­­­­

**Guia para desenvolvimento de uma Política de Segurança da Informação e Comunicações**

**CAIS/RNP**

**APRESENTAÇÃO**

Este documento apresenta orientações para o desenvolvimento de uma Política de Segurança da Informação e Comunicações (POSIC), se consolidando como um guia para auxiliar as organizações usuárias da RNP a desenvolverem um documento personalizado e aderente a sua realidade.

Seu conteúdo é baseado nas legislações aplicáveis aos órgãos da Administração Pública Federal e em boas práticas de mercado.

Ao longo do documento são descritas as etapas para construção de uma POSIC e são apresentadas as boas práticas para desenvolvimento de cada seção.

**LISTA DE ABREVIATURAS E SIGLAS**

1. APF – Administração Pública Federal
2. BSI *- British Standard Institute*
3. CAIS – Centro de Atendimento a Incidentes de Segurança
4. CSIC – Comitê de Segurança da Informação e Comunicações
5. ISO *- International Organization for Standardization*
6. OU – Organização Usuária dos serviços da RNP
7. POSIC – Política de Segurança da Informação e Comunicações
8. RNP – Rede Nacional de Ensino e Pesquisa
9. SI – Segurança da Informação
10. TCU – Tribunal de Contas da União
11. TIC – Tecnologia da Informação e Comunicações

**SUMÁRIO**

[1. Introdução 6](#_Toc465089208)

[2. Objetivo 7](#_Toc465089209)

[3. Referências 7](#_Toc465089210)

[4. FASES PARA O DESENVOLVIMENTO DA POSIC 8](#_Toc465089211)

[5. Planejando o desenvolvimento da POSIC 8](#_Toc465089212)

[5.1. FORMALIZAÇÃO DE UM GRUPO DE TRABALHo 9](#_Toc465089213)

[5.2. Conhecendo a organização 10](#_Toc465089214)

[5.3. Identificando as partes interessadas 11](#_Toc465089215)

[5.4. Identificando o modelo de estrutura normativa utilizado pela organização 12](#_Toc465089216)

[6. Desenvolvimento, aprovação e divulgação da POSIC 14](#_Toc465089217)

[6.1. Desenvolvimento do documento 14](#_Toc465089218)

[6.2. Revisão e aprovação pelo Comitê de SI 14](#_Toc465089219)

[6.3. Revisão e aprovação pela ALTA DIREÇÃO ORGANIZACIONAL 15](#_Toc465089220)

[6.4. Publicação da POSIC 15](#_Toc465089221)

[6.5. Divulgação da POSIC 16](#_Toc465089222)

[7. Estrutura mínima para a POSIC 16](#_Toc465089223)

[7.1. APRESENTAÇÃO 18](#_Toc465089224)

[7.2. Distribuição e atualização 19](#_Toc465089225)

[7.3. Índice 20](#_Toc465089226)

[7.4. Objetivo da POSIC 21](#_Toc465089227)

[7.5. escopo da POSIC 22](#_Toc465089228)

[7.6. Referências legais e normativas 23](#_Toc465089229)

[7.7. Conceitos e definições 24](#_Toc465089230)

[7.8. Princípios da Segurança da Informação 25](#_Toc465089231)

[7.9. Diretrizes Gerais 26](#_Toc465089232)

[7.10. Responsabilidades 28](#_Toc465089233)

[7.11. monitoramento e auditoria 29](#_Toc465089234)

[7.12. Sanções Disciplinares 30](#_Toc465089235)

[8. Considerações finais 32](#_Toc465089236)

[ANEXO A – CHECKLIST PARA DESENVOLVIMENTO DE UMA POSIC 33](#_Toc465089237)

[Créditos 35](#_Toc465089238)

# Introdução

É de conhecimento comum que a Internet e os meios computacionais aumentaram e aceleraram, consideravelmente, o fluxo de informações entre pessoas e organizações. Este cenário, por sua vez, aumentou o número de ameaças aos requisitos de segurança das informações, algo que até então era inexpressivo já que os mecanismos de comunicação eram mais rudimentares e fáceis de serem controlados. A necessidade de controlar e proteger as informações torna-se, então, um item mandatório para as organizações, seja por requisitos legais ou do negócio, permitindo que a organização mantenha sua plena operação.

No que tange os órgãos e entidades da Administração Pública Federal (APF), foi publicado o Decreto nº. 3.505, de 13 de junho de 2000, instituindo a Política Nacional de Segurança das Informações, devendo ser implementada pelos órgãos e entidades da APF, direta e indireta.

O Gabinete de Segurança Institucional da Presidência da República estabeleceu a Instrução Normativa Nº. 01 (IN01), de 13 de junho de 2008, a qual resolve aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da APF, direta e indireta. Essas orientações são detalhadas em 21 normas complementares, sendo a Norma Complementar nº 03, específica sobre a elaboração da POSIC nos Órgãos e Entidades da APF.

Como forma de avaliar o nível de maturidade dos órgãos e entidades da APF em relação ao tema, o Tribunal de Contas da União (TCU) realiza a cada dois anos um levantamento de informações sobre Governança de TI. Em 2014, foi constatado que 50% dos órgãos/entidades pesquisados não possuem uma POSIC formalmente definida. Conforme o TCU, a ausência da POSIC é um indício preocupante já que esse documento de diretrizes é um dos primeiros passos na construção de uma gestão da segurança da informação.

Mediante o levantamento do TCU pode-se elencar alguns fatores que impactam as instituições e dificultam a elaboração de uma POSIC:

* Falta de pessoal capacitado;
* Falta de recursos;
* Falta de apoio da direção da organização;
* Não possuir uma área específica de segurança da informação;
* Falta de um guia prático que possa orientar no processo de elaboração.

A Rede Nacional de Ensino e Pesquisa (RNP), motivada em auxiliar as organizações usuárias na proteção de suas informações, desenvolveu este guia com recomendações para a elaboração de uma POSIC. Este guia está baseado nas melhoras práticas sobre o tema e possui duas partes principais: os passos para o desenvolvimento, aprovação e divulgação da POSIC apresentados nos capítulos 4 a 6, e uma proposta de estrutura mínima para o documento apresentada no Capítulo 7.

# Objetivo

O objetivo deste documento é ser um guia prático para auxiliar as organizações usuárias da RNP na elaboração da Política de Segurança da Informação e Comunicações, apresentando um conjunto de atividades e boas práticas para a construção do documento, auxiliando as organizações no atendimento ao estabelecido na Norma Complementar nº 03, de 3 de Julho de 2009.

# Referências

* ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão de segurança da informação – Requisitos;
* ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação;
* Norma complementar nº 03/IN01/DSIC/GSIPR de 3 de Julho de 2009 – Departamento de Segurança da Informação e Comunicações.

# FASES PARA O DESENVOLVIMENTO DA POSIC

Neste guia serão apresentadas, passo a passo, as etapas para o desenvolvimento de uma POSIC, bem como sua revisão, aprovação e divulgação às partes interessadas. O fluxograma a seguir presenta, visualmente, estas etapas.



O Anexo A apresenta um *checklist* que pode ser utilizado como base para acompanhamento das fases e atividades descritas neste guia, incluindo referências internas, externas e status. O *checklist* pode ser customizado de acordo com as necessidades da instituição, incluindo status de revisão e aprovação das instâncias necessárias.

# Planejando o desenvolvimento da POSIC

Uma fase essencial para o sucesso de uma POSIC em uma organização é o planejamento inicial, o qual ajudará a entender o cenário atual e levantar subsídios para que a POSIC seja adequada e efetiva para a organização.

As atividades que devem compor o planejamento são:

* Formalização de um Grupo de Trabalho;

Mais:

ISO 27001 - Seção 4

ISO 27002 – Controle 5.1.1

* Conhecendo a organização;
* Identificando as partes interessadas;
* Identificando o modelo de estrutura normativa utilizado pela organização.

As seções a seguir detalham as fases do planejamento, apresentando suas atividades, documentos necessários e exemplos práticos.

## FORMALIZAÇÃO DE UM GRUPO DE TRABALHo



Antes de iniciar o desenvolvimento da POSIC, recomenda-se o estabelecimento de um Grupo de Trabalho (GT) para conduzir as atividades envolvidas na elaboração e aprovação do documento. Esse grupo de trabalho deve ser formado, minimamente, por um especialista em gestão de segurança da informação e representantes das áreas de TI, recursos humanos, segurança patrimonial e jurídico, este último com sólidos conhecimentos em Direito Digital.

A atribuição das responsabilidades do GT deve ser formal e oficializada pela organização, por exemplo, através de portarias institucionais. Caso a organização possua um Comitê de Segurança da Informação e Comunicações (CSIC) estabelecido, este deve ser responsável pela formação do GT.

Recomenda-se que o GT desenvolva seu trabalho, seguindo as práticas de Gerenciamento de Projeto, formalizando, no mínimo, um plano de projeto e cronograma. Recomenda-se que o cronograma para elaboração e aprovação tenha, no máximo, 6 meses de duração. Isso porque o contexto da organização pode mudar e as definições iniciais podem ficar defasadas, implicando em um retrabalho. Para que isso seja possível, é importante que os membros do GT tenham carga horária reservada ao projeto e que reporte periodicamente o andamento do projeto à alta direção da organização e ao CSIC. Essas recomendações ajudarão na formação de um GT que realmente gere resultado, ao invés de nunca cumprir o seu objetivo por falta de priorização e foco.

## Conhecendo a organização



Realizar o levantamento de informações sobre a organização, conhecendo suas características e objetivos, é um fator crítico de sucesso para a POSIC, uma vez que este documento deve ser adaptado às necessidades da organização e apoiar no cumprimento dos objetivos do negócio.

Mais:

ISO 27001 – seção 4.1

|  |
| --- |
| **Quais informações devem ser levantadas?**  Identificar documentos e informações relacionadas ao modelo de gestão organizacional, estratégia organizacional, objetivos estratégicos, metas, missão e visão da organização.  É importante identificar:   * Estrutura organizacional; * Objetivos da organização em curto, médio e longo prazo; * Processos de negócio; * Tipos de usuários; * Leis e regulamentações com requisitos de segurança aplicáveis à organização; * Requisitos contratuais; * Histórico de incidentes; * Informações sobre os riscos de SI. |

O cenário da organização pode ser muito dinâmico e as diretrizes da POSIC terão como base o cenário levantado nesta fase. Por isso, é importante documentar o momento atual do início do desenvolvimento da POSIC e que esta atividade não dure mais que 6 meses, evitando que levantamento desta fase fique defasado.

## Identificando as partes interessadas



A POSIC apresenta a orientação da alta direção sobre o tema segurança da informação para toda a organização e partes externas relevantes. Para isso, é necessário identificar quem compõe a alta direção e quem são as partes interessadas que apoiarão o desenvolvimento e aprovação da POSIC.

Mais:

ISO 27001 – seção 4.2

É importante também levantar quais as expectativas das partes interessadas, identificando requisitos relevantes para a segurança da informação. Por exemplo, um requisito pode ser o atendimento de uma determinada legislação ou dos normativos do DSIC.

|  |
| --- |
| **Quais informações devem ser levantadas?**  Identificar como é composta a alta direção organizacional da organização e qual o cargo de maior relevância para declarar internamente a importância da POSIC e apoiar sua implementação.  É importante identificar:   * Composição da alta direção organizacional; * Gestores das principais áreas de negócio (exemplo: pró-reitor de extensão, pró-reitor de pesquisa, etc.); * Gestores ligados a TIC e a governança de TIC; * Gestores envolvidos com processos de segurança da informação; * Especialista em Direito Digital da Área Jurídica; * Gestores ligados a áreas de controladoria e/ou conformidade; * Gestores da área de Recursos Humanos ou Pessoal; * Representações internas, como DCE, sindicatos de professores, CIPA, etc.   Para cada parte interessada, identificar as expectativas e requisitos de segurança da informação. Recomenda-se que este levantamento seja realizado em entrevistas presenciais, pois é possível fornecer esclarecimentos e orientar a atividade para uma visão mais correta e adequada ao trabalho. |

**Importante**: As partes interessadas identificadas podem ser o ponto de partida para a formação do Comitê de Segurança da Informação e Comunicações (CSIC) da organização, caso o mesmo ainda não esteja estabelecido. A instituição do CSIC é um item mandatório, segundo a Norma Complementar nº 03 do DSIC, e deve ter as seguintes responsabilidades:

* Assessorar na implementação das ações de segurança da informação e comunicações;
* Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
* Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

Não é objetivo deste documento apresentar orientações para o estabelecimento do CSIC, porém é premissa para o restante do trabalho que o mesmo esteja formalmente instituído na organização.

## Identificando o modelo de estrutura normativa utilizado pela organização



O modelo de estrutura normativa utilizado pela organização ajudará a definir a melhor maneira para documentar a POSIC. A ISO 27001 apresenta o conceito de políticas de segurança da informação, com o termo no plural, para que cada organização formalize as diretrizes da maneira que for mais apropriada para seu negócio, que pode ser um único ou diversos documentos, por exemplo. O importante é que o conteúdo final apresente as diretrizes ou direcionadores para todos os temas relevantes para a segurança da informação.

Mais:

ISO 27001 – seção 7.5

Neste passo devem ser definidos a nomenclatura e o padrão para os documentos de segurança. Caso a organização já possua um modelo para o desenvolvimento de normativos, recomenda-se a adoção do mesmo. Caso contrário, é importante definir a estrutura do documento e a nomenclatura para identificação de todos os documentos da estrutura normativa de segurança.

|  |
| --- |
| **Quais informações devem ser levantadas?**  Identifique como é composta a estrutura normativa de sua organização, a nomenclatura utilizada para cada tipo de documento e se existem modelos para a construção de documentos normativos.  É importante identificar:   * Estrutura normativa ou hierarquia dos documentos existente; * Nomenclatura utilizada para documentos, no mínimo três níveis:   + Nomenclatura utilizada para documentos que apresentam diretrizes estratégicas (ex. política, regulamento, decreto);   + Nomenclatura utilizada para documentos que apresentam diretrizes táticas (ex. norma, instrução normativa);   + Nomenclatura utilizada para documentos que apresentam informações operacionais (ex. procedimentos); * Regras existentes para classificação e distribuição de documentos; * Modelos utilizados para construção de documentos normativos. |

# **Desenvolvimento, aprovação e divulgação da POSIC**

## Desenvolvimento do documento



A atividade de desenvolvimento do documento consiste em escrever efetivamente a POSIC, com base em todos os insumos levantados.

Recomenda-se que o desenvolvimento do documento seja conduzido pelo gestor ou especialista da área de segurança da informação e que este esteja familiarizado com a criação de normativos. Esta pessoa orientará o GT na definição das diretrizes.

O capítulo 7 apresenta a estrutura mínima para a POSIC, trazendo as seções que devem ser contempladas no documento e apresentando referências para seu desenvolvimento.

Mais:

ISO 27001 e 27002

DSIC NC 03

A elaboração da POSIC deve levar em consideração a natureza e objetivos da organização, alinhando-se à missão e ao planejamento estratégico.

## Revisão e aprovação pelo Comitê de SI



Após o desenvolvimento do documento devem ser realizadas as etapas de revisão e aprovação pelo CSIC. O papel do Comitê é analisar criticamente o documento e suas diretrizes, verificando se estão aderentes aos processos, ao negócio e à cultura da organização. O olhar do Comitê deve trazer uma visão estratégica da organização.

Após a finalização da análise e da implementação dos possíveis ajustes na POSIC, o Comitê deve emitir um parecer recomendando a aprovação pela instância máxima da organização.

## Revisão e aprovação pela ALTA DIREÇÃO ORGANIZACIONAL



A revisão e a aprovação pela alta direção organizacional são os últimos passos para que a POSIC possa ser publicada e divulgada à toda organização.

A alta direção de sua organização pode ser representada pela Diretoria, pelo Presidente, pelo Reitor, pelo Conselho Universitário, entre outros. Verifique na sua organização qual instância é responsável pela aprovação de normativos.

Mais:

ISO 27001 – seção 5.2

## Publicação da POSIC



A POSIC deve ser publicada em um canal de comunicação oficial da organização e acessível a todos que deverão conhecer e cumprir as diretrizes, além de ser divulgado no Diário Oficial.

## Divulgação da POSIC



Após a publicação da POSIC é necessário comunicar as partes relevantes sobre o documento e a necessidade de seguir as diretrizes de segurança. A divulgação pode ser realizada em diversos veículos internos da organização, como e-mail, site institucional, dentre outros. Uma opção é a realização de uma campanha de conscientização, que apresente a POSIC e realize um treinamento dos usuários.

Mais:

DSIC NC03 – seção 7

É importante que a divulgação seja feita de forma efetiva e registrada, atingindo todos os usuários, seja através da assinatura de um termo de ciência da POSIC ou através da presença em um treinamento.

Recomenda-se a elaboração de materiais de apoio, em linguagem simples, com informações sobre a POSIC, como seu objetivo, a quem se destina, onde está disponível, contatos em caso de dúvidas, dentre outros.

# Estrutura mínima para a POSIC

A Política de Segurança da Informação e Comunicações de cada organização é um documento único e desenvolvido para uma organização, respeitando sua cultura, missão, objetivos, tipo de gestão entre outras particularidades. Para a apoiar o desenvolvimento da POSIC, a organização pode consultar diversas referências disponíveis como a ISO 27001, ISO 27002, a Norma Complementar nº 03 do DSIC e outras boas práticas sobre o tema.

Ao desenvolver a POSIC, a organização pode optar por diferentes estruturas. É possível consultar diversos tipos de políticas, algumas mais detalhadas e outras mais concisas. Não existe o modelo correto e, sim, o mais adequado para aquela organização.

Entretanto, é possível definir alguns fatores para avaliar se a POSIC está boa e adequada. Uma boa POSIC é aquela que traz direcionadores claros e objetivos, alinhados à organização e que contribui de forma efetiva com os objetivos estratégicos e metas da organização. Outro fator é que a leitura da POSIC deve ser de fácil entendimento por todas as partes relevantes.

O primeiro desafio no desenvolvimento da POSIC consiste, então, em definir a sua estrutura. Recomenda-se a adoção de uma estrutura simples e enxuta, e a escrita de diretrizes macros, por se tratar de um documento de caráter mais amplo e estratégico para a segurança da informação. O detalhamento das diretrizes, nos níveis tático e operacional, pode estar disponível em outros documentos normativos que tratem de temas específicos, por exemplo, uma norma de gestão de incidentes de segurança.

Este capítulo apresenta uma sugestão de estrutura mínima para que seja construída uma boa POSIC. Em cada seção são abordados os temas e as boas práticas para conduzir o desenvolvimento do tema. A organização pode utilizar esta estrutura na sua POSIC ou customizá-la, de acordo com as necessidades.

As seções mínimas recomendadas para a POSIC são:

* Apresentação;
* Distribuição e atualização;
* Índice;
* Objetivo da POSIC;
* Escopo da POSIC;
* Referências legais e normativas;
* Conceitos e definições;
* Princípios de Segurança da Informação;
* Diretrizes gerais;
* Responsabilidades;
* Monitoramento e auditoria;
* Sanções disciplinares.



As seções a seguir apresentarão o conteúdo que deve ser abordado em cada item acima e como a construção pode ser conduzida internamente, como as boas práticas de escrita, os grupos ou áreas que podem ser consultados e os documentos de referência.

Não é objetivo deste documento apresentar modelos de textos para as diretrizes. Este conteúdo pode ser encontrado no documento “Modelo para construção de uma Política de Segurança da Informação e Comunicação (POSIC)” também disponibilizado pela RNP.

## APRESENTAÇÃO



Esta seção apresenta um texto que demonstre o apoio e a visão da alta direção organizacional sobre a POSIC e sobre o tema segurança da informação.

O apoio da alta direção organizacional mostra credibilidade para o documento, fazendo com que as pessoas deem mais importância e atenção ao tema. Este engajamento da organização é fundamental para o sucesso e a implementação da POSIC.

A pessoa com o cargo mais alto na organização poderá escrever uma carta ou uma abertura destacando a importância das informações e a necessidade de protegê-las.

## Distribuição e atualização



Esta seção apoia o processo de controle de documentos, que é obrigatório para os normativos do Sistema de Gestão de Segurança da Informação (SGSI). Devem ser informados: a distribuição, quem tem permissão de acesso e a atualização da revisão do documento.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique se a organização já possui um padrão para classificação e distribuição dos documentos; * Verifique se a organização já possui um padrão para revisão de documentos, definindo a periodicidade e o fluxo que deve ser seguido. |
| Atividades para construção da seção | * Identifique o público alvo da POSIC. Pode ser todos os usuários da organização – incluindo prestadores de serviço e visitantes – ou apenas uma parte deles, como os funcionários concursados; * Escreva um texto deixando claro qual o público de distribuição da POSIC, ou seja, para quem se aplica as diretrizes da POSIC. Isso facilitará o processo de auditoria e a identificação de incidentes de segurança, como o acesso não autorizado; * Identifique qual a melhor periodicidade para revisão do documento. Leve em consideração a cultura da organização e o tempo e complexidade do processo de aprovação. Não é uma boa prática determinar um período inferior a um (1) ano, pois a política deve conter diretrizes mais amplas que não devem ser alteradas em curto prazo. Caso isso ocorra, deve-se verificar se o seu conteúdo está correto. O DSIC recomenda que o prazo de revisão da POSIC não ultrapasse três (3) anos. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Responsáveis pelo controle de documentos corporativos; * Responsáveis pelo Sistema de Gestão da Qualidade. |
| Informações adicionais | * ISO 27001 - Seção 7.5 * DSIC NC 03 – item 5.3.8 e 8 |

## Índice

Este item é opcional e também depende da cultura de sua organização. Se não for um padrão dos documentos utilizar o índice, não há problemas em não ser inserido no documento.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique o padrão dos documentos da organização para definir se a POSIC deve ter um índice ou não. |
| Atividades para construção da seção | * Construa o índice apresentando, no mínimo, três níveis de títulos. Isso facilitará o entendimento do documento pelo leitor. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Não se aplica |
| Informações adicionais | * Não se aplica |

## Objetivo da POSIC

Esta seção deve apresentar o objetivo da POSIC, o porquê deste documento, o papel da segurança da informação, a importância das informações para a organização, entre outros.

Este texto deve ser claro e objetivo, sem palavras muito técnicas, ou que requeiram um conhecimento prévio sobre o assunto.

Quanto mais simples o texto for, maior a chance do leitor, que não entende tecnicamente de segurança da informação, captar a mensagem e se interessar pelo conteúdo. Lembre-se que a maior parte do público que terá que ler, entender e cumprir a POSIC não é da área de segurança ou TI.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique a linguagem utilizada por outras políticas da organização e também o tipo de linguagem utilizada pela maioria dos colaboradores. Dependendo da cultura da organização, pode ser um texto mais ou menos formal. * Levante as referências legais que obrigam a organização a ter uma POSIC; * Levante as boas práticas de mercado que direcionam para a construção de uma POSIC; * Levante informações sobre as organizações que atuam no mesmo segmento e quantas delas possuem POSIC. Os relatórios do TCU também possuem informações que podem ser consultadas. |
| Atividades para construção da seção | * Escreva o texto com uma linguagem conhecida e de fácil entendimento pelos colaboradores; * Inclua no texto a motivação e o objetivo da POSIC, além da importância de se cuidar das informações. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Alta direção organizacional; * CSIC; * Responsáveis pelas principais áreas de negócio. |
| Informações adicionais | * ISO 27001 – seção 5.2 * DSIC NC 03 – item 5.1 e 5.2 |

## escopo da POSIC

Esta seção deve apresentar a aplicação e abrangência da POSIC na organização, a quais pessoas e processos o documento está relacionado. O escopo define os limites no qual as ações de segurança da informação se aplicam na organização.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Levante informações do público alvo, a quem a POSIC se destina e que tipo de usuários deverão conhecer e cumprir suas diretrizes; * Levante a abrangência da POSIC, se sua aplicação será para toda a organização ou apenas para algumas áreas ou processos específicos. |
| Atividades para construção da seção | * Liste as informações levantadas, dividindo, se possível, em dois parágrafos distintos para descrição do público alvo e da abrangência da POSIC. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Alta direção organizacional; * CSIC; * Responsáveis pelas principais áreas de negócio. |
| Informações adicionais | * DSIC NC 03 – seção 5.3.1 |

## Referências legais e normativas



As referências legais e normativas orientam o desenvolvimento da POSIC e dos demais documentos de segurança da informação. Apresentá-los no documento mostra o peso que a POSIC possui, confirma as informações apresentadas no objetivo e escopo do documento e oferece a possibilidade do leitor se informar sobre o assunto.

O conteúdo desta seção pode ser transferido para um anexo, caso a relação de referências fique extensa. Neste caso, no corpo da POSIC, coloca-se apenas a informação onde encontram-se as referências legais e normativas.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Levante as referências legais que obrigam a organização a ter uma POSIC (se ainda não tiver feito anteriormente); * Verifique com a área jurídica se existe um levantamento das referências legais relacionadas à SI ou se existe algum consultor especializado em Direito digital que possa apoiar; * Veja se outros documentos da organização possuem o conteúdo dessa seção dentro do próprio documento ou em um documento apartado. |
| Atividades para construção da seção | * Escreva o texto com base nos insumos levantados, nas orientações da alta direção organizacional e do Comitê de SI para a POSIC. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Jurídico; * CSIC; * Auditoria interna/conformidade. |
| Informações adicionais | * DSIC NC 03 – seção 5.3.3 |

## Conceitos e definições



Esta seção apresenta os principais conceitos e definições de segurança da informação utilizados na POSIC e cujo entendimento se faz necessário para a correta leitura do documento, evitando-se dificuldades de interpretação ou significados ambíguos.

O conteúdo desta seção pode ser transferido para um anexo, caso a relação de conceitos e definições fique extensa. Neste caso, no corpo da POSIC, coloca-se apenas a informação onde encontram-se os conceitos.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique se a organização possui algum dicionário de termos e definições ou dicionário de TIC; * Verifique se outros documentos da organização possuem o conteúdo dessa seção dentro do próprio documento ou em um documento apartado. |
| Atividades para construção da seção | * Identifique palavras e conceitos utilizados na POSIC que mereçam ser explicados. Inclua a lista nesta seção ou crie um documento anexo ou complementar. Veja o modelo mais utilizado na organização. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Gestores responsáveis por políticas de TIC, que já tenham termos definidos; * Áreas envolvidas no conceito ou termo, por exemplo, se há uma área de Auditoria Interna, a mesma pode ajudar na definição do termo conformidade; * Especialistas em segurança da informação da organização. |
| Informações adicionais | * DSIC NC 03 – seção 5.3.2 * ISO/IEC 27000:2016 – Information Technology – Security Techniques – Information Security management systems – Overview and vocabulary |

## Princípios da Segurança da Informação



O tema segurança da informação pode ser desconhecido de muitas pessoas, por isso é necessário apresentar os princípios e a importância do tema. Os princípios regem a segurança da informação na organização e orientam a definição das diretrizes.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique se existe publicado na organização os princípios de segurança da informação; * Verifique se a organização possui outros princípios legais, éticos, de acesso a informação, entre outros, que podem ser referenciados nesta seção. |
| Atividades para construção da seção | * Descreva os princípios de segurança da informação, incluindo os requisitos de confidencialidade, integridade e disponibilidade; * Descreva outros princípios que são pregados pela organização e que tenham relação com a segurança da informação. Podem ser princípios sobre ética, conduta, legislação, acesso à informação, entre outros. |
| Grupos ou áreas que podem ser consultados na construção da seção | * CSIC; * Outras áreas e profissionais que tenham conhecimento técnico da área de segurança da informação. |
| Informações adicionais | * DSIC NC 03 – seção 5.3.4 |

## Diretrizes Gerais



Esta é a parte mais importante da POSIC. Nesta seção devem ser apresentadas as diretrizes para a proteção das informações da organização e para que a segurança seja estabelecida e cumpra seu papel.

No anexo A da ISO 27001 e na ISO 27002 são apresentados os objetivos e controles que devem ser implementados na organização. Este anexo pode ser utilizado como base para o desenvolvimento das diretrizes, porém não é necessário que sejam abordados todos os controles apresentados, pois os mesmos podem ser apresentados em normas específicas sobre o tema.

A Tabela apresenta uma sugestão de temas que podem ter diretrizes declaradas na POSIC. Recomenda-se que o responsável pelo desenvolvimento da POSIC consulte a ISO 27001 e 27002 para analisar a pertinência de outras diretrizes dentro do seu escopo, assim como a Norma Complementar do DSIC nº 03 (item 5.3.5).

|  |  |
| --- | --- |
| Tema | Propostas de conteúdo a ser abordado |
| Uso de e-mail | * Diretrizes sobre o uso do e-mail institucional, inclusive sobre o uso aceitável. |
| Acesso à Internet | * Diretrizes sobre permissões e restrições de acesso à Internet e monitoramento dos acessos. |
| Tratamento da Informação | * Diretrizes relacionadas a necessidade de classificação das informações; * Diretrizes relacionadas ao armazenamento e descarte seguro de informações. |
| Controles de Acesso | * Diretrizes relacionadas a controle de acesso lógico; * Diretrizes relacionadas a controle de acesso físico; * Diretrizes relacionadas a proteção de perímetro. |
| Segurança em Recursos Humanos | * Diretrizes voltadas à área de recursos humanos ou departamento pessoal que tratem sobre inclusão de controles de SI no ciclo de vida de um funcionário na organização. |
| Gestão de Incidentes | * Diretrizes que tratem sobre a necessidade de se estabelecer um processo de gestão de incidentes de SI; * Diretrizes que tratem sobre a necessidade de uma área para tratamento dos incidentes de SI; * Diretrizes voltadas ao usuário sobre a responsabilidade de reporte dos incidentes de SI. |
| Gestão de Riscos | * Diretrizes que apresentem orientações para a gestão de riscos de SI. |
| Gestão de Continuidade | * Diretrizes que tratem sobre a necessidade de se estabelecer um processo de gestão de continuidade. |
| Auditoria e Conformidade | * Diretrizes que definam a necessidade de auditoria de SI e conformidade com requisitos legais, diretrizes e regras de SI. |

Para escrever as diretrizes de cada tema, considere utilizar verbos que representam a obrigatoriedade (deve) e evite os que deixam a escolha para os usuários (convém, recomenda-se).

O conteúdo das diretrizes deve ser mais genérico e menos operacional, definindo apenas a necessidade de criação, desenvolvimento ou aplicação de controles.

Este nível de detalhamento depende da cultura da organização e do formato das políticas. De um modo geral, recomenda-se que o conteúdo das diretrizes esteja focado em fornecer orientações macro, de nível estratégico. As orientações mais específicas poderão ser apresentadas em normas sobre temas específicos e em procedimentos operacionais.

## Responsabilidades



Esta seção deve apresentar as responsabilidades relacionadas à segurança da informação. As responsabilidades estão diretamente relacionadas com as diretrizes e o detalhamento apresentados.

Nesta seção, devem ser definidos a estrutura responsável pelo processo de Gestão de Segurança da Informação, as responsabilidades do Comitê de Segurança da Informação e Comunicações e a institucionalização da Equipe de Tratamento e Resposta a Incidentes da organização.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique se a organização costuma apresentar as responsabilidades aos cargos (diretores, gerentes, coordenadores entre outros) ou as áreas de forma genérica (Pró-reitoria de Extensão, Diretoria de Pesquisa entre outros). |
| Atividades para construção da seção | * Identifique os cargos ou áreas que possuem diretrizes na POSIC relacionadas a eles; * Identifique outras áreas que terão responsabilidade sobre algum aspecto apresentado na POSIC; * Descreva as responsabilidades dos usuários; * Descreva as responsabilidades com a Gestão de Segurança da Informação; * Descreva as responsabilidades do CSIC; * Descreva as responsabilidades da Equipe de Tratamento e Resposta a Incidentes; * Descreva as responsabilidades de forma clara, apresentando a ação que deve ser realizada, por exemplo: revisar, aprovar, apoiar, determinar. |
| Grupos ou áreas que podem ser consultados na construção da seção | * CSIC; * Área de recursos humanos. |
| Informações adicionais | * DSIC NC 03 – seção 5.3.7 * ISO 27001 – seção 5.3 * ISO 27002 – seção 6.1.1 |

## monitoramento e auditoria



A POSIC deve apresentar as diretrizes sobre o monitoramento que será realizado para garantir que as diretrizes estão sendo cumpridas. Também deve apresentar diretrizes sobre a necessidade de auditorias de conformidade.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique se a organização possui uma área de auditoria interna que possa apoiar no processo de monitoramento e auditoria de conformidade; * Identifique se a organização possui um processo de auditoria interna e peça para que o escopo da POSIC seja incluído. |
| Atividades para construção da seção | * Identifique quais ações serão realizadas para o monitoramento do cumprimento das diretrizes, que pode ser através de controles tecnológicos automatizados, monitoramento de acessos entre outros; * Juntamente com o CSIC desenvolva um processo para a realização do monitoramento e da revisão dos resultados; * Insira o escopo da POSIC nas auditorias internas ou, se a organização não tiver um processo de auditoria interna, desenvolva um especificamente para a POSIC; * Defina uma periodicidade para a realização das auditorias e análise dos resultados. Estes resultados serão utilizados como insumo para as melhorias da POSIC e os normativos relacionados. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Auditoria interna; * CSIC. |
| Informações adicionais | * ISO 27001 – seção 9 * ISO 27002 – seção 18.2 |

## Sanções Disciplinares



A POSIC deve prever sanções disciplinares para o caso de descumprimento das diretrizes. As sanções devem estar alinhadas as praticadas pela organização e previstas nos contratos de trabalho e norma administrativas.

É importante que haja um processo aprovado para os casos de descumprimento da POSIC, apresentando as atividades e seus responsáveis. Cabe salientar que este processo deve ser conduzido pela área de recursos humanos, com o apoio da área de Segurança da informação e do CSIC.

Recomenda-se o desenvolvimento de um Termo de Responsabilidade para obter a ciência do usuário sobre a POSIC, a necessidade de segui-la e a possibilidade de aplicação de penalidades pelo seu descumprimento. Este termo deve ser assinado, minimamente, pelos servidores públicos da organização.

|  |  |
| --- | --- |
| Insumos que apoiam o desenvolvimento da seção | * Verifique com a área de recursos humanos como são tratadas as penalidades nos contratos atuais da organização. * Verifique se existe um processo estabelecido para o tratamento de violações das políticas institucionais. |
| Atividades para construção da seção | * Apresente no texto de forma clara que o descumprimento de uma diretriz da POSIC pode acarretar em penalidades. Não é recomendado que a penalidade já esteja descrita no próprio documento. É uma boa prática que cada caso seja analisado separadamente seguindo um processo. |
| Grupos ou áreas que podem ser consultados na construção da seção | * Jurídico; * Área de recursos humanos. |
| Informações adicionais | * DSIC NC 03 – seção 5.3.6 * ISO 27002 – seções 5.1.1, 7.1.2 e 7.2.3 |

# Considerações finais

A POSIC é uma peça fundamental no estabelecimento e amadurecimento da segurança da informação em uma organização. É um documento de caráter estratégico, pois declara o compromisso da alta direção organizacional e provê diretrizes, responsabilidades e o apoio para a proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações da organização.

A elaboração e aprovação de uma POSIC é um desafio para as organizações usuárias, tanto pela dificuldade em obter agenda e apoio da alta direção organizacional, quanto pela complexidade envolvida neste processo.

A RNP, através deste guia, espera apoiar o desenvolvimento da POSIC por suas organizações usuárias, atuando, dessa forma, no fortalecimento da segurança das informações destas, o que, indiretamente, contribuirá também na segurança da Rede Ipê e dos serviços oferecidos através dela.

Adicionalmente o conteúdo apresentado neste documento, a RNP disponibiliza também o documento “Modelo para construção de uma Política de Segurança da Informação e Comunicação (POSIC)” com exemplos de textos para as diretrizes. Recomenda-se a leitura deste material para complementar o conhecimento adquirido ao longo deste guia.

# ANEXO A – CHECKLIST PARA DESENVOLVIMENTO DE UMA POSIC

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Referência no Guia | Informações adicionais | Status |
| PLANEJANDO O DESENVOLVIMENTO DA POSIC | | | |
| Formalização de um grupo de trabalho | 5.1 |  |  |
| Conhecendo a organização | 5.2 | ISO 27001 – seção 4.1 |  |
| Identificando as partes interessadas | 5.3 | ISO 27001 – seção 4.2 |  |
| Identificando o modelo de estrutura normativa | 5.4 | ISO 27001 – seção 7.5 |  |
| DESENVOLVIMENTO, APROVAÇÃO E DIVULGAÇÃO DA POSIC | | | |
| Desenvolvimento do documento | 6.1 | ISO 27001 e 27002  DSIC NC 03 |  |
| Revisão e Aprovação pelo Comitê de SI | 6.2 |  |  |
| Revisão e Aprovação pela Alta Direção Organizacional | 6.3 | ISO 27001 – seção 5.2  DSIC NC 03 – item 6.1 |  |
| Publicação da POSIC | 6.4 | - |  |
| Divulgação da POSIC | 6.5 | DSIC NC 03 – item 7 |  |
| ESTRUTURA MÍNIMA PARA A POSIC | | | |
| Apresentação | 7.1 | - |  |
| Distribuição e atualização | 7.2 | ISO 27001 – seção 7.5.3  DSIC NC 03 – seção 5.3.8 e item 8 |  |
| Índice | 7.3 | - |  |
| Objetivo da POSIC | 7.4 | ISO 27001 – seção 5.2  DSIC NC 03 – seção 5.1 e 5.2 |  |
| Escopo da POSIC | 7.5 | DSIC NC 03 – seção 5.3.1 |  |
| Referências legais e normativas | 7.6 | DSIC NC 03 – seção 5.3.3 |  |
| Conceitos e definições | 7.7 | DSIC NC 03 – seção 5.3.2  ISO/IEC 27000 |  |
| Princípios de SI | 7.8 | DSIC NC 03 – seção 5.3.4 |  |
| Diretrizes gerais | 7.9 | ISO 27002  DSIC NC 03 – seção 5.3.5 |  |
| Responsabilidades | 7.10 | DSIC NC 03 – seção 5.3.7  ISO 27001 – seção 5.3  ISO 27002 – seção 6.1.1 |  |
| Monitoramento e auditoria | 7.11 | ISO 27001 – seção 9  ISO 27002 – seção 18.2 |  |
| Sanções Disciplinares | 7.12 | DSIC NC 03 – seção 5.3.6  ISO 27002 – seção 5.1.1, 7.1.2 e 7.2.3 |  |

# Créditos

**RNP**

Rede Nacional de Ensino e Pesquisa

**Nelson Simões**

*Diretor Geral*

**José Luiz Ribeiro Filho**

*Diretor de Serviços e Soluções*

**Realização:**

**CAIS**

Centro de Atendimento a Incidentes de Segurança da RNP

Liliana Velásquez Solha

*Gerente de Segurança da Informação*

**Desenvolvimento:**

Carla Freitas

Cristiane Rodrigues

Ronald Huppers

Vanessa Suzuki

**Contribuições:**

Afonso Araújo Neto (UFRGS)

Ana Carolina Fukushima (RNP)

Anderson Almeida (RNP)

Christian Lyra (RNP)

Edilson Lima (RNP)

Johnathan Dezan Vago (IFES)

Mário Meyer (RNP)

Yuri Alexandro (RNP)