PORTARIA IN/SG/PR Nº 31, DE 29 DE ABRIL DE 2021

Institui, no âmbito da Imprensa Nacional, a Política de Segurança da Informação e Comunicações POSIC/IN.

O DIRETOR-GERAL DA IMPRENSA NACIONAL, no uso das atribuições que lhe confere o art. 1º da Portaria nº 14, de 17 de março de 2021, do Ministro de Estado Chefe da Secretaria-Geral da Presidência da República, com fundamento no art. 17 do Decreto nº 9.215, de 29 de novembro de 2017, resolve:

Considerando as diretrizes do Governo Federal, representado pelo Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre as orientações para gestão de segurança da informação que deverão ser observadas e implementadas pelos órgãos e pelas entidades da administração pública federal, direta e indireta, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional, conforme preconiza a Instrução Normativa - IN nº 01/DSIC/GSI/PR, de 27 de maio de 2020;

Considerando o advento da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, alterada pela Lei nº 14.129, de 29 de março de 2021;

Considerando as boas práticas em segurança preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2010, 27005:2011 e 27014:2013;

Considerando que a norma ABNT NBR ISO/IEC 27002:2013 recomenda revisões periódicas da política de segurança da informação das instituições;

Considerando a necessidade de estabelecer os direcionamentos e os valores adotados para a gestão de segurança da informação e comunicações no âmbito da Imprensa Nacional;

Considerando a importância que deve ser dada à garantia da integridade, à disponibilidade, à confidencialidade e à autenticidade dos dados e das informações utilizados na Imprensa Nacional;

Considerando o Acórdão nº 1.233 -TCU/2012, que trata da adoção dos normativos de Segurança da Informação e Comunicações (SIC), não facultativos, mas obrigação da alta administ ração, Acórdão nº 3.051-TCU/2014, que prevê a estratégia geral de Segurança da Informação, e Acórdão nº 1.033/2009 – TCU –Plenário; e

Considerando a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais –LGPD), que dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014 (Marco Civil da Internet), resolve:

Art. 1º Aprovar e instituir, no âmbito da Imprensa Nacional, a Política de Segurança da Informação e Comunicações POSIC/IN, na forma do Anexo a esta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação, ficando revogada a Portaria nº 95, de 28 de fevereiro de 2019, publicada no Boletim de Serviço nº 24, de 1° de março de 2019.

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – POSIC/IN

CAPÍTULO I

OBJETIVO

1.1. Estabelecer diretrizes, critérios e procedimentos para institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) na Imprensa Nacional.

CAPÍTULO II

ABRANGÊNCIA

2.1. A Política de Segurança da Informação e Comunicações declara o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações na Imprensa Nacional;

2.2. As diretrizes constantes na Política de Segurança da Informação e Comunicações no âmbito da Imprensa Nacional visam assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas, transmitidas ou processadas nos meios tecnológicos da Imprensa Nacional, assim como proteger a imagem institucional da Imprensa Nacional decorrente de incidente de segurança da informação.

2.2.1 Parágrafo único. A Imprensa Nacional, no exercício de suas competências legais, recebe, editora, armazena e dá publicidade a informações de órgãos e entidades da administração pública federal, das esferas estadual e municipal e de entidades privadas. As referidas informações são consideradas sigilosas até a respectiva publicação no Diário Oficial da União, conforme art. 19 da Portaria nº 147/2006 da Casa Civil da Presidência da República.

CAPÍTULO III

FUNDAMENTOS LEGAIS

3.1. Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.2 Para o planejamento da gestão da segurança da informação, cabe aos órgãos e às entidades da administração pública federal observar, sem prejuízo das demais normas em vigor:

3.2.1 A Instrução Normativa nº. 01, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal.

3.2.2 O Decreto nº 10.641, de 02 de março de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação - PNSI;

3.2.3 O Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; e

3.2.4 As instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO IV

CONCEITOS E DEFINIÇÕES

4.1. Para os efeitos desta POSIC e em atendimento à Portaria GSI/PR No. 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação, estão estabelecidos os seguintes conceitos e definições:

4.2. **Ativo**: é tudo aquilo que tenha valor (tangível ou intangível) e que dá suporte à missão e visão da instituição, tais como: pessoas, informações, programas de computador, equipamentos, instalações, serviços e imagem institucional.

4.3. **Autenticação**: processo que busca verificar a identidade digital de uma entidade de um sistema quando ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

4.4. **Autenticidade**: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

4.5. **Ciclo de Vida da Informação**: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua confidencialidade, integridade e disponibilidade.

4.6. **Classificação da Informação**: atribuição, pela autoridade competente, de grau de sigilo, disponibilidade e integridade dado a informação, documento, material, área ou instalação.

4.7. **Comitê Gestor de Segurança da Informação e Comunicações**: grupo de pessoas com nível hierárquico, convidados para participar de deliberações conjuntas das ações de Segurança da Informação e Comunicações no âmbito da Imprensa nacional, e submissão para aprovação da alta gestão. O Comitê deve ser composto de, ao mínimo, 01 (um) representante da área de Tecnologia da Informação e Comunicação, e da ETIR.

4.8. **Confidencialidade**: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidades não autorizadas nem credenciadas;

4.9. **Conta de Serviço**: conta de acesso a recursos computacionais necessários a um procedimento automático (aplicação, script etc.) sem qualquer intervenção humana no seu uso.

4.11. **Credenciais ou Contas de Acesso**: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão ou lógica como identificação de usuário e senha.

4.12. **Controle de Acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

4.13. **Controle de Acesso Lógico**: é o conjunto de regras definidas que norteiam a concessão de acesso a sistemas de informação e recursos computacionais.

4.14. **Criticidade**: grau de importância da informação para continuidade das atividades e serviços da Imprensa Nacional.

4.15. **Custodiante**: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia.

4.15.1 **Custodiante da Informação**: qualquer indivíduo ou estrutura de órgão ou entidade da APF, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de SI comunicadas pelo proprietário da informação

4.16. **Descarte**: eliminação correta de informações, documentos, mídias e acervos digitais.

4.17. **Disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

4.18. **Equipe de Tratamento e Resposta a Incidentes em Infraestrutura e Segurança da Informação (ETIR)**: grupo de pessoas com a responsabilidade de receber, analisar e responder a incidentes de infraestrutura e segurança da informação, atividades relacionadas à Segurança da Informação e Comunicações produzidas por terceiros e/ou pela Imprensa Nacional.

4.19. **Gestão de Risco**: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

4.20. **Gestão de Segurança da Informação e Comunicações**: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

4.21. **Gestor de Segurança da Informação e das Comunicações**: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

4.22. **Incidente**: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

4.22.1 **Incidente de Segurança**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

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

4.24. **Informação Custodiada**: informação sob a guarda e responsabilidade da Imprensa Nacional.

4.25. **Integridade**: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.26. **Plano de Contingência**: descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim a paralisação prolongada.

4.27. **Plano de Continuidade de Negócios (PCN)**: documentação de procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em caso de incidentes.

4.28. **Política de Segurança da Informação e das Comunicações (POSIC)**: documento aprovado pela autoridade responsável pelo órgão ou entidades da APF, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações.

4.29. **Quebra de Segurança**: é a ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e Comunicações.

4.30. **Segurança da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações produzidas e custodiadas pela Imprensa Nacional.

4.31. **Sistema de Gestão da Segurança da Informação (SGSI)**: É o sistema de gestão adotado pela corporação para a Segurança da Informação, o qual inclui toda a abordagem organizacional usada para proteger a informação e seus critérios de Confidencialidade, Integridade e Disponibilidade.

4.32. **Usuário Colaborador:** Compreendem a força de trabalho da organização com vínculo efetivo com a Administração Pública (ex. servidores e empregados concursados, inclusive requisitados) e a força de trabalho contratada com base no art. 37, IX, da Constituição Federal que não exercem função de gestão de pessoas. Exclui-se então gestores, estagiários, terceirizados e outras pessoas que não se enquadram nesse conceito.

4.33. **Usuário Externo**: é qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a recursos computacionais, aos sistemas de informação ou às informações produzidas ou custodiadas pela Imprensa Nacional, e que não seja caracterizado como usuário interno, usuário colaborador e usuário visitante.

4.34. **Usuário Interno**: é qualquer servidor ou empregado público alocado na Imprensa Nacional que tenha acesso, de forma autorizada, a recursos computacionais, aos sistemas de informação ou às informações produzidas ou custodiadas pela Imprensa Nacional.

4.35. **Usuário Terceirizado**: prestador de serviço terceirizado, consultor externo, estagiário, contratado temporário, menor aprendiz e participante de grupos deliberativos esporádicos, de empresas formalmente contratada, que possam fazer uso dos recursos ou acessem informações e sistemas informacionais da Imprensa Nacional.

4.36. **Usuário Visitante**: é qualquer pessoa física que tenha acesso precário, de forma autorizada, na forma definida em norma complementar.

4.37. **Termo de Responsabilidade:** Termo assinado pelo usuário concordando em contribuir com a confidencialidade, integridade, disponibilidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso; e

4.38. **Vulnerabilidade**: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO V

COMPETÊNCIAS E RESPONSABILIDADES

5.1. Compete à Imprensa Nacional, em seu âmbito de atuação:

I - Designar um Gestor de Segurança da Informação interno, indicado pela alta administração do órgão ou da entidade;

II - Instituir Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação - PNSI;

CAPÍTULO VI

DIRETRIZES GERAIS

6.1. Acesso à Internet

6.1.1. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Imprensa Nacional, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

6.1.2. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Imprensa Nacional, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta POSIC.

6.2. **Auditoria e Conformidade**

6.2.1. Estão criados e instituídos controles apropriados, trilha de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Imprensa Nacional julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, nos acessos à internet, no correio eletrônico, nos sistemas desenvolvidos pela Imprensa Nacional ou por Terceiros.

6.3. Classificação da Informação

6.3.1. O processo de classificação da informação tem por objetivo assegurar que a informação receba o nível adequado de proteção de acordo com a sua importância para Imprensa Nacional.

6.3.2. As informações são classificadas em termo do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

6.3.2.1. O processo de classificação está descrito na norma complementar de Classificação da Informação.

6.4. Controles de Acesso

6.4.1. Os dispositivos de identificação e senhas protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Imprensa Nacional e/ou terceiros.

6.4.2. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

6.4.3. Tal norma visa estabelecer critérios de responsabilidades sobre o controle de acesso e é aplicada a todos os usuários.

6.4.4. Todos os dispositivos de identificação utilizados na Imprensa Nacional, como o número de registro do usuário, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos estão associados a uma pessoa física e vinculados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

6.4.5. O usuário, que está vinculado a esses dispositivos, é responsável pelo seu uso correto perante a Imprensa Nacional e a legislação vigente, e não poderá compartilhar com outros usuários sob qualquer hipótese, respondendo de forma cível e criminal pelo uso incorreto.

6.5. Controle dos Ativos de Informação

6.5.1. A gestão dos ativos de informação assegura que esses ativos:

6.5.1.1. São inventariados e protegidos;

6.5.1.2. Tem entrada e saída nas dependências da Imprensa Nacional autorizadas e registradas por autoridade competente;

6.5.1.3. São passíveis de monitoramento, garantindo a rastreabilidade do seu uso;

6.5.1.4. Têm identificados os seus custodiantes responsáveis;

6.5.1.5. São utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins, observando a legislação em vigor; e

6.5.1.6. Quando se tratar de dispositivos portáteis, tem registrada sua cessão.

6.5.2. Ocorrências como extravio ou roubo devem ser imediatamente comunicadas ao superior imediato para que sejam registradas como incidente de segurança da informação, sem prejuízo das demais providências necessárias.

6.6. Correio Eletrônico

6.6.1. O objetivo desta norma é informar aos colaboradores da Imprensa Nacional quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico do órgão.

6.6.2. O uso do correio eletrônico da Imprensa Nacional é para fins corporativos e relacionados às atividades do colaborador usuário dentro do órgão. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudicando a Imprensa Nacional e não causando impacto no tráfego da rede e esteja, sempre, apoiado na ciência e autorização do coordenador imediato.

6.7. Gestão de Continuidade

6.7.1. A Imprensa Nacional mantém processo de gestão de continuidade das atividades e processos críticos, visando não permitir que sejam interrompidos e assegurar a sua retomada em tempo hábil.

6.7.2. Um Plano de Contingência e a continuidade dos principais sistemas e serviços estão implantados e é testado no mínimo a cada seis meses, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

6.8. Gestão de Risco

6.8.1. A gestão de Riscos de Segurança da Informação e das Comunicações é realizada de forma sistemática e contínua e engloba ativos de informação da Imprensa Nacional, visando tratar riscos relacionados a disponibilidade, integridade, confidencialidade e autenticidade.

6.8.2. Aplicam-se à Segurança da Informação e das Comunicações, no que couber, os princípios e diretrizes de Gestão de Riscos definidos pela Política de Gestão de Riscos de TIC da Imprensa Nacional.

6.8.3. A Gestão de Riscos de Segurança da Informação e das Comunicações é operacionalizada por meio de Metodologia específica.

6.8.4. Compete ao Comitê Gestor de Segurança da Informação a definição da periodicidade máxima para a execução dos processos de Gestão de Riscos de Segurança da Informação e das Comunicações.

6.8.5. Compete a cada servidor da Imprensa Nacional o monitoramento da evolução dos níveis de riscos e da efetividade das medidas de tratamento de riscos de Segurança da Informação e Comunicações, no que compete a sua atribuição atual.

6.9. Relação com Terceiros

6.9.1. Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadores de serviços para Imprensa Nacional, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC/IN.

6.9.2. A Imprensa Nacional identifica e exige controles de segurança da informação para tratar, especificamente, do acesso do fornecedor às informações da organização.

6.10. Segurança em Gestão de Pessoas

6.10.1. O Gestor de Segurança da Informação é responsável por propor ações de divulgação e conscientização de agente públicos, colaboradores e visitantes com acesso à Imprensa Nacional ou aos seus ativos de informação, que abordem os princípios, diretrizes, procedimentos e responsabilidades relacionados à Segurança da Informação e das Comunicações.

6.10.2. Qualquer agente público ou usuário pode propor ações de divulgação e conscientização, as quais serão apreciadas pelo Gestor de Segurança da Informação e Comunicações.

6.10.3. O Gestor de Segurança da Informação Comunicações é responsável por propor atividades de capacitação, de divulgação e de disseminação das orientações previstas nesta POSIC aos agentes públicos e colaboradores.

6.10.4. Agentes públicos e colaboradores devem possuir ciência dos riscos de SI em processos que executam, das informações que acessam e processam em suas responsabilidades.

6.10.5. O ingresso, a movimentação e o desligamento dos agentes públicos e colaboradores, bem como o encerramento de contratos, são realizados de modo controlado, garantindo:

6.10.5.1. A devolução de todos os ativos de informação;

6.10.5.2. O cancelamento de autorizações de acesso às informações classificadas; e

6.10.5.3. A entrega de compromisso assinado de não divulgação de informações sigilosas.

6.11. Segurança Física das Instalações de TI

6.11.1. A segurança física e patrimonial, disposta em normativo específico tem por objetivo, em relação à segurança da informação, prevenir danos e interferências nas instalações da Imprensa Nacional que possam causar perda, roubo ou comprometimento das informações, em consonância com a Política de Gestão de Riscos da Imprensa Nacional.

6.11.2. Está assegurada a salvaguarda das instalações e dos demais ativos de informação em que são elaborados, tratados, custodiados, manuseados ou guardados dados e informações críticas ou sensíveis, independentemente do meio em que estão armazenados.

6.11.3. O ingresso de visitantes deve ser controlado de forma a impedir o seu acesso às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados, com autorização do responsável.

6.11.4. Todas as pessoas que tiverem acesso às instalações físicas portam identificação visível e, quando necessário, nível de autorização de acesso.

6.12. Segurança Lógica

6.12.1. A sistematização de controle de acesso à informação, detalhada em norma complementar, tem por objetivo garantir que o acesso à informação e aos ativos que armazenam esteja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

6.12.2. O acesso aos computadores, à rede corporativa e aos serviços oferecidos depende de prévia autenticação.

6.12.3. O acesso a qualquer informação veiculada eletronicamente é passível de monitoramento com vistas a garantir a rastreabilidade e a auditoria das ações realizadas.

6.12.4. A utilização dos meios de comunicação, inclusive o uso de dispositivos móveis, backup, Data Center, bem como as responsabilidades dos usuários no tocante às informações em trânsito são tratados em norma específica.

6.13. Tratamento da Informação

6.13.1. Toda informação produzida, recebida ou custodiada pelo agente público, no exercício de suas atividades para a Imprensa Nacional, é considerada um ativo e deve ser protegida pela organização de acordo com as regulamentações de segurança existentes, tendo o seu custodiante as seguintes responsabilidades:

6.13.1.1. É princípio da norma, o usuário comunicar tempestivamente ao gestor da informação situações que comprometam a segurança das informações e comunicações sob custódia;

6.13.1.2. As informações são protegidas de acordo com as diretrizes descritas nesta POSIC/IN e demais regulamentações em vigor, com o objetivo de minimizar riscos de segurança da informação às atividades e serviços da Imprensa Nacional e preservar sua imagem.

6.13.1.3. O acesso às informações produzidas ou custodiadas pela Imprensa Nacional que não sejam de domínio público é limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários (Colaborador, Externo, Interno e Terceirizado).

6.13.1.4. Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários internos ou usuários colaboradores necessita de prévia autorização formal.

6.13.1.5. O acesso a informações produzidas ou custodiadas pela Imprensa Nacional que não sejam de domínio público é definido pela norma complementar de Classificação da Informação.

6.13.1.6. As informações produzidas por usuários definidos nesta política, no exercício de suas funções, são patrimônio intelectual da Imprensa Nacional e não cabe a seus criadores qualquer forma de direito autoral.

6.13.1.7. Quando as informações são produzidas por esses usuários para uso exclusivo da Imprensa Nacional, instrumento próprio obriga os criadores ao sigilo permanente do conteúdo.

6.13.1.8. É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pela Imprensa Nacional, salvo autorização específica da Diretoria-Geral, nos processos e documentos de sua competência.

6.13.1.9. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela Imprensa Nacional observam, no que cabe, as cláusulas definidas nesta POSIC/IN.

6.14. Tratamento de Incidentes de Rede

6.14.1. A unidade responsável pela segurança da informação e comunicações, conforme definição do Regimento Interno, mantém a Equipe de Tratamento e Resposta a Incidentes em segurança da informação e infraestrutura tecnológica – ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança da informação e infraestrutura tecnológica.

CAPÍTULO VII

CONFORMIDADE

7.1. **Institucionalização da POSIC**

7.1.1 Para a institucionalização da POSIC na Imprensa Nacional, são recomendadas as seguintes ações:

7.1.2. Implementar a POSIC através da formalização e da aprovação por parte da autoridade máxima responsável pela Imprensa Nacional, demonstrando a todos os servidores e usuários o seu comprometimento.

7.1.3. Garantir a provisão dos recursos necessários para implementação da POSIC por parte da Imprensa Nacional.

7.1.4. Promover na Imprensa Nacional, a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.

7.1.5. A POSIC também tem por objetivo a implementação do SGSI da Imprensa Nacional em conformidade com a norma ABNT NBR ISO/IEC 27001:2013.

7.2. **Comunicação da Política**

7.2.1. A POSIC e suas atualizações devem ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham na Imprensa Nacional.

7.3**. Suporte para Implementação do SGSI**

7.3**.**1. O Comitê Gestor de Segurança da Informação declara que a implementação do SGSI e seu contínuo aprimoramento serão suportados pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como atender todos os requisitos identificados.

7.4. **Validade e Gestão de Documentos**

7.4.1. A presente política aprovada é mantida sob a gestão documental da área de tecnologia da informação da Imprensa Nacional.

7.4.2. O Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da Imprensa Nacional, é responsável pela elaboração deste documento, o analisa criticamente, e, se necessário, atualiza a POSIC a cada 01 (um) ano.

7.4.3. Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios dever ser considerados:

7.4.3.1. Quantidade de usuários e terceiros que têm um papel no SGSI, mas não conhecem este documento;

7.4.3.2. Não conformidade do SGSI com as leis e as regulamentações, obrigações contratuais e outros documentos internos da organização; e

7.4.3.3. Ineficácia da manutenção e da implementação do SGSI.

CAPÍTULO VIII

AUDITORIA E PENALIDADES

8.1. Conforme art. 14 do Decreto nº 10.641, de 2 de março de 2021, compete à Controladoria-Geral da União auditar a execução das ações desta POSIC.

8.2. Quaisquer usuários com ações suspeitas e passíveis de violação desta Política e documentos relacionados poderão ter suspensos os privilégios de acesso aos recursos computacionais da Imprensa Nacional temporariamente, sem aviso prévio, até que a investigação seja encerrada;

8.3. Toda ação que comprovadamente viole esta Política e documentos relacionados, ou que infrinjam quaisquer controles de segurança da informação, será passível de penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

ANEXO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA ACESSO ÀS SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO DA IMPRENSA NACIONAL

1. Declaro-me ciente das normas e regras que disciplinam a utilização de soluções e recursos de Tecnologia da Informação (TI) colocados à minha disposição para exercício de atividades no âmbito da Imprensa Nacional, nos termos definidos na Política de Segurança da Informação e Comunicações (POSIC/Imprensa Nacional) e suas normas de segurança específicas, cujas cópias encontram-se disponíveis em repositório eletrônico de meu conhecimento, bem assim que:

1.1. As senhas vinculadas ao meu código de usuário, destinadas ao acesso às soluções da Imprensa Nacional, são de meu uso pessoal e intransferíveis, sendo meu dever zelar pela sua proteção e pelo seu sigilo;

1.2. Devo cumprir as normas e regras para utilização dos recursos e soluções de TI fornecidos pela Imprensa Nacional, assim como respeitar a legislação aplicável em todo acesso obtido por meio do meu código de usuário e da senha a ele vinculada, inclusive nos casos em que o acesso seja realizado a partir de equipamentos e canais de comunicação não pertencentes à Imprensa Nacional;

1.3. Constitui infração o uso indevido ou fraudulento de recursos e soluções de TI da Imprensa Nacional, bem como a divulgação de dados e informações da instituição classificados como sigilosos ou a sua utilização para quaisquer outros fins que estejam em desacordo com o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, com o Código de Ética dos Servidores da Imprensa Nacional ou com a POSIC/Imprensa Nacional e suas normas de segurança específicas, sujeitando-me às penalidades administrativas, civis e penais decorrentes;

1.4. Por se tratar de recursos corporativos a serem usados de modo compatível com o exercício do cargo e sem comprometer a segurança da informação, as soluções de TI colocadas à minha disposição estão sujeitas a monitoramento pela Imprensa Nacional, inclusive no que se refere ao conteúdo de arquivos e mensagens de correio eletrônico;

1.5. A utilização das soluções de TI da Imprensa Nacional não se constituem um direito do usuário, mas sim uma concessão, e desta forma a Imprensa Nacional resguarda o direito de suspender o meu acesso, de forma justificada, a sistemas de informação, correio eletrônico, internet e outras soluções e recursos de TI a qualquer momento, ainda que sem prévia comunicação;

1.6. A ETIR/IN (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da Imprensa Nacional) poderá bloquear, temporariamente, sem aviso prévio, o acesso individual ou coletivo às soluções de TI, a fim de coletar evidências ou minimizar os riscos à segurança da informação e comunicações.

2. Declaro-me ciente, ainda, que devo notificar à ETIR/IN por meio da caixa corporativa etir@in.gov.br, a respeito de suspeitas de infração de SI, os incidentes que afetem a segurança da informação e comunicações e o descumprimento das regras previstas na POSIC/Imprensa Nacional e suas normas de segurança específicas.

<<No caso de servidor: Nome e SIAPE>>

<<No caso de profissional terceirizado: Nome e CPF do preposto da empresa>>

<<No caso de estagiário: Nome e SIAPE do Gestor Direto >>

<<No caso de estagiário menor: Nome e CPF do responsável legal >>