POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO - PO 900-01

SUMÁRIO

1. FINALIDADE

1.1 Instituir diretrizes, critérios e regras de segurança da informação e da comunicação no âmbito da Empresa Brasil de Comunicação S.A. - EBC.

2. CONCEITUAÇÃO

2.1 AMEAÇA

Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a EBC.

2.2 ATIVOS DE INFORMAÇÃO

Meios de armazenamento, transmissão e processamento de informação, os sistemas de informação, bem como os locais onde se encontram esses meios, as pessoas que a eles têm acesso, a imagem institucional, os serviços e tudo aquilo que tem valor para a EBC e que esteja relacionado com a informação e da Comunicação.

2.3 COMPUTAÇÃO EM NUVEM

Modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação, rede de computadores, servidores, processamento, armazenamento, aplicativos e serviços, provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

2.4 CONTROLE DE ACESSO

Permissões concedidas por autoridade competente da EBC após o processo de credenciamento, que habilitem determinada pessoa, sistema ou organização ao acesso mediante a assinatura ou não de termo de responsabilidade ou outro instrumento formal, podendo a credencial ser física, como crachá, cartão, *token*, selo ou lógica para identificação de usuários.

2.5 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, HD*s externos e cartões de memória.

2.6 GESTÃO DE CONTINUIDADE DE NEGÓCIOS

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.

2.7 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO

Conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de tecnologia da informação, de modo a assegurar, a um nível aceitável de risco, a eficiente utilização de recursos, apoio aos processos e alinhamento dos objetivos e estratégias, garantindo que o uso da Tecnologia da Informação e da Comunicação - TIC agregue valor ao negócio da organização.

2.8 INCIDENTE DE SEGURANÇA

Qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou a autenticidade de qualquer ativo de informação da EBC.

2.9 NORMAS INTERNAS COMPLEMENTARES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO:

Estabelece responsabilidades e procedimentos definidos de acordo com as diretrizes da POSIC.

2.10 PLANO DE GERENCIAMENTO DE INCIDENTES

Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra os principais ativos de informação que sejam necessários para implementar o processo de gerenciamento de incidentes.

2.11 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.

2.12 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO - POSIC

Define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e da Comunicação.

2.13 QUEBRA DE SEGURANÇA

Ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e da Comunicação - SIC da EBC.

2.14 REDES SOCIAIS

Estruturas sociais conectadas que permitem a troca, em geral não hierárquica, de informações, conteúdos, objetivos e valores.

2.15 RESILIÊNCIA

Poder de recuperação ou capacidade de enfrentamento ágil de situações inesperadas e de superação das adversidades para restabelecer o processo de normalidade da EBC e resistir aos efeitos de um incidente.

2.16 SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO - SIC

Ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação, abrangendo não só aspectos tecnológicos, mas também recursos humanos e processos.

2.17 TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO - TIC

Conjunto de todas as atividades e soluções providas por recursos de computação. Serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. Este termo é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação.

2.18 USUÁRIO

Empregados, agentes públicos, terceirizados, colaboradores, consultores, auditores, estagiários e pessoas que obtiveram acesso aos Ativos de Informação da EBC.

2.19 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 mitigados por uma ação interna de segurança da informação.

3. OBJETIVO

3.1 A Política de Segurança da Informação e da Comunicação – POSIC tem o propósito de direcionar a Empresa Brasil de Comunicação S.A – EBC no que diz respeito à gestão dos riscos e do tratamento dos incidentes de segurança da informação e da Comunicação - SIC.

3.2 Seu objetivo é instituir diretrizes estratégicas, responsabilidades e competências visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, documentos e conhecimentos de sua propriedade, ou sob sua guarda, produzidos, armazenados ou transmitidos, por qualquer meio dos sistemas de informação da EBC, fazendo a gestão dos riscos, ameaças e vulnerabilidades, adotando procedimentos e mecanismos, que visam a eliminação ou redução de ocorrência de modificações não autorizadas, bem como a disponibilidade de recursos e sistemas críticos para garantir a continuidade dos negócios da EBC, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de SIC, de modo a preservar os seus ativos, inclusive sua imagem institucional.

3.3 A POSIC estabelece o comprometimento da alta direção organizacional da EBC, com vistas a prover apoio para implantação da Gestão de Segurança da Informação e da Comunicação - GESIC, buscando um ambiente seguro que proporcione uma melhor qualidade nos processos de gestão e controle dos sistemas de informação e informática.

4. ABRANGÊNCIA E VIGÊNCIA

4.1 A POSIC se aplica a todas unidades, empregados, visitantes e colaboradores externos que prestem serviço em razão de qualquer tipo de instrumento firmado e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas.

4.2 A POSIC será revisada sempre que necessário, não excedendo o prazo máximo de três anos e sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

5. DIVULGAÇÃO E CONSCIENTIZAÇÃO

5.1 A divulgação das regras e orientações de segurança aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança dentro da EBC.

5.2 O Gestor de Segurança da Informação e da Comunicação - GESEG, com o apoio das áreas responsáveis pelos processos de comunicação interna, deverá providenciar a divulgação interna desta Política de Segurança da Informação e da Comunicação - POSIC e suas respectivas Normas Complementares, inclusive com publicação permanente na página da Intranet da EBC, para que seu conteúdo possa ser consultado a qualquer momento e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIC.

6. ATUALIZAÇÃO

6.1 A SIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

6.2 Os instrumentos normativos gerados a partir desta POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal, ou conforme os seguintes critérios:

I - Política de Segurança da Informação e da Comunicação - POSIC:

a) Nível de Aprovação: Conselho de Administração - CONSAD; e

b) Periodicidade de Revisão: a cada três anos, no máximo.

II - Normas Técnicas Complementares da Política de Segurança da Informação e da Comunicação - POSIC:

a) Nível de Aprovação: Comitê de Segurança da Informação e da Comunicação - COSIC; e

b) Periodicidade de Revisão: a cada três anos, no máximo.

7 COMPETÊNCIAS E RESPONSABILIDADES

7.1 Compete ao Conselho de Administração - CONSAD aprovar a Política de Segurança da Informação e da Comunicação – POSIC e suas alterações.

7.2 Compete à Diretoria Executiva aprovar as Normas Complementares da Política de Segurança da Informação e da Comunicação – POSIC;

7.3 Compete ao Comitê de Segurança da Informação e da Comunicação - COSIC:

I - implementar, acompanhar, avaliar e propor alterações da Política de Segurança da Informação e da Comunicação - POSIC da EBC e de suas normas complementares;

II - formular propostas normativas e procedimentos complementares à POSIC, politicas de segurança e medidas de adequação atinentes à Segurança da Informação e da Comunicação, que serão submetidas à Diretoria-Executiva para deliberação;

III – propor a adoção de ações de conscientização e capacitação de pessoal, visando difundir os conhecimentos e dar efetividade à POSIC;

IV – supervisionar as ações de SIC no âmbito da EBC;

V – solicitar às unidades da EBC informações e mapear as demandas relacionadas à Política de Segurança da Informação e da Comunicação;

VI – propor a adoção de medidas corretivas, as adequações normativas e procedimentais necessárias a prevenção de situações de vulnerabilidade à Segurança da Informação e da Comunicação;

VII - instituir Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

VIII – solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

IX – propor a nomeação do Gestor de Segurança da Informação e da Comunicação - GESEG;

X – propor o conhecimento das práticas mais modernas e adequadas afetas à segurança corporativa, bem como compartilhar informações sobre novas tecnologias, produtos, ameaças, vulnerabilidades, gerenciamento de risco,

políticas de segurança e outras atividades relativas à segurança corporativa com entes públicos e/ou privados;

XI – aprovar a classificação, reclassificação e desclassificação de informações quanto ao grau de sigilo e os prazos de restrição de acesso à informação no âmbito da EBC, para dar cumprimento à legislação que regula o acesso a informações.

XII – interagir com o Comitê de Tecnologia da Informação e da Comunicação – CTIC, buscando a melhor forma de conjugação de esforços sobre matérias de mútuo interesse;

XIII – criar Grupos Técnicos de Trabalho para análise e manifestação sobre temas específicos:

a) os Grupos Técnicos de Trabalho serão constituídos por meio de ato deliberativo do COSIC, na qual serão fixados os objetivos, prazos e as equipes responsáveis pelas realizações dos trabalhos.

b) os resultados dos trabalhos serão submetidos a análise do COSIC, o qual fará a supervisão e prestará o apoio necessário ao desenvolvimento das atividades dos Grupos.

XIV – solicitar apurações quando da suspeita de ocorrência de quebras de Segurança da Informação e da Comunicação;

XV - estruturar ações conjuntas com os colegiados, quando da necessidade.

XVI – aprovar seu Regimento Interno e suas alterações;

XVII – dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC;

XVIII - Aprovar as Normas Técnicas relativas à SIC.

7.4 Todos os projetos e ações relacionados à segurança da informação e da comunicação – SIC devem ser destacados com uma rubrica ou identificador específico.

7.5 Cabe ao Gestor de Segurança da Informação e da Comunicação - GESEG no âmbito da EBC:

I – assessorar o Comitê;

II - promover cultura de SIC;

III - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

IV - propor a alocação de recursos materiais e humanos necessários à realização de ações de SIC e a plena consecução da POSIC e suas normas complementares;

V - coordenar as ações da ETIR;

VI - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

VII - manter contato com o Departamento de Segurança da Informação e da Comunicação da Presidência da República - DSIC para o trato de assuntos relativos à SIC;

VIII – propor Normas Técnicas relativas à SIC;

IX – subsidiar os membros com informações do Comitê, estudos e dados técnicos referentes à matéria a ser apreciada; e

X – indicar representantes para participar de fóruns de debates com instituições que desenvolvam projetos de pesquisa ou estudos sobre segurança da informação e da comunicação.

7.6 Cabe ao titular da unidade:

I - comunicar, de imediato, todo incidente de SIC que ocorra no âmbito de suas atividades ao ETIR, e posteriormente o envio de relatório circunstanciado ao COSIC;

II - corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

III - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

IV - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

V - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

VI - realizar o tratamento e a classificação da informação, conforme norma complementar específica;

VII – providenciar a documentação formal relativa a cessão de informação da EBC a terceiros, observadas as restrições estabelecidas em norma complementar;

VIII - comunicar à ETIR os casos de quebra de segurança;

IX - manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores;

X - definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta POSIC; e

XI – designar, formalmente, um usuário dos ativos de informação, quando aplicável. A não designação pressupõe que o gestor é o próprio titular da unidade.

7.7 Cabe ao usuário:

I - manter a segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações;

II - conhecer e zelar pelo cumprimento desta Política de Segurança da Informação e da Comunicação e de suas normas técnicas complementares;

III - responsabilizar-se pelas ações de SIC, observando de forma específica as atribuições pertinentes a cada cargo e /ou função; e

IV – comunicar os incidentes que afetam a segurança dos ativos de informação e da comunicação ao titular da unidade.

7.8 Compete aos terceiros e fornecedores, conforme previsto em contrato:

I – tomar conhecimento desta POSIC;

II - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato, quando solicitado; e

III - fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

7.9 Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR:

I – facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II – promover a recuperação de sistemas;

III – agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações;

IV – avaliar condições de segurança de redes por meio de verificações de conformidade;

V – realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

VI – analisar ataques e intrusões na rede da EBC;

VII – executar as ações necessárias para tratar de quebras de segurança;

VIII - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

IX - cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

X - participar em fóruns, redes nacionais e internacionais relativos à SIC.

8 PRINCÍPIOS

8.1 As ações relacionadas com a SIC na EBC serão norteadas pelos seguintes princípios, assim definidos:

8.1.1 CELERIDADE: As ações de SIC devem oferecer respostas rápidas a incidentes e falhas de segurança.

8.1.2 CONHECIMENTO: Os usuários devem conhecer e respeitar a POSIC, NIC e demais regulamentações sobre SIC da EBC.

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

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

8.1.5 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 EBC.

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

8.1.7 PUBLICIDADE: Transparência no trato da informação, observados os critérios legais.

8.1.8 RESPONSABILIDADE: As responsabilidades primárias e finais pela segurança dos ativos da EBC e pelo cumprimento de processos de segurança devem ser claramente definidas.

9. DIRETRIZES DE SEGURANÇA

9.1 Esta POSIC define as diretrizes para a SIC da EBC e descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

9.2 As diretrizes da POSIC constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração das Normas Complementares da Política de Segurança da Informação e da Comunicação.

9.3 Deverão ser criados e mantidos os Plano de Gerenciamento de Incidentes e Plano de Recuperação de Desastres, formalizados e periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade.

9.4 Os sistemas, as informações e os serviços da EBC utilizados pelos usuários, no exercício de suas atividades, são de exclusiva propriedade da EBC, não podendo ser

interpretados como de uso pessoal e devem ser protegidos, segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

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

9.6 Os recursos de tecnologia da informação de propriedade da EBC são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração.

9.6.1 É considerada imprópria a utilização desses recursos para propósitos não profissionais ou não autorizados.

9.7 Os usuários, e os visitantes que tomarem conhecimento do disposto no subitem 9.6.1 devem levar o fato ao conhecimento do superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

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

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

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

9.11 Qualquer tipo de dúvida sobre a POSIC, Normas Complementares da Política de Segurança da Informação e da Comunicação e demais regulamentações de SIC deve ser imediatamente esclarecido com o Gestor de Segurança da Informação e da Comunicação.

10. DIRETRIZES GERAIS

10.1 GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO - GESIC

10.1.1 Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade do negócio.

10.1.2 As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido.

10.1.3 Os requisitos de SIC da EBC devem estar explicitamente citados em todos os termos de compromisso celebrados entre a EBC e terceiros.

10.2 GESTÃO DE ATIVOS

10.2.1 A gestão dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

10.2.2 Os ativos de informação da EBC deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de SIC e são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

10.2.3 Todos os ativos deverão ser classificados em termos de valor, requisitos legais, sensibilidade e criticidade para a Empresa.

10.2.4 O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação.

10.2.5 É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela EBC.

10.3 TRATAMENTO DA INFORMAÇÃO

10.3.1 A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços da EBC.

10.3.2 Os dados, as informações e os sistemas de informação da EBC devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

10.3.3 A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade, elaborando-se, para tanto, sistema de classificação da informação.

10.4 CLASSIFICAÇÃO DA INFORMAÇÃO

10.4.1 As informações criadas, armazenadas, manuseadas, transportadas ou descartadas na EBC deverão ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas e legislação específica em vigor.

10.4.2 Todo usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pela EBC e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

10.5 MATERIAL IMPRÓPRIO

10.5.1 É expressamente proibido o acesso, uso, guarda e encaminhamento de material não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios e recursos de comunicações disponibilizados pela EBC.

10.6 GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES - GETIR

10.6.1 A área de Tecnologia da Informação deverá criar e manter uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, instituída

pelo Comitê da Segurança da Informação e da Comunicação - COSIC, com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas à incidentes de segurança em redes de computadores.

10.6.2 Os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes específico, comunicados e registrados.

10.7 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO - GRSIC

10.7.1 A GRSIC é um conjunto de processos que permite identificar e implementar as medidas 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.

10.7.2 As áreas responsáveis por ativos de informação deverão implementar processo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIC.

10.7.3 A GRSIC deve ser realizada no âmbito da EBC, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades. Trata-se de um instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócio e um Plano de Gerenciamento de Incidentes.

10.7.4 O Plano de Continuidade de Negócio deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

10.7.5 O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

10.8 GESTÃO DE CONTINUIDADE DE NEGÓCIOS - GECON

10.8.1 A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da EBC e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da EBC, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, objetivando salvaguardar os interesses da EBC e da sociedade.

10.8.2 As áreas da EBC deverão manter processo de gestão de continuidade de negócios, visando não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

10.8.3 A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática pró-ativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional da EBC.

10.8.4 Todas as áreas da EBC que dependam de recursos de Tecnologia da Informação e da Comunicação deverão criar Planos de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

10.8.5 As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

10.9 FISCALIZAÇÃO

10.9.1 A área de Tecnologia da Informação deverá manter registros e procedimentos, como trilhas de fiscalização e outros que assegurem a conformidade por meio de rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e rede interna da EBC.

10.9.1.1 Fiscalizar conformidades significa aferir a aderência das ações aos regramentos vigentes e o grau de comprometimento dos profissionais em relação aos princípios e práticas da Segurança da Informação e da Comunicação.

10.9.2 A fiscalização uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e melhorar as operações da EBC. Além disso, assiste à EBC na consecução dos seus objetivos por meio de abordagem sistemática e disciplinada, na avaliação da eficácia da gestão de riscos, do controle e dos processos de Governança de TI.

10.9.3 A fiscalização efetua a verificação de forma aleatória e temporal por meio de amostragens para certificar-se do cumprimento das normas e processos instituídos pela alta administração.

10.9.4 A unidade de Auditoria Interna da EBC, no exercício de suas atividades, poderá realizar auditagens e outras ações de acompanhamento e controle sobre a segurança da informação e da comunicação, apoiando-se nos registros e procedimentos de fiscalização da área de Tecnologia da Informação e da Comunicação existentes.

10.10. CONFORMIDADE

10.10.1 A conformidade é o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as diretrizes, a POSIC, suas Normas Complementares e os procedimentos estabelecidos para o negócio e para as atividades da EBC, bem

como para evitar, detectar e tratar qualquer desvio ou não conformidade que possa ocorrer, objetivando:

I - evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações contratuais e de quaisquer requisitos de SIC;

II - executar atividades de verificações de forma rotineira e permanente, monitorando-as para assegurar, de maneira corporativa, que os departamentos e unidades estejam respeitando as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para a prevenção e controle dos riscos envolvidos em cada atividade;

III - ser tão independente quanto à auditoria, reportando-se à alta administração para informá-la de eventos que representem riscos que possam afetar a reputação da EBC;

IV - englobar o acompanhamento dos pontos falhos identificados pela fiscalização e auditoria até que sejam regularizados, configurando interseção das duas áreas; e

V - auxiliar os usuários na resolução de situações não cobertas pela legislação.

10.10.2 Metodologias voltadas à boa conduta e de conformidade devem estar integradas, pois se baseiam em valores e responsabilidade morais, bem como no cumprimento e conformidade das leis e políticas internas.

10.11 CONTROLE DE ACESSO

10.11.1 As regras de controle de acesso a todo sistema corporativo, Intranet, Internet, informações, dados e às instalações da EBC deverão ser definidas e regulamentadas, por meio de Normas Complementares da Política de Segurança da Informação e da Comunicação, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da EBC.

10.11.2 Todo acesso às informações e aos ambientes lógicos da EBC deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação, contemplando:

I - Controle de Acesso Lógico: Permite que os sistemas de TI verifiquem a identidade dos usuários que tentam utilizar seus serviços. Deve ainda utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro; e

II - Controle de Acesso Físico: Por questão de segurança, é obrigatório o uso de identificação física em todos os ambientes e instalações da EBC.

10 12 USO DE E-MAIL

10.12.1 O correio eletrônico é um recurso de comunicação corporativa da EBC. As regras de acesso e utilização de e-mail devem atender a todas as orientações

desta POSIC e das Normas Internas Complementares da Política de Segurança da Informação, além das demais diretrizes do Governo.

10.13 ACESSO A INTERNET

10.13.1 O acesso à rede mundial de computadores - Internet, no ambiente de trabalho, deve ser regido por Normas Internas Complementares da Política de Segurança da Informação e da Comunicação atendendo às determinações desta POSIC, e demais orientações governamentais e legislação em vigor.

10. 14 USO DAS REDES SOCIAIS

10.14.1 O uso das Redes Sociais disponíveis internamente e na rede mundial de computadores - Internet, com o objetivo de prestar atendimento e serviços púbicos, divulgando ou compartilhando informações da EBC, deve ser regido por Norma Complementar da Política de Segurança da Informação e da Comunicação atendendo às determinações desta POSIC, e demais orientações governamentais e legislação em vigor.

10.15 USO DE DISPOSITIVOS MÓVEIS

10.15.1 As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da EBC, devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a esta Política de Segurança da Informação e da Comunicação e regidas por Normas Complementares, a qual contemplará recomendações sobre o uso desses dispositivos.

10.16 USO DE COMPUTAÇÃO EM NUVEM

10.16.1 O uso de recursos de Computação em Nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por Normas Complementares da Política de Segurança da Informação e da Comunicação, atendendo às determinações desta POSIC e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

10.17 ÁREAS DO CONHECIMENTO NORMATIZADAS EM SIC

10.17.1 As normas complementares deverão contemplar as Instruções Normativas da Presidência da República.

10.18 DEMAIS RECURSOS

10.18.1 Todos os demais recursos não descritos acima, que estejam relacionados à POSIC, também deverão ser regulamentados em Normas Complementares.

11. INDICADORES

11.1 Percentual de Incidentes de Segurança, a ser apurado pelo número de tentativas x tentativas frustradas de invasão.

11.2 Percentual de conhecimento sobre o conteúdo da POSIC e suas normas complementares pelos empregados da Empresa, a ser apurado por pesquisa interna.

12. PENALIDADES

12.1 O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e da Comunicação - POSIC poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

12.2 O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à EBC, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

13. LEGISLAÇÃO DE REFERÊNCIA

13.1 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.

13.2 Lei nº 12.527, de 18 de novembro de 2011, que regulamento o acesso às informações públicas;

13.3 Decreto nº 5.452, de 1º de maio de 1943, que aprova a Consolidação das Leis do Trabalho;

13.4 Decreto nº 6.689, de 11 de dezembro de 2008, que aprova o Estatuto Social da Empresa Brasil de Comunicação S.A., e revoga o art. 4º do Decreto nº 6.246, de 24 de outubro de 2007;

13.5 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;

13.6 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.

13.7 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.

13.8 Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências.

13.9 Norma ABNT NBR/ISO/IEC 27002:2013, que institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação.

13.10 Norma ABNT NBR/ISO/IEC 27001:2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e da Comunicação.

13.11 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.

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

13.13 Norma ABNT NBR ISO/IEC 27005:2011, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação e da Comunicação.

13.14 Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e da Comunicação na Administração Pública Federal, direta e indireta, e dá outras providências, e respectivas normas complementares.

13.15 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.

13.16 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.

13.17 Norma de Conflito de Interesses da EBC – NOR 308, de 27 de novembro de 2014.

14. DISPOSIÇÕES GERAIS

14.1 Os casos omissos e as dúvidas surgidas na aplicação desta POSIC serão analisados, dirimidos ou solucionados pelo COSIC.

15. SIGLAS

- ABNT - Associação Brasileira de Normas Técnicas;
- CGOI - Coordenação-Geral de Inovação e Organização Institucional e de Informática;
- COSIC - Comitê da Segurança da Informação e da Comunicação;
- DSIC - Departamento de Segurança da Informação e da Comunicação da Presidência; da República;
- ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

- GECON - Gestão de Continuidade de Negócios em Segurança da Informação e da Comunicação;
- GESIC - Gestão de Segurança da Informação e da Comunicação;
- GESEG – Gestor da Segurança da Informação e da Comunicação;
- GETIR - Gestão de Tratamento de Incidentes de Segurança em Redes de Computadores;
- GRSIC - Gestão de Riscos de Segurança da Informação e da Comunicação;
- GSI/PR - Gabinete de Segurança Institucional da Presidência da República;
- IEC - International Electrotechnical Commission;
- ISO - International Organization for Standardization;
- NBR - Norma Brasileira;
- NIG - Norma Interna Geral;
- POSIC - Política de Segurança da Informação e da Comunicação;
- SIC - Segurança da Informação e da Comunicação;
- SISP - Sistema de Administração dos Recursos de Informação e Informática;
- TIC - Tecnologia da Informação e da Comunicação.