

[12]Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

[13]Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

[14]Lei nº. 8.112, de 11 de novembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

[15]Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

[16]DSIC/GSIPR. NC 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009.

[17]DSIC/GSIPR. NC 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

[18]O CSIC foi criado pela Resolução de Diretoria Colegiada ANCINE nº 57, de 09 de outubro de 2013.

[19]A função de Gestor de Segurança da Informação e Comunicações foi instituída pela Resolução de Diretoria Colegiada ANCINE nº 57, de 09 de outubro de 2013.

[20]DSIC/GSIPR. NC 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.