Ministério da Integração Nacional

Departamento Nacional de Obras Contra as Secas – DNOCS

Política de Segurança da Informação e Comunicações

ORIGEM

Departamento Nacional de Obras Contra as Secas

REFERÊNCIA NORMATIVA

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
Decreto nº 1.171, de 22 de junho de 1994.
Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 4.553, de 27 de dezembro de 2002.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e suas normas complementares.
Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação / MPOG, de 12 de novembro de 2010.
Plano Diretor de Tecnologia da Informação – PDTI 2011-2012 DNOCS.
Política de Segurança da Informação do Ministério do Planejamento, Orçamento e Gestão.
Relatório de auditoria do TCU (Acórdão 592/2011 – Plenário).

CAMPO DE APLICAÇÃO

Esta Política de Segurança da Informação e Comunicações se aplica no âmbito do DNOCS.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

ELIAS FERNANDES NETO
Diretor Geral do DNOCS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1. ESCOPO

1.1. Objetivos

A Política de Segurança da Informação e Comunicações (PoSIC) tem como objetivo declarar o comprometimento da Direção Geral do Departamento Nacional de Obras Contra as Secas com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações no DNOCS.

A PoSIC estabelece diretrizes, normas, procedimentos, mecanismos, competências, responsabilidades, direcionamentos e valores a serem adotados para a Gestão de Segurança da Informação e Comunicações (GSIC) no âmbito do DNOCS, adequados às responsabilidades, funcionalidades e peculiaridades de cada uma de suas áreas funcionais.

As diretrizes de Segurança da Informação e Comunicações (SIC) do DNOCS devem considerar, prioritariamente, seus processos, requisitos legais e sua estrutura.

A GSIC deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficácia e eficiência das atividades de SIC.

Os objetivos das ações a serem implementadas são a salvaguarda dos dados, das informações e materiais sensíveis, críticos e sigilosos de interesse do DNOCS, dos sistemas computacionais, suas instalações e das áreas de trabalho, além da preservação da inviolabilidade e da intimidade da vida privada, da honra e da imagem das pessoas.

Integram também a PoSIC normas e procedimentos complementares destinados à proteção da informação e a disciplina de sua utilização.

1.2. Abrangência

As diretrizes, normas complementares e manuais de procedimentos da PoSIC do DNOCS aplicam-se aos usuários dos ativos de informação da Administração Central e Coordenadorias Estaduais e a quem de alguma forma execute atividades vinculadas a esta Autarquia.

Os acordos de cooperação, contratos, convênios e outros instrumentos do mesmo gênero celebrados com o DNOCS devem observar o conteúdo desta PoSIC.

Aplica-se esta política, no que couber, no relacionamento do DNOCS com outros órgãos públicos ou entidades privadas.

2. CONCEITOS E DEFINIÇÕES

Para efeitos desta PoSIC, adotam-se as seguintes conceituações:

I. acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

II. ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III. ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

IV. ativo de informação: ativo que guarda informações do órgão;

V. autenticidade: asseveração de que o dado ou a informação é verdadeiro e fidedigno tanto na origem quanto no destino;

VI. cessão de bases de dados: ato de disponibilizar cópia, total ou parcial, de dados do DNOCS, aprovada pelo gestor competente;

VII. ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua autenticidade, confidencialidade, integridade e disponibilidade;

VIII. classificação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

IX. Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do DNOCS;

X. comprometimento: perda de segurança resultante do acesso não-autorizado;

XI. concedente: responsável pelo fornecimento da base de dados confidenciais pelo DNOCS;

XII. confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XIII. conta de acesso: conjunto do "nome de usuário" e "senha" utilizado para acesso aos sistemas informatizados e recursos de TIC;

XIV. controles de segurança: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XV. credencial de segurança: certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo;

XVI. custodiante: agente público responsável por zelar pelo armazenamento e pela preservação do ativo sob sua propriedade;

XVII. dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XVIII. dados confidenciais: dados pessoais que permitam a identificação da pessoa e possam ser associados a outros dados referentes ao endereço, idade, raça, opiniões políticas e religiosas, crenças, ideologia, saúde física, saúde mental, vida sexual, registros policiais, assuntos familiares, profissão e outros que a lei assim o definir, não podendo ser divulgados ou utilizados para finalidade distinta da que motivou a estruturação do banco de dados, salvo por ordem judicial ou com anuência expressa do titular ou de seu representante legal;

XIX. dados pessoais: representação de fatos, juízos ou situações referentes a uma pessoa física ou jurídica, passível de ser captada, armazenada, processada ou transmitida por meios informatizados ou não;

XX. disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XXI. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de

pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

XXII. evento: 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 conhecida que possa ser relevante para a segurança da informação;

XXIII. gestor da informação: agente público do DNOCS responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

XXIV. Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de segurança da informação e comunicações no âmbito do DNOCS;

XXV. grau de sigilo: gradação de segurança atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;

XXVI. incidente de segurança: indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores;

XXVII. informação custodiada: informação sob a guarda e responsabilidade de alguém;

XXVIII. integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino;

XXIX. investigação para credenciamento: averiguação sobre a existência dos requisitos indispensáveis para a concessão de credencial de segurança;

XXX. legitimidade: asseveração de que o emissor e o receptor de dados ou informações são legítimos e fidedignos tanto na origem quanto no destino;

XXXI. marcação: aposição de marca assinalando o grau de sigilo;

XXXII. medidas especiais de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade, legitimidade e disponibilidade de dados e informações sigilosos. Também objetivam prevenir, detectar, anular e registrar ameaças reais ou potenciais a esses dados e informações;

XXXIII. necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou informações sigilosos;

XXXIV. ostensivo: sem classificação, cujo acesso pode ser franqueado;

XXXV. quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXVI. reclassificação: alteração, pela autoridade competente, da classificação de dado, informação, área ou instalação sigilosos;

XXXVII. recursos de TIC: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, *notebooks*, servidores de rede, equipamentos de conectividade e infraestrutura;

XXXVIII. rede corporativa: conjunto de todas as redes locais sob a gestão do DNOCS;

XXXIX. rede local: conjunto de equipamentos interligados localmente com o objetivo de disponibilizar serviços aos usuários de rede do DNOCS;

XL. segurança da informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

XLI. senha ou palavra-chave: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;

XLII. sigilo: segredo de conhecimento restrito a pessoas credenciadas e protegido contra revelação não autorizada;

XLIII. software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas;

XLIV. usuário da rede: qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa do DNOCS;

XLV. usuário de sistema: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pelo DNOCS;

XLVI. visita: pessoa cuja entrada foi admitida, em caráter excepcional, em área sigilosa; e

XLVII. vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3. PRINCÍPIOS

Esta PoSIC e os documentos elaborados a partir dela devem obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

4. IRETRIZES GERAIS

O DNOCS deve instituir uma estrutura organizacional estratégica de Gestão de SIC, refletida no regimento interno, com a responsabilidade de executar os processos de SIC.

Essa estrutura deve definir um Plano de SIC juntamente com um orçamento adequado para a implementação das ações definidas no Plano.

A Gestão de SIC do DNOCS deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as orientações estratégicas e necessidades operacionais prioritárias da Autarquia e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

O DNOCS deve se orientar pelas melhores práticas e procedimentos de segurança da informação, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

O DNOCS deve assegurar que os usuários entendam suas responsabilidades e estejam de acordo com os seus papéis para prevenir fraudes, roubos ou mau uso dos recursos.

Os contratos firmados pelo DNOCS devem conter cláusulas que determinem a observância desta PoSIC e seus respectivos documentos.

As medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança.

Para cada uma das diretrizes abaixo, deve ser elaborada norma tática específica e Manual de Procedimentos.

4.1. Tratamento da Informação

O DNOCS deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

4.2. Gestão de Incidentes

Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a impedir a interrupção das atividades e não afetar o alcance dos objetivos estratégicos.

4.3. Gestão de Risco

Deve ser estabelecido um processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) com vistas a minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

4.4. Gestão de Continuidade

Deve ser estabelecida a Gestão de Continuidade de Negócio no âmbito do DNOCS visando reduzir a possibilidade de interrupção causada por desastres ou falhas graves nos recursos que suportam as operações críticas desta Autarquia.

4.5. Auditoria e Conformidade

O cumprimento desta PoSIC deve ser avaliado, periodicamente, pela alta direção, em conformidade com Normas Complementares, Manuais de Procedimentos e legislação específica de SIC, buscando a certificação do atendimento dos requisitos de segurança da informação. A alta direção poderá se valer de grupos internos ou externos para consecução de auditorias.

4.6. Controles de Acesso

Devem ser instituídas normas que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação.

4.7. Gestão de operações e comunicações

Ações de segurança deverão garantir a operação segura e correta dos recursos de processamento da informação desta Autarquia.

As atividades do DNOCS deverão ser protegidas contra interrupções não programadas.

O gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços.

As informações e os recursos de processamento de informação deverão ter controles específicos que garantam a integridade e a disponibilidade dos mesmos.

As trocas de informações, tanto internamente, quanto externamente, deverão ser reguladas de forma a manter o nível adequado da segurança.

As operações deverão ser adequadamente monitoradas de forma a detectar atividades não autorizadas.

4.8. Segurança Física e do Ambiente

Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados.

5. PENALIDADES

Ações que violem esta PoSIC, diretrizes, normas e procedimentos, ou que quebrem os controles de SIC serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Processo disciplinar específico deverá ser elaborado para apurar as ações que constituem em quebra das diretrizes impostas por esta PoSIC.

6. COMPETÊNCIAS E RESPONSABILIDADES

É de responsabilidade de todos que têm acesso aos ativos do DNOCS manter níveis de segurança da informação adequados, segundo preceitos desta política.

6.1. Alta Direção

É de responsabilidade da alta administração desta Autarquia prover a orientação e o apoio necessários às ações de SIC, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

6.2. Gestor de Segurança da Informação e Comunicações

Compete ao Gestor de Segurança da Informação e Comunicações do DNOCS:

I - promover cultura de segurança da informação e comunicações;

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

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações; e

VII - propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do DNOCS;

VIII - coordenar a Gestão de Riscos de Segurança da Informação e Comunicações;

IX - coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;

X - prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR; e

XI - implementar procedimentos relativos ao uso dos recursos criptográficos, em conformidade com as orientações contidas na Norma Complementar 09/IN01/DSIC/GSIPR, de 22 de novembro de 2010.

6.3. Comitê de Segurança da Informação e Comunicações (CSIC)

Compete ao Comitê de Segurança da Informação e Comunicações do DNOCS:

I - assessorar na implementação das ações de SIC no DNOCS;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

III - propor Normas e Procedimentos internos relativos à SIC em conformidade com as legislações existentes sobre o tema;

IV – apurar incidentes que violem esta PoSIC; e

V - avaliar, revisar, analisar criticamente, propor alterações, dirimir eventuais dúvidas e deliberar sobre assuntos relativos a esta PoSIC e suas normas complementares, visando a sua aderência e concordância aos objetivos institucionais desta Autarquia e às legislações vigentes.

6.4. Gestor do Ativo de Informação

Cabe ao Gestor do Ativo de Informação:

I - tratar e classificar a informação;

II - definir os requisitos de segurança para os ativos sob sua responsabilidade;

III - conceder e revogar acessos;

IV - autorizar a divulgação de informações;

6.5. Custodiante do Ativo de Informação

Cada ativo de informação ou conjunto de ativos, dentro do DNOCS, deve ter um custodiante designado, pela autoridade competente da unidade administrativa, como o responsável por proteger e manter as informações e controlar o acesso conforme requisitos definidos pelo gestor da informação e em conformidade com esta POSIC.

6.6. Equipe de Segurança

Compete à Equipe de Segurança:

I - desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos do DNOCS;

II - avaliar, selecionar, utilizar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

III - conscientizar os usuários a respeito da implementação desses controles;

IV - verificar se todos os usuários colaboram com as medidas de segurança implantadas.

6.7. Gestores Administrativos

Cabe aos Gestores Administrativos:

I - multiplicar e catalisar os princípios de segurança;

II - autorizar concessão, transferência e revogação de acessos;

III - responder conjuntamente pelas ações realizadas por seus subordinados;

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

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

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

6.8. Terceiros e Fornecedores

É responsabilidade dos terceiros e fornecedores:

I - proteger os ativos de informação desta Autarquia, incluindo informação, evitando perda ou modificação de dados, *software* e *hardware*;

II - assegurar o retorno ou a destruição da informação e dos ativos no final do contrato, ou em um dado momento definido no acordo;

III - observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;

IV - observar restrições em relação à manutenção e instalação de *software* e *hardware*;

V - atender à política de controle de acesso desta Autarquia;

VI - relatar incidentes de segurança da informação e violação da segurança à equipe de segurança e à equipe de tratamento e respostas a incidentes; e

VII - atender aos princípios e diretrizes contidos nesta PoSIC, incluindo normas e procedimentos complementares destinados à SIC.

6.9. Usuários

É responsabilidade dos usuários:

I - difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema;

II - proteger os ativos de informação desta Autarquia, incluindo informação, evitando perda ou modificação de dados, *software* e *hardware*;

III - observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;

IV - observar restrições em relação à manutenção e instalação de *software* e *hardware*;

V - atender à política de controle de acesso desta Autarquia;

VI - relatar incidentes de segurança da informação e violação da segurança; e

VII - atender aos princípios e diretrizes contidos nesta PoSIC, incluindo normas e procedimentos complementares destinados à SIC; e

VIII - ser responsável por todos os atos praticados com suas identificações (login, crachá, carimbo, e-mail, assinatura digital, etc).

7. ATUALIZAÇÃO

Esta PoSIC, bem como os documentos gerados a partir dela, devem ser revisados e atualizados no mínimo uma vez ao ano, ou quando mudanças significativas ocorrerem.

8. VIGÊNCIA

Esta PoSIC entra em vigor na data de sua publicação.