­­­­

**Modelos para construção de uma Política de Segurança da Informação e Comunicações (POSIC)**

**CAIS/RNP**

**APRESENTAÇÃO**

Este documento apresenta modelos de texto que podem ser utilizados pelas organizações usuárias da RNP para redigir a Política de Segurança da Informação e Comunicação (POSIC).

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

Este documento complementa o conteúdo do Guia para Desenvolvimento de uma Política de Segurança da Informação e Comunicações, também de autoria da RNP, exemplificando as orientações e dicas apresentadas.

**SUMÁRIO**

[1. Objetivo 4](#_Toc469567229)

[2. Referências 4](#_Toc469567230)

[3. Exemplos de texto para POSIC 4](#_Toc469567231)

[3.1. APRESENTAÇÃO 5](#_Toc469567232)

[3.2. Distribuição e atualização 6](#_Toc469567233)

[3.3. Índice 7](#_Toc469567234)

[3.4. Objetivo da POSIC 7](#_Toc469567235)

[3.5. escopo da POSIC 7](#_Toc469567236)

[3.6. Referências legais e normativas 8](#_Toc469567237)

[3.7. Conceitos e definições 9](#_Toc469567238)

[3.8. Princípios da Segurança da Informação 11](#_Toc469567239)

[3.9. Diretrizes Gerais 13](#_Toc469567240)

[3.10. Responsabilidades 21](#_Toc469567241)

[3.11. monitoramento e auditoria 24](#_Toc469567242)

[3.12. Sanções Disciplinares 25](#_Toc469567243)

[4. Considerações Finais 27](#_Toc469567244)

# Objetivo

O objetivo deste documento é apresentar modelos de texto para cada um dos tópicos necessários para a elaboração de uma Política de Segurança da Informação e Comunicação (POSIC) alinhados com o Guia para desenvolvimento de uma Política de Segurança da Informação e Comunicações, auxiliando assim as Instituições no desenvolvimento deste importante instrumento normativo.

# 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;
* Guia para desenvolvimento de uma Política de Segurança da Informação e Comunicações;
* Norma complementar nº 03/IN01/DSIC/GSIPR de 3 de julho de 2009 – Departamento de Segurança da Informação e Comunicações.

# Exemplos de texto para POSIC

Está seção apresenta no máximo três exemplos de diretrizes para a elaboração da POSIC de forma alinhada e integrada ao Guia para desenvolvimento de uma Política de Segurança da Informação e Comunicações, as melhores práticas e normativos relacionados ao tema.

Os exemplos apresentados podem ser usados livremente, porém recomenda-se que cada instituição os utilize como referência e customize as diretrizes de acordo com suas necessidades e realidade. Inclusive, alguns exemplos não são excludentes e a organização pode adotar mais de uma proposta sugerida.

## APRESENTAÇÃO

|  |  |
| --- | --- |
| Modelo 1 | A reitoria da <Nome da Instituição> formaliza e aprova a Política de Segurança da Informação e Comunicação (POSIC) com a finalidade de estabelecer diretrizes sobre o tema alinhadas aos requisitos de negócio, obrigações legais, regulamentações e objetivos estratégicos da organização.  A segurança da informação, na visão desta política, está diretamente ligada a preservação da confidencialidade, integridade e disponibilidade das informações da <Nome da Instituição> ou sob a sua responsabilidade, bem como a confiabilidade, autenticidade, não repúdio e outros requisitos aplicáveis.  A segurança da informação é responsabilidade de todos aqueles que direta ou indiretamente, têm acesso ou manipulam informações.  A reitoria da <Nome da Instituição> declara-se comprometida em proteger os ativos de informação da organização, apoiando as metas e princípios da segurança da informação estabelecidos nesta POSIC. |
| Modelo 2 | A Política de Segurança da Informação e Comunicação da <Nome da Instituição> observará os princípios, objetivos e diretrizes, bem como as disposições constitucionais, legais e regimentais vigentes.  Integram a esta POSIC normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinados à proteção da informação. |
| Modelo 3 | A Política de Segurança da Informação e Comunicação – POSIC da <Nome da Instituição> é uma declaração formal do compromisso com a segurança das informações.  A POSIC é direcionada a todos os agentes públicos, alunos, colaboradores e prestadores de serviço que atuam na <Nome da Instituição> e acessam a sua estrutura de Tecnologia da Informação. |

## Distribuição e atualização

|  |  |
| --- | --- |
| Modelo 1 | A Política de Segurança da Informação e Comunicação (POSIC) deve ser de ciência de todos os agentes públicos, alunos, colaboradores e prestadores de serviço da <Nome da Instituição>.  Este documento, juntamente com os seus anexos, entra em vigor imediatamente após a sua publicação e revoga as versões anteriores, se houver.  O prazo de validade da POSIC é indeterminado e as suas revisões devem ser realizadas a cada <XX> anos, considerando a validade ou mudanças nos requisitos legais ou mudança da <Nome da Instituição> ou governamentais. |
| Modelo 2 | A POSIC deve ser de conhecimento de toda a comunidade universitária da <Nome da Instituição>.  Está POSIC deverá ser revisada e atualizada a cada <XX> anos após a sua publicação ou quando for identificada a necessidade pelo <Comitê de Segurança da Informação / área de Segurança da Informação>. |
| Modelo 3 | A Política de Segurança da Informação e Comunicação (POSIC) deve ser divulgada a todos os servidores da <Nome da Instituição> e publicada de forma que o seu conteúdo possa ser consultado a qualquer momento.  Todos os normativos relacionados à segurança da informação, incluindo a POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de <XX> anos. |

## Índice

O índice deve representar as divisões das seções para que o leitor possa encontrar um tema específico com maior facilidade. Dependendo do aplicativo utilizado na edição da POSIC, o índice é gerado automaticamente.

## Objetivo da POSIC

|  |  |
| --- | --- |
| Modelo 1 | Fica estabelecida a Política de Segurança da Informação e Comunicação (POSIC) da <Nome da Instituição>, contendo as diretrizes de segurança da informação a serem observadas no âmbito desta instituição, assim como as responsabilidades, competências na implementação da gestão de segurança da informação, buscando assegurar a disponibilidade, integridade e confidencialidade das informações. |
| Modelo 2 | A Política de Segurança da Informação e Comunicação (POSIC) alinha-se às estratégias da <Nome da Instituição> e tem por objetivo garantir a autenticidade, a confidencialidade, a disponibilidade, a integridade e demais requisitos das informações produzidas ou custodiadas. |
| Modelo 3 | A Política de Segurança da Informação e Comunicação (POSIC) tem como objetivo definir um conjunto de regras para assegurar que os requisitos de segurança (disponibilidade, confidencialidade e integridade) das informações que suportam os serviços, processos e atividades da <Nome da Instituição> sejam implementados. |

## escopo da POSIC

|  |  |
| --- | --- |
| Modelo 1 | A POSIC aplica-se a todos os agentes públicos, alunos, colaboradores e prestadores de serviço <Nome da Instituição>. |
| Modelo 2 | A POSIC aplica-se à comunidade acadêmica e demais usuários que possuem interação com os ativos de informação da <Nome da Instituição>. |
| Modelo 3 | A Política de Segurança da Informação e Comunicações (POSIC) se aplica a todas as unidades administrativas, servidores, estudantes, prestadores de serviço e demais usuários da instituição. |

## Referências legais e normativas

|  |  |
| --- | --- |
| Modelo 1 | Para a elaboração desta POSIC foram utilizadas as seguintes referências:   * ABNT NBR ISO/IEC 27001:2013 – Sistemas de gestão de segurança da informação – Requisitos; * ABNT NBR ISO/IEC 27002:2013 - Código de prática para segurança da informação; * DSIC/GSI/PR - Norma complementar nº 03 – Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. |
| Modelo 2 | * IN 01/DSIC/GSI/PR – Disciplina a gestão de segurança da informação e comunicações na APF e dá outras providências. * NC 03/IN01/DSIC/GSI/PR – Diretrizes para elaboração de política de segurança da informação nos órgãos e entidades da APF. * NC 04/IN01/DSIC/GSI/PR – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos e entidades da APF. * NC 05/IN01/DSIC/GSIPR – Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais nos órgãos e entidades da APF. * NC 10/IN01/DSIC/GSIPR – Diretrizes para o processo de inventário e mapeamento de ativos de informação, para apoiar a segurança da informação e comunicações. * NC 11/IN01/DSIC/GSIPR – Diretrizes para avaliação de conformidade nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da APF. * NC 16/IN01/DSIC/GSIPR – Estabelece diretrizes para o desenvolvimento e obtenção de software seguro nos órgãos e entidades da APF. * NC 20/IN01/DSIC/GSIPR – Diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da APF. * ABNT NBR ISO/IEC 27001:2013 – Sistemas de gestão de segurança da informação – Requisitos. * ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação. |
| Modelo 3 | As referências legais e normativas apresentadas nesta POSIC e em seus normativos estão definidos no documento “Anexo B – Referências Legais e Normativas para a Segurança da Informação”. |

## Conceitos e definições

|  |  |
| --- | --- |
| Modelo 1 | Nesta Política são utilizadas as seguintes definições:   * Ameaça – causa potencial de um incidente de segurança, que pode resultar em dano para um ativo da instituição; * Ativo – qualquer bem, tangível ou intangível, que possui valor para a instituição; * Autenticidade – garantia da veracidade da fonte da informação; * Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoas, processos não autorizados; * Cópia de segurança (backup) – imagem fiel de um ativo (documento, arquivo, sistema, outros) que possa ser restaurado em caso de impossibilidade de acesso ao original; * Disponibilidade – propriedade da informação estar acessível para pessoas, sistemas e serviços autorizados, sempre que necessário; * Evento de segurança da informação – ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da POSIC ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação; * Gestor do ativo – membro da instituição responsável pela segurança de um determinado ativo; * Incidente de segurança da informação – ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança das informações no que tange a confidencialidade, integridade ou disponibilidade; * Integridade - propriedade de salvaguarda da exatidão e completeza da informação. A certeza de que uma informação não foi modificada de forma não autorizada; * Risco de segurança da informação - combinação entre a probabilidade de ocorrência de um incidente de segurança e as suas consequências; * Segurança da Informação – preservação da confidencialidade, integridade e disponibilidade da informação que estão sob responsabilidade da instituição; * Usuário – servidores, aposentados, discentes, terceirizados, colaboradores, consultores, auditores, agentes públicos, alunos, estagiários, bolsistas, pesquisadores, visitantes, empresas, organizações ou qualquer agente público que tenha o acesso aos ativos autorizados pelo responsável do ativo; * Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. |
| Modelo 2 | Os termos e definições apresentados nesta POSIC e em seus normativos estão definidos no documento “Anexo A – Termos e Definições para a Segurança da Informação”. |

## Princípios da Segurança da Informação

|  |  |
| --- | --- |
| Modelo 1 | A segurança da informação e comunicação da <Nome da Instituição> tem como base os seguintes princípios:   * Responsabilidade – preservar e tratar de maneira adequada, de acordo com sua classificação, a informação bem como preservar e zelar pelos ativos; * Clareza – as diretrizes que são apresentadas na POSIC devem ser claras, objetivas e concisas a fim de viabilizar a sua compreensão por todos aqueles que tiverem acesso a ela; * Publicidade – dar transparência às informações, respeitando a legislação, privacidade e a classificação da informação.   Está POSIC deve estar também em conformidade com a constituição e administrativos que regem a Administração Pública Federal, bem como os demais dispositivos legais aplicáveis. |
| Modelo 2 | Os princípios que regem a segurança da informação e comunicação da <Nome da Instituição>, no âmbito dos serviços, recursos e das informações estão relacionados a:   * Autenticidade – propriedade de ser genuíno e apto a ser verificável e confiável; * Confidencialidade – garantia que a informação esteja disponível, ou seja, revelada somente a usuários ou processo autorizados; * Disponibilidade – a propriedade de um sistema ou recurso de estar acessível ou utilizável sob demanda do usuário; * Integridade – a propriedade de assegurar que as informações não foram alteradas, perdidas ou destruídas de maneira não autorizada ou acidental; * Legalidade – a propriedade de garantir a obediência aos princípios constitucionais, administrativos e à legislação vigente. |
| Modelo 3 | * + Princípio dos Requisitos de Segurança da Informação   A POSIC da <Nome da Instituição> visa proteger os requisitos de confidencialidade, integridade, disponibilidade e autenticidade das informações, além de outros requisitos estabelecidos como auditabilidade, preservação (pelo prazo que a lei, ou a própria organização fixar) e não repúdio.   * + Princípio do Respeito e Conformidade com a Legislação e Código de Ética   A POSIC não se sobrepõe à legislação brasileira vigente. Nenhuma diretriz de segurança da informação deve ser contrária a Lei, jurisprudência.   * + Princípio do Respeito ao Ser Humano   A POSIC tem como princípio o respeito à dignidade do ser humano e à privacidade dos usuários da <Nome da Instituição>.   * + Princípio da Eficiência dos Processos e Alcance dos Objetivos   A implementação de diretrizes e regras de segurança da informação deve permitir o pleno e seguro atendimento da missão da <Nome da Instituição>, o alcance dos objetivos estratégicos e a operacionalização eficiente dos processos.   * + Princípio do Acesso à Informação   As diretrizes, regras ou controles de segurança da informação não se sobrepõem ao Princípio da Publicidade que estabelece a necessidade da divulgação de informações para fins de transparência, prestação de contas e fiscalização. Ressalta-se que qualquer nível de restrição de acesso à informação deve estar amparado neste princípio, na legislação vigente e nas diretrizes a serem estabelecidas para a classificação da informação da <Nome da Instituição>. |

## Diretrizes Gerais

|  |  |
| --- | --- |
| Uso de e-mail | |
| Modelo 1 | O e-mail da organização é ferramenta de comunicação e apenas como tal deve ser utilizada, sendo permitida sua utilização para fins pessoais, desde que não infrinja as regras contidas nesta política, em suas normas complementares ou legislação aplicável.  Critérios para concessão de acesso ao e-mail, padrões de nomenclatura dos e-mails, período de retenção de mensagens e demais características do serviço devem ser definidas pela área de TIC e serem comunicadas para a organização sempre que alguma mudança ocorrer e que possa afetar diretamente o usuário.  Não é permitida, em nenhuma circunstância, a divulgação dos endereços eletrônicos dos usuários da organização sem a devida anuência destes. |
| Modelo 2 | O e-mail é disponibilizado como ferramenta de apoio aos alunos, docentes e servidores no cumprimento de seus objetivos nas áreas de educação, pesquisa, extensão e demais serviços da organização.  O uso pessoal poderá ser permitido, salientando que o uso é passível de auditoria e monitoramento e que deve ser utilizado com cautela, considerando as diretrizes contidas na POSIC e demais normativos e principalmente a legislação vigente e a ética. |
| Modelo 3 | O e-mail é disponibilizado como ferramenta de apoio e comunicação, sendo vetado o uso para fins pessoais, conforme legislação vigente e as diretrizes contidas nesta POSIC. O uso do e-mail será monitorado e é passível de auditoria. |

|  |  |
| --- | --- |
| Acesso à Internet | |
| Modelo 1 | O acesso à Internet da <Nome da Instituição> deve ser regido por norma específica, atendendo às determinações desta POSIC, e demais orientações governamentais e legislação em vigor.  Todo o conteúdo acessado pelos usuários poderá ser monitorado e gravado para futuras averiguações.  O uso da Internet para fins pessoais é permitido conforme orientação do gestor. É proibido acessar sites com conteúdo relacionado a crimes, drogas, pornografia, pedofilia, racismo, difamação, entre outros. |
| Modelo 2 | Todos os alunos, docentes e servidores têm o direito de acesso à internet, com utilização exclusiva para fins de complementação às suas atividades, para o enriquecimento intelectual ou como ferramenta de busca por informações que venham a contribuir para o desenvolvimento de seus trabalhos.  O acesso à internet deve ser controlado e limitado ao necessário, considerando as atribuições de cada usuário, onde qualquer outra forma de uso ou acesso requer prévia autorização do gestor da área responsável pela informação.  É proibido acessar sites com conteúdo relacionado a crimes, drogas, pornografia, pedofilia, racismo, difamação, entre outros. |
| Modelo 3 | O acesso à Internet deve restringir-se à execução de atividades acadêmicas e administrativas e exclusivamente por meio de softwares homologados pela área de TIC. O uso da Internet para fins pessoais não é permitido.  A área de TIC deve prover mecanismos para que os usuários acessem a Internet de maneira segura, incluindo o uso de softwares de monitoramento e registro das atividades dos usuários. É proibido acessar sites com conteúdo relacionado a crimes, drogas, pornografia, pedofilia, racismo, difamação, entre outros. |

|  |  |
| --- | --- |
| Tratamento da Informação | |
| Modelo 1 | Toda informação sob responsabilidade da <Nome da Instituição> é considerada um bem e deve ser protegida de acordo com as diretrizes descritas nesta POSIC, normas e demais regulamentações em vigor, com o objetivo de minimizar os riscos que afetem os requisitos de segurança das informações e preservando a imagem da instituição.  As informações críticas devem possuir cópia de segurança atualizada e essa cópia deve ser testada periodicamente. |
| Modelo 2 | Deve-se implementar procedimentos para tratamento, armazenamento, identificação, classificação e descarte das informações da <Nome da Instituição> para assegurar a integridade, disponibilidade e confidencialidade das informações.  As informações críticas devem possuir cópia de segurança atualizada e essa cópia deve ser testada periodicamente. |
| Modelo 3 | As regras para as operações de armazenamento, divulgação, reprodução e destruição da informação devem ser definidas na norma de classificação da informação.  Todas as informações devem possuir cópia de segurança atualizada e essa cópia deve ser testada periodicamente. |

|  |  |
| --- | --- |
| Controle de Acesso Lógico | |
| Modelo 1 | O acesso a informação será regulamentado por normas específicas onde toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela organização é considerada seu patrimônio e deve ser passível de proteção e monitoramento. |
| Modelo 2 | As regras de controle de acesso a todos os sistemas da instituição deverão ser definidas e regulamentadas, através de norma a ser desenvolvida, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da <Nome da Instituição>  Todo acesso às informações deve ser controlado de forma a garantir que apenas pessoas autorizadas, pelo respectivo proprietário da informação, tenham acesso. |
| Modelo 3 | A gestão de acessos a informação deverá obedecer ao princípio de menor privilégio possível, podendo os usuários terem acesso à não mais do que as informações e recursos computacionais necessários para o pleno desenvolvimento de suas atividades acadêmicas e/ou administrativas.  As credenciais de acesso concedidas aos usuários são pessoais e intransferíveis, podendo seu uso ser auditado e monitorado, não devendo o usuário conceder suas credenciais a terceiro sob quaisquer circunstâncias.  Visitantes que necessitarem acessar à Internet, porém, poderão fazê-lo por meio de solicitação formal, devidamente autorizada pelo gestor da área visitada, com período de acesso previamente definido. |

|  |  |
| --- | --- |
| Controle de Acesso Físico e proteção do perímetro | |
| Modelo 1 | O acesso às dependências da organização deve ser controlado e monitorado. O porte e uso das devidas credenciais de acesso, as quais são pessoais, únicas e intransferíveis, devendo estas permitir de maneira clara e inequívoca o reconhecimento de seu detentor.  Os ativos de TI da <Nome da Instituição> devem ser mantidos em áreas seguras, protegidos por um perímetro de segurança, com barreiras apropriadas e recursos para controle de acesso conforme regras a serem estabelecidas em norma específica sobre o tema. |
| Modelo 2 | As instalações físicas, estações de trabalho, servidores, softwares e demais equipamentos de TIC da <Nome da Instituição> devem ser protegidos contra acessos indevidos e riscos de indisponibilidade.  Os servidores devem ser mantidos em áreas protegidas por controle de acesso, conforme regras a serem definidas em norma específica. |
| Modelo 3 | A instituição deve implementar controles para monitorar o acesso físico ao ambiente, equipamentos, documentos de modo que a segurança seja mantida, restringindo o acesso a apenas usuários autorizados, as regras e controles devem ser definidos e norma específica sobre o tema.  Locais considerados críticos devem possuir métodos de controle de acesso rígido, de modo que somente pessoas autorizadas e acompanhadas possam ter acesso. Os acessos devem ser registrados e as autorizações devem ter tempo determinado, o controle de acesso deve ser preferencialmente de forma eletrônica, através de biometria ou cartões de acesso e senha. |

|  |  |
| --- | --- |
| Segurança em Recursos Humanos | |
| Modelo 1 | Os usuários da <Nome da Instituição> devem ter ciência de suas responsabilidades e obrigações relacionadas a POSIC e demais normativos complementares, assim como cumprir está política.  Devem ser estabelecidos processos e procedimentos relacionados a disseminação da cultura em segurança da informação, ao ciclo de vida dos usuários da instituição e responsabilidades atreladas a cada processo. |
| Modelo 2 | <Nome da Instituição> deve definir regras, em normativo específico, no que diz respeito ao ciclo de vida dos usuários na instituição desde a contratação/início do curso até o desligamento/término do curso, incluindo as movimentações e promoções, como também o processo de coleta do termo de ciência / responsabilidade em relação à está política e demais normativos.  Deve prever como será a disseminação da cultura de segurança da informação na instituição. |
| Modelo 3 | As responsabilidades em relação à segurança da informação devem ser comunicadas na fase de contratação dos <colaboradores, servidores>. Estes devem ser orientados a seguir as diretrizes desta política e de suas normas complementares, assinando um termo de ciência que deverá ficar de posse do departamento pessoal.  É responsabilidade do gestor do usuário ou do contrato, em conjunto com o departamento pessoal, informar a área de TIC sobre o desligamento de um colaborador, servidor ou término de um contrato para que as credenciais de acesso sejam devidamente revogadas. Para os alunos é de responsabilidade da <secretaria/departamento xx> informar a área de TIC sobre o cancelamento das atividades escolares após X meses após o término do curso.  Como forma de manter os usuários atualizados quanto às normas de segurança da informação, é responsabilidade da área <a definir pela instituição> em conjunto com o gestor de segurança da informação, implementar um plano de treinamentos e conscientização permanente na organização, inclusive avaliando a eficácia destes treinamentos frente aos controles de segurança implementados e eventuais incidentes de segurança da informação ocorridos. |

|  |  |
| --- | --- |
| Gestão de incidentes de segurança | |
| Modelo 1 | Os incidentes de segurança da informação devem ser identificados, registrados, tratados e monitorados. As regras e controles devem ser definidos em norma e processo específico sobre o tema.  Os usuários devem ser estimulados a reportar os incidentes, atividades ou comportamentos suspeitos, assim como o não cumprimento desta política e demais normativos de segurança da informação ao <informe o canal>. |
| Modelo 2 | Na <Nome da Instituição>, uma equipe irá receber, filtrar, classificar, analisar e responder os incidentes de segurança conforme regras definidas em norma específica para o tema. |
| Modelo 3 | Todo e qualquer incidente de segurança da informação deve ser comunicado imediatamente. Os incidentes devem ser identificados, registrados, respondidos e monitorados por uma equipe capacitada para este fim através de um processo formal e de conhecimento de toda a organização. |

|  |  |
| --- | --- |
| Gestão de Riscos de Segurança da Informação | |
| Modelo 1 | A <Nome da Instituição> deve estabelecer um processo de Gestão de Risco de Segurança da Informação contínuo e estruturado.  Os riscos de segurança da informação devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto. |
| Modelo 2 | Deve ser implementado e mantido um processo de gestão de riscos de segurança da informação visando minimizar impactos nos processos da instituição.  Os ativos de informação a serem protegidos deverão ser priorizados, de acordo com o mapa de risco, bem como a definição e implantação de controles para a o tratamento dos riscos. |
| Modelo 3 | Os riscos relativos à informação devem ser gerenciados de modo a reduzir vulnerabilidades e impactos referentes aos ativos de informação.  A gestão de riscos de segurança da informação deve ser implementada por meio de planejamento de segurança fundamentado em desenvolvimento de cultura corporativa para riscos, qualificação de pessoas, desenvolvimento de procedimentos e implantação de tecnologia e recursos. |

|  |  |
| --- | --- |
| Gestão de Continuidade dos Negócios | |
| Modelo 1 | O processo de gestão de continuidade de negócios deve ser desenvolvido para gerenciar e manter em funcionamento os serviços e processos críticos da <Nome da Instituição>, na ocorrência de desastres, falhas ou incidentes.  Os planos devem ser desenvolvidos com base na análise de riscos de segurança da informação. |
| Modelo 2 | O processo de gestão da continuidade de negócios deve ser implementado, mantido e testado periodicamente visando reduzir, para um nível aceitável, o tempo de interrupção causado por um desastre ou falhas nos recursos que suportam os ativos da organização. |
| Modelo 3 | A <Nome da Instituição> devem manter planos de continuidade de negócios, atualizados e testados periodicamente, a fim de evitar que os processos e atividades críticas sejam interrompidas por um desastre ou incidente. A instituição deve estabelecer as regras para a continuidade dos negócios em norma específica. |

## Responsabilidades

|  |  |
| --- | --- |
| Usuários da <Nome da Instituição> | * Desenvolver as suas atividades seguindo as diretrizes e definições da Política de Segurança da Informação e Comunicação (POSIC) e demais normativos relacionados ao tema; * Assinar o termo de responsabilidade para o uso dos recursos tecnológicos da instituição; * Reportar os incidentes de segurança através dos meios divulgados pela instituição; * Ter ciência, compreender e aplicar as diretrizes e regras estabelecidas na POSIC; * Tratar as informações como patrimônio da <Nome da Instituição>, e como tal, preservar pela confidencialidade, disponibilidade e integridades das informações, não divulgando para pessoas não autorizadas; * Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas credenciais e senhas a outros usuários. |
| Chefia da <Nome da Instituição> | * Gerenciar o cumprimento da POSIC e demais da <Nome da Instituição> por parte de seus subordinados; * Identificar os desvios praticados e adotar medidas corretivas, quando necessário; * Proteger, em nível físico e lógico, os ativos que estão sob a sua responsabilidade; * Garantir que os usuários sob a sua responsabilidade receberam o devido treinamento em relação à segurança da informação e comunicação; * Aplicar, quando necessário, em conjunto com a área de pessoal as medidas disciplinares, conforme legislação vigente; * Autorizar o acesso as informações sob sua responsabilidade; * Requisitar auditoria nos processos envolvidos com a POSIC no intuito de aferir o nível de segurança da informação, violações de segurança e não conformidades; * Classificar as informações quanto à confidencialidade no momento em que a informação for produzida ou obtida. |
| Responsável pelo Departamento Pessoal | * Apoiar na aplicação de sanções disciplinares; * Obter dos usuários a assinatura do termo de ciência / responsabilidade; * Apoiar no processo de disseminação da cultura em segurança da informação, quando aplicável; * Definir, nas descrições de cargos e funções, as responsabilidades dos servidores pela manutenção das ações de segurança da informação e comunicação; * Promover a ambientação / integração de todo servidor, por meio de treinamento e capacitação no tema segurança da informação e comunicação. |
| Comitê de Segurança da Informação | * Propor o desenvolvimento de Normas e Procedimentos relativos à segurança da informação e comunicações na instituição; * Apresentar proposta de revisão da POSIC e demais normativos, de forma a mantê-los sempre atualizados e de acordo com a legislação vigente; * Assessorar a reitoria / diretoria geral nos assuntos relativos a segurança da informação e comunicação; * Construir grupos de trabalho para tratar temas e propor soluções específicas sobre Segurança da Informação e Comunicações; * Elaborar proposta e promover um Plano de Gestão de Riscos que inclua um Plano de Gestão de Incidentes de Segurança da Informação e um Plano de Continuidade de Negócio, com medidas que garantam a continuidade das atividades da <Nome da Instituição> em caso de desastre ou falhas nos recursos que suportam os processos vitais de negócio. |
| Gestor de Segurança da Informação | * Presidir o Comitê de Segurança da Informação; * Promover a disseminação da cultura de segurança da informação e comunicação na instituição; * Atuar na investigação e tratamento de incidentes de segurança da informação; * Propor recursos necessários para as ações de segurança da informação; * Manter o sistema normativo de segurança da informação e comunicação sempre atualizado, mantendo a melhoria contínua; * Realizar a gestão de riscos e continuidade dos negócios na instituição. |
| Reitoria / Diretoria Geral | * Aprovar a POSIC e demais normativos relacionados à segurança da informação e comunicação; * Promover a disseminação da cultura de segurança da informação e comunicação na instituição; * Prover os recursos necessários para a implementação dos controles e ações de segurança da informação e comunicação na instituição; * Indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes. |

## monitoramento e auditoria

|  |  |
| --- | --- |
| Modelo 1 | O cumprimento da POSIC e demais normativos relacionados à segurança da informação e comunicação da <Nome da Instituição> devem ser auditados pela área de Segurança da Informação.  A <Nome da Instituição> poderá monitorar os acessos dos usuários, incluindo o acesso à internet e uso do correio eletrônico, conforme necessidade e aprovação do gestor imediato. |
| Modelo 2 | Para efeitos de verificação do cumprimento das diretrizes e regras de segurança da organização a <Nome da Instituição> poderá monitorar os acessos dos usuários aos sistemas corporativos, e-mail e à Internet, mediante decisão e autorização da <Reitoria/Alta Gestão>.  O cumprimento da POSIC e das normas deverá ser avaliado a cada <X anos> por meios de auditorias de conformidade, conforme regras a serem estabelecidas em norma específica sobre o tema. |
| Modelo 3 | A <Nome da Instituição> irá monitorar, automaticamente, todos os acessos dos usuários aos sistemas da instituição.  Deve ser realizada, periodicamente, verificação de conformidade das práticas de segurança da informação da <Nome da Instituição> com a POSIC, normas, processos e procedimentos complementares, bem como com a legislação vigente.  É vedado aos usuários realizar a condução de verificação de conformidade dos processos aos quais está envolvido ou vinculado. |

## Sanções Disciplinares

|  |  |
| --- | --- |
| Modelo 1 | A não observância das diretrizes da POSIC da <Nome da Instituição> pode acarretar, isoladamente ou cumulativamente, nos termos da legislação vigente em sanções administrativas, civis e/ou penais. |
| Modelo 2 | O descumprimento ou violação pelo usuário das diretrizes previstas na POSIC ou nos normativos poderá resultar na aplicação de punições previstas nos regulamentos internos, em sanções administrativas ou na legislação em vigor. |
| Modelo 3 | A violação da POSIC da <Nome da Instituição> e demais normativos relacionados à segurança da informação e comunicação poderá resultar em ação disciplinar, apoiada na legislação vigente e regulamentos internos.  Docentes usuários administrativos estão sujeitos a Lei no 8.112/1990 que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. No Artigo 127 estão listadas as penalidades aplicáveis, a saber:  I. advertência;  II. suspensão;  III. demissão;  No caso de alunos, resoluções específicas devem ser aprovadas para que membros do corpo discente sofram punições em caso de violação das normas de segurança de informação. As penalidades devem variar de advertência ao desligamento da Universidade, sem prejuízo de outras sanções legais. |

# Considerações Finais

Este documento apresenta um conjunto de modelos para a elaboração de uma POSIC pelas organizações usuárias da RNP. Espera-se que este documento, utilizado em conjunto com o Guia para desenvolvimento de uma POSIC, possa contribuir na construção das diretrizes de acordo com as necessidades de cada instituição.

Este modelo pode ser utilizado livremente e não deve ser a única fonte de consulta. Recomenda-se que o responsável pela elaboração da POSIC consulte políticas de outras instituições, especialmente das que atuam no mesmo segmento de negócio de sua instituição. A troca de experiência com gestores de outras organizações também será um importante insumo para a construção da POSIC, assim como a consulta a boas práticas como a ABNT NBR ISO/IEC 27002 e a observância às regulamentações do DSIC/GSI/PR.

É importante observar também que as diretrizes de segurança da informação devem reduzir os riscos relacionados a suas informações, protegendo seus requisitos de segurança. Um controle restritivo deve ser justificado como forma de mitigação de um risco de segurança existente.

Por fim, neste documento, foram detalhadas diretrizes genéricas, que se aplicam praticamente a todos os ambientes, cabendo a cada responsável pelo desenvolvimento da POSIC customizá-las de acordo com a realidade de sua instituição.