



**Universidade Federal da Bahia**

**Comitê de Segurança da Informação e Comunicações – CSIC**

**Política de Segurança da Informação e Comunicações – PoSIC**


Código: P.POSIC.001

Revisão: 1.3.0

Última aprovação pelo CSIC em: 11/06/2018


Classificação:  
**Uso Interno**

**Salvador – BA**


|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 2 / 37             |

## Sumário

|  |    |
|--|----|
| Apresentação   | 4  |
| Objetivo e Abrangência                                       | 4  |
| Referências Legais e Normativas                              | 5  |
| Conceitos e Definições                                       | 5  |
| Princípios da Política de Segurança                          | 5  |
| Diretrizes Gerais  | 7  |
| Diretrizes Específicas                                       | 8  |
| 7.2 Gestão de Ativos da Informação                           | 8  |
| 7.3 Gestão de Riscos   | 9  |
| 7.4 Segurança Física e do Ambiente                           | 10 |
| 7.6 Gestão de Operações e Comunicações                       | 10 |
| 7.7 Controles de Acesso                                      | 11 |
| 7.8 Criptografia   | 12 |
| 7.9 Aquisição, Desenvolvimento e Manutenção de Sistemas      | 12 |
| 7.10 Segurança nas operações                                 | 12 |
| 7.11 Gestão de Incidentes de Segurança da Informação         | 15 |
| 7.12 Gestão de Continuidade do Negócio                       | 15 |
| 7.13 Auditoria e Conformidade                                | 15 |
| 7.14 Plano de Investimentos em SIC                           | 16 |
| 7.15 Propriedade Intelectual                                 | 16 |
| 7.16 Contratos, Convênios, Acordos e Instrumentos Congêneres | 17 |
| 7.17 Uso de Recursos e Serviços de TIC                       | 17 |
| 7.18 Acesso à Internet                                       | 17 |

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 3 / 37             |

|      |   |    |
|------|---|----|
| 7.19 | Uso de Equipamentos Computacionais Pessoais                                 | 18 |
| 7.20 | Uso de Mídias Removíveis  | 18 |
| 8    | Penalidades   | 19 |
| 9    | Competências e Responsabilidades  | 19 |
| 9.1  | Cabe ao Comitê de Governança Digital  | 19 |
| 9.2  | Cabe à área de Gestão de Segurança da Informação e Comunicações             | 19 |
| 9.3  | Cabe ao Comitê de Segurança da Informação e Comunicações                    | 20 |
| 9.4  | Cabe à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais | 21 |
| 9.5  | Cabe aos gestores dos ativos de informação                                  | 22 |
| 9.6  | Cabe aos custodiantes de ativos de informação                               | 22 |
| 9.7  | Cabe aos titulares das unidades da UFBA                                     | 22 |
| 9.8  | Cabe aos terceiros, fornecedores e prestadores de serviço                   | 23 |
| 9.9  | Cabe aos gestores de pessoal  | 23 |
| 9.10 | Cabe a todos os usuários dos ativos de informação da UFBA                   | 24 |
| 10   | Divulgação e Atualização  | 24 |
| 11   | Disposições Finais  | 25 |
|      | Anexo I – Referências Legais e Normativas aplicáveis à                      | 26 |
|      | Anexo II – Termos e Definições do Sistema Normativo de                      | 32 |
|      | Anexo III – Termo de Responsabilidade                                       | 36 |


|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 4 / 37             |

## 1 Apresentação

1.1 Esta Política de Segurança da Informação e Comunicações – PoSIC, elaborada pelo Comitê de Segurança da Informação e Comunicações – CSIC, e aprovada pelo Comitê de Governança Digital da Universidade Federal da Bahia, define as diretrizes gerais de Segurança da Informação e Comunicações – SIC no âmbito desta instituição, visando a preservação da disponibilidade, integridade, confidencialidade e autenticidade dos seus ativos de informação.

## 2 Objetivo e Abrangência

- 2.1 Esta PoSIC tem por objetivo fornecer as diretrizes gerais de SIC da Universidade Federal da Bahia, como parte integrante do seu Sistema de Gestão de Segurança da Informação – SGSI, instituído pela Portaria Nº 592/2011, e de acordo com a legislação vigente.
- 2.2 As diretrizes de SIC descritas neste documento consideram, prioritariamente, os objetivos estratégicos, processos, requisitos legais e a estrutura organizacional da UFBA, e não se limitam apenas a aspectos de tecnologia da informação.
- 2.3 Além desta PoSIC, integram o conjunto de documentos de apoio à SIC as normas e os procedimentos complementares, destinados à proteção dos ativos de informação nos níveis tático e operacional, respectivamente.
- 2.4 As diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta PoSIC devem ser observados e cumpridos em todo o âmbito da UFBA, nas suas diversas instâncias.
- 2.5 As diretrizes desta PoSIC, assim como o disposto nas normas e procedimentos complementares, aplicam-se a servidores, alunos, bolsistas, estagiários, prestadores de serviço, visitantes, colaboradores, consultores externos e a quem, de alguma forma, execute atividades vinculadas a esta Universidade.
- 2.6 Todos aqueles mencionados no item anterior são responsáveis pela proteção dos ativos de informação de propriedade ou custodiados pela UFBA, e devem estar comprometidos com o cumprimento desta PoSIC e seus documentos complementares.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 5 / 37             |

2.7 Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela UFBA devem atender às determinações dispostas nesta PoSIC.

2.8 Esta PoSIC também se aplica, no que couber, ao relacionamento da UFBA com terceiros.

### 3 Referências Legais e Normativas

Esta PoSIC foi desenvolvida principalmente com base nos seguintes documentos:

- Legislação brasileira, normas e regimentos internos da Universidade, conforme Anexo I – Referências Legais e Normativas aplicáveis à Segurança da Informação e Comunicações da UFBA.


### 4 Conceitos e Definições

4.1 Os termos e definições aplicáveis a segurança da informação e comunicações na UFBA estão relacionados no documento Anexo II – Termos e Definições do Sistema Normativo de Segurança da Informação e Comunicações da UFBA.

### 5 Princípios da Política de Segurança

5.1 A PoSIC da UFBA, bem como os seus documentos complementares, deve estar alinhada aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal, e aos seguintes:


- 5.1.1 **Clareza** – as determinações relacionadas à SIC devem ser suficientemente claras, concisas e de fácil entendimento, de modo que todos aqueles envolvidos com os ativos de informação da UFBA possam compreender as suas responsabilidades, direitos e limites;
- 5.1.2 **Responsabilidade** – todo usuário dos ativos de informação da UFBA é responsável pela sua apropriada utilização, devendo zelar e contribuir com a preservação da sua segurança;
- 5.1.3 **Consentimento tácito** – os usuários deverão estar cientes e concordar como cumprimento de todas as determinações de SIC aplicáveis à Universidade e às unidades que compõem a sua estrutura organizacional;

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 6 / 37             |

- 5.1.4 **Ética** – todos os direitos, bens e interesses legítimos dos usuários dos ativos da Universidade, bem como de terceiros, devem ser mutuamente respeitados e preservados de acordo com os princípios da ética, estando aí incluídos os direitos de propriedade intelectual;
- 5.1.5 **Celeridade** – as ações voltadas para a preservação da SIC no âmbito da UFBA devem ser encaminhadas o mais rapidamente possível, de modo a evitar ou ao menos mitigar quaisquer impactos negativos decorrentes de incidentes e violações de segurança;
- 5.1.6 **Conscientização** – deve-se promover, em todas as instâncias da UFBA, a contínua conscientização e capacitação dos usuários dos ativos de informação, visando o desenvolvimento de uma cultura de preservação da SIC no meio institucional, bem como o aprimoramento das competências relacionadas;
- 5.1.7 **Privacidade** – a utilização dos ativos de informação da UFBA deve ocorrer em conformidade com a preservação da intimidade, da vida privada e da honra dos seus usuários, conforme disposto na Constituição Federal, sem prejuízo das auditorias de acesso aos sistemas que se fizerem necessárias para a condução de investigações de violações de segurança; e
- 5.1.8 **Livre expressão** – valores como liberdade de pensamento, investigação e expressão, imprescindíveis em uma comunidade acadêmica, deverão ser respeitados. Em contrapartida, qualquer comportamento que seja contrário aos princípios da SIC no âmbito da UFBA, que possa comprometer os seus ativos de informação ou esteja em desacordo com as determinações de segurança, extrapola o princípio da livre expressão e deverá ser evitado.


## 6 Diretrizes Gerais

- 6.1 O cumprimento desta PoSIC e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Segurança da Informação e Comunicações – CSIC.
- 6.2 Caberá à área de Gestão de Segurança da Informação e Comunicações da UFBA – GSIC, sob a responsabilidade do Gestor de Segurança da Informação e

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 7 / 37             |

Comunicações e em conformidade com as suas atribuições previstas na Portaria Nº 592/2011 e legislação vigente, conduzir as ações de Segurança da Informação e Comunicações no âmbito da Universidade.

- 6.3 A GSIC, com apoio da Pró-Reitoria de Desenvolvimento de Pessoas – PRODEP e demais instâncias da UFBA pertinentes, deve propor programas permanentes e regulares de conscientização, sensibilização e capacitação em SIC, buscando parcerias com outras unidades, órgãos e entidades.
- 6.4 A GSIC deve definir e manter um Plano de Segurança da Informação e Comunicações para a UFBA.
- 6.5 A GSIC deve possuir um sistema de registro de incidentes de SIC, que torne possível o fornecimento de relatórios gerenciais periódicos ao CSIC e à alta administração da UFBA.
- 6.6 Os membros do SGSI da UFBA (CSIC, GSIC e ETIR) devem receber, regularmente, capacitação especializada nas disciplinas relacionadas à SIC, de acordo com suas funções.
- 6.7 O CSIC e a GSIC deverão auxiliar a alta administração da UFBA na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da Universidade e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.
- 6.8 A GSIC deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.
- 6.9 Além de seguir as diretrizes estabelecidas nesta PoSIC, a UFBA também deve se orientar pelas melhores práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.
- 6.10 É vedado a qualquer usuário comprometer a disponibilidade, integridade, a confidencialidade ou a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela UFBA.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 8 / 37             |

6.11 O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação. A falta de designação pressupõe que o gestor é o próprio custodiante.

6.12 Os contratos, convênios, acordos e instrumentos congêneres firmados pela UFBA devem conter cláusulas que determinem a observância desta PoSIC e seus respectivos documentos complementares.

## **7 Diretrizes Específicas**


7.1 Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaboradas normas táticas específicas, bem como manuais e procedimentos operacionais, quando for o caso.

### **7.2 Gestão de Ativos da Informação**

7.2.1 Os ativos de informação devem:

- a) ser inventariados e protegidos;
- b) ter identificados os seus gestores e custodiantes;
- c) ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
- d) ter a sua entrada e saída nas dependências da UFBA autorizadas e registradas por autoridade competente;
- e) ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
- f) ser regulamentados por norma específica quanto à sua utilização; e
- g) ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.
- h) Ter monitorados os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;



|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 9 / 37             |

- 7.2.2 A UFBA 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.
- 7.2.3 Os ativos de informação devem ser protegidos contra quebra de segurança, independente do meio de armazenamento, processamento ou transmissão utilizada.
- 7.2.4 O acesso dos usuários aos ativos de informação e sua utilização pode ser condicionado ao aceite a Termo de Responsabilidade, sem prejuízo do princípio do consentimento tácito.


### **7.3 Gestão de Riscos**

- 7.3.1 A GSIC deve estabelecer um processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação, alinhado com a Gestão de Riscos Institucional.
- 7.3.2 A GRSIC é um processo contínuo e deve ser aplicado na implantação e operação da Gestão de Segurança da Informação e Comunicações, levando em consideração o planejamento, a execução, a análise crítica e a melhoria da SIC na instituição.
- 7.3.3 As unidades administrativas e acadêmicas da UFBA devem colaborar com a GSIC, fornecendo as informações por ela solicitadas, de modo a viabilizar o processo de GRSIC.

### **7.4 Segurança Física e do Ambiente**

- 7.4.1 O CSIC deve estabelecer normas de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.
- 7.4.2 As normas de proteção devem estar alinhados e serem proporcionais aos riscos identificados.

### **7.5 Segurança em Recursos Humanos**

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 10 / 37            |

7.5.1 Os usuários devem ter ciência:

- a) das ameaças e preocupações relativas à SIC; e
- b) de suas responsabilidades e obrigações no âmbito desta PoSIC.

7.5.2 Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em SIC que alcancem todos os usuários da UFBA, de acordo com suas competências funcionais.

7.5.3 Os usuários devem ser sensibilizados e conscientizados para apoiar esta PoSIC no exercício das suas atribuições.

7.5.4 Os usuários devem assinar o Termo de Uso de confidencialidade da UFBA, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.

## **7.6 Gestão de Operações e Comunicações**

7.6.1 O CSIC deve estabelecer parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da UFBA.


7.6.2 Os acordos de nível de serviço firmados pela UFBA devem ser compatíveis com padrões de governança digital e requisitos de segurança.

## **7.7 Controles de Acesso**

7.7.1 O controle de acesso à informação deverá ser implantado nos níveis físico e lógico, e conforme a classificação que lhe for atribuída, baseado na sua criticidade e importância para a instituição.

7.7.2 Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.


7.7.3 Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 11 / 37            |

- 7.7.4 Os usuários da UFBA são responsáveis por todos os atos praticados com suas identificações, tais como: credenciais de acesso, crachás, carimbos, correio eletrônico e assinaturas digitais.
- 7.7.5 A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.
- 7.7.6 A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além daquelas previamente definidas depende de autorização do gestor da área responsável pela informação.
- 7.7.7 Todos os sistemas de informação da UFBA, automatizados ou não, devem possuir um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.
- 7.7.8 Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da UFBA, ou bloqueados em caso de afastamento.
- 7.7.9 Os sistemas de informação de uso institucional da UFBA devem possuir normas específicas, no âmbito de sua atuação, que regulamentem o controle de acesso tais como: o acesso às suas bases de dados, a extração, carga e transformação de dados, e os serviços acessíveis via linguagem de programação, etc.
- 7.7.10 O acesso remoto externo à Rede Corporativa da UFBA deve estar de acordo com as regras estabelecidas em norma específica da instituição.
- 7.7.11 É responsabilidade dos gestores de pessoal disponibilizar periodicamente aos gestores dos ativos de informação os registros de todas as movimentações de pessoal, na forma definida por norma complementar.

## **7.8 Criptografia**

- 7.8.1 O CSIC deve normatizar o uso de recursos criptográficos no âmbito das informações produzidas e custodiadas pela UFBA, com as orientações contidas em norma específica.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 12 / 37            |

7.8.2 O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

## **7.9 Aquisição, Desenvolvimento e Manutenção de Sistemas**

7.9.1 O CSIC deve aprovar, conforme proposto pela área técnica responsável, critérios e metodologias de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento, inclusive atividades de manutenção.

7.9.2 O processo de aquisição de sistemas e aplicações institucionais deve atender requisitos de segurança previstos em norma específica.

## **7.10 Segurança nas operações**

### **7.10.1 Proteção contra malware**


A UFBA deverá manter ferramentas capazes de detectar e prevenir a ação de malwares. As correções necessárias em caso de comprometimento de informações deverão ser executadas, como: desconectar ativos da rede caso necessário, restaurar backup com informações seguras, atualização de ativos e sistemas, troca de senhas possivelmente comprometidas, dentre outras ações.

### **7.10.2 Cópias de segurança**

Todo e qualquer dado ou informação (em formato físico ou lógico) gerada, adquirida, utilizada, armazenada ou que trafegue pela rede de dados da UFBA deve ser protegida.

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário de funcionamento da Universidade, períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática. Os servidores responsáveis pela gestão do sistema de backup deverão identificar atualizações de correção, ciclo de vida do software/hardware e sugestões de melhorias.

As mídias de backup devem ser acondicionadas em local climatizado, de preferência em cofres corta-fogo e distantes o máximo possível do data center. O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis para evitar que mídias ruins danifiquem as cópias.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 13 / 37            |

Somente servidores autorizados poderão manipular os backups, bem como as mídias que estejam armazenadas em outros locais.


### **7.10.3 Gestão de vulnerabilidades**

A Gestão de Vulnerabilidades visa evitar a ocorrência de incidentes de segurança da informação e impactos negativos aos negócios da UFBA, antecipando a correção ou tratamento de fraquezas do ambiente. A gestão das vulnerabilidades deve estar de acordo com as regras estabelecidas em norma específica da instituição.

### **7.10.4 Proteção e privacidade de informações de identificação pessoal**

Os dados pessoais que trafegam na rede de dados da Universidade Federal da Bahia, sendo eles de alunos, professores, servidores, dentre outros e qualquer ação que se faça com esses dados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração deverão seguir princípios para as atividades de tratamento de dados pessoais, segundo a LGPD:

- Finalidade legítima, específica e explícita, que deve ser informada ao titular. É vedado o tratamento posterior dos dados para outras finalidades e fins discriminatórios ilícitos ou abusivos;
- Adequação do tratamento dos dados, que deve ser compatível com as finalidades informadas ao usuário;
- Necessidade do tratamento dos dados limitada aos objetivos para os quais serão processados, abrangendo somente os dados pertinentes, proporcionais e não excessivos, em relação à finalidade do tratamento dos dados para a qual foram coletados;
- Livre acesso: a consulta sobre a forma, a duração do tratamento, e a integralidade de seus dados pessoais deve ser gratuita e facilitada aos titulares;
- Qualidade dos dados: também é garantido aos titulares que os seus dados sejam tratados e apresentados com exatidão, clareza, relevância, além de serem

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 14 / 37            |

atualizados de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;


- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança e prevenção:** garante a utilização de medidas técnicas e administrativas adequadas ao tratamento e proteção de dados pessoais quanto aos acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Não discriminação:** diz respeito à proibição do tratamento para fins discriminatórios ilícitos ou abusivos;
- **Responsabilização e prestação de contas:** o agente deve demonstrar que tomou as providências necessárias e medidas eficazes para o cumprimento das normas de proteção de dados pessoais.

### **7.11 Gestão de Incidentes de Segurança da Informação**

- 7.11.1 Os incidentes de segurança da informação corporativos devem ser identificados, registrados, adequadamente tratados e monitorados através de um processo formalizado e que deve observar as regras a serem definidas em uma norma específica sobre o tema.
- 7.11.2 O CSIC deve aprovar metodologias e normas que estabeleçam processos de gestão para tratamento e resposta a incidentes de segurança da informação, conforme definido pela área específica.
- 7.11.3 Caberá à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, sob a coordenação do Gestor de SIC, realizar o tratamento de incidentes de segurança no meio digital no âmbito da UFBA, conforme disposto em portaria específica.

### **7.12 Gestão de Continuidade do Negócio**

- 7.12.1 O CSIC deve aprovar metodologias e normas que estabeleçam a Gestão de Continuidade do Negócio na UFBA, conforme definido pela área específica.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 15 / 37            |

7.12.2 A Gestão de Continuidade deverá obedecer a um Plano de Continuidade do Negócio, cujas medidas visam minimizar os impactos sofridos pelos ativos de informação da UFBA diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que retornem à normalidade.

### **7.13 Auditoria e Conformidade**

7.13.1 A GSIC deverá definir registros e procedimentos, como trilhas de auditoria e outros, que possam assegurar o rastreamento, acompanhamento, controle e verificação de acessos aos ativos de informação em meio digital da UFBA.

7.13.2 Deve ser realizada, periodicamente, a verificação de conformidade das práticas de SIC da UFBA e de suas unidades com esta PoSIC e seus documentos complementares, bem como com a legislação específica de SIC, conforme diretrizes definidas em norma específica.

7.13.3 A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a UFBA.


### **7.14 Plano de Investimentos em SIC**

7.14.1 Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.

7.14.2 O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados.

7.14.3 O plano de investimentos, assim como a sua proposta orçamentária correspondente, será aprovado pelo CSIC, mediante recomendação elaborada pela GSIC, conforme e posteriormente pelas instâncias superiores.

7.14.4 Caso haja limitação na execução orçamentária, caberá ao CSIC realizar a correspondente revisão do plano de investimentos.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 16 / 37            |


## 7.15 Propriedade Intelectual

- 7.15.1 As informações administrativas produzidas por usuários internos, colaboradores e prestadores de serviço, no exercício de suas funções, são patrimônio intelectual da UFBA.
- 7.15.2 É vedada a utilização de informações produzidas para uso exclusivo da UFBA em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela Universidade, salvo com autorização específica pelos gestores dos ativos de informação, nos processos e documentos de sua competência.
- 7.15.3 Aplica-se a legislação vigente no país sobre direitos autorais e propriedade industrial.

## 7.16 Contratos, Convênios, Acordos e Instrumentos Congêneres

- 7.16.1 Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.
- 7.16.2 Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos, desde que expressamente autorizadas pela UFBA.
- 7.16.3 Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.
- 7.16.4 O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na UFBA.
- 7.16.5 Um plano de contingência deve ser elaborado para o caso de uma das partes desejar encerrar a relação antes do final do acordo.



|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 17 / 37            |

## **7.17 Uso de Recursos e Serviços de TIC**


- 7.17.1 Os recursos e serviços de tecnologia da informação e comunicações devem ser utilizados para a execução das atividades profissionais na UFBA, considerando uso exclusivamente institucional e atendendo aos princípios desta PoSIC.
- 7.17.2 A área técnica responsável pelo recurso ou serviço de TIC definirá controles de segurança que propiciem um uso seguro dos recursos e serviços, conforme regulamentados através de norma específica.

## **7.18 Acesso à Internet**

- 7.18.1 O acesso à rede mundial de computadores – Internet a partir da infraestrutura de telecomunicações da UFBA deve ser utilizado prioritariamente para atender às atividades acadêmicas e administrativas da instituição, obedecendo à legislação vigente.
- 7.18.2 Quando necessário, o acesso a serviços e conteúdos na Internet poderá ser normatizado em conformidade com legislação vigente ou com boas práticas de segurança da informação.
- 7.18.3 Caberá aos titulares de cada unidade definir quais conteúdos da Internet estarão acessíveis aos seus usuários, visando o efetivo cumprimento das suas atividades acadêmicas e/ou administrativas, conforme definido em norma complementar.

## **7.19 Uso de Equipamentos Computacionais Pessoais**

- a) O uso de dispositivos pessoais deve ser restringido contra o acesso indevido ou não autorizado às informações da UFBA e deve estar de acordo com as regras estabelecidas em norma específica da instituição.
- b) Os dispositivos móveis da UFBA devem ser protegidos adequadamente contra o acesso indevido ou não autorizado às informações neles armazenadas ou por meio deles disponíveis.
- c) A proteção desses recursos deve estar de acordo com as regras estabelecidas em norma específica da instituição.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 18 / 37            |

## 7.20 Uso de Mídias Removíveis

- 7.20.1 O uso de mídias removíveis na UFBA não é estimulado, devendo ser tratado como exceção.
- 7.20.2 Informações devem ser transmitidas usando as ferramentas corporativas.
- 7.20.3 Usuários de mídias removíveis, caso comprovado, serão responsabilizados quando os mesmos causarem dano à UFBA, seja por perda ou vazamento de informação confidencial, ou ainda que permita a entrada de softwares maliciosos na rede corporativa.
- 7.20.4 Caso seja necessário transportar arquivos através de mídias removíveis como (HDs Externos e PenDrives) é recomendado que os arquivos sejam criptografados e posteriormente apagados, a fim de evitar vazamento de informações sensíveis.

## 8 Penalidades

- 8.1 Ações que violem os princípios desta PoSIC, quaisquer de suas diretrizes, normas e procedimentos, ou que quebrem os controles de SIC, serão devidamente apuradas e poderão acarretar medidas, inclusive abertura de processo administrativo disciplinar, de responsabilização administrativa, civil, criminal e penal em vigor.


## 9 Competências e Responsabilidades

### 9.1 Cabe ao Comitê de Governança Digital:

- a) aprovar esta PoSIC, bem como as suas revisões; e
- b) tomar decisões administrativas, em instância superior, referentes ao descumprimento desta PoSIC e dos seus documentos complementares.

### 9.2 Cabe à área de Gestão de Segurança da Informação e Comunicações:


- a) promover a cultura de Segurança da Informação e Comunicações na UFBA;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 19 / 37            |

- c) propor os recursos necessários às ações de Segurança da Informação e Comunicações;
- d) coordenar e organizar as questões administrativas do Comitê de Segurança da Informação e Comunicações;
- e) coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
- f) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;
- g) atuar como instância de interlocução com grupos e órgãos de segurança da informação nacionais e internacionais para o trato de assuntos relativos à Segurança da Informação e Comunicações;
- h) propor ao CSIC diretrizes, normas e procedimentos relativos à SIC no âmbito da UFBA;
- i) promover ampla divulgação dos documentos relevantes à comunidade UFBA relacionados à SIC, e garantir que sejam fornecidos orientações e treinamentos relacionados;
- j) fornecer informações relativas a incidentes de segurança, em atendimento a demandas judiciais;
- k) nos casos de violação das diretrizes, normas e procedimentos de SIC, notificar a sua origem e reportar às autoridades competentes, quando cabível; e
- l) nos casos de violação acima referidos, notificar o autor, quando identificado, dando ciência ao seu superior hierárquico.

### **9.3 Cabe ao Comitê de Segurança da Informação e Comunicações:**


- a) assessorar o Comitê de Governança Digital e o Gabinete da Reitoria na implementação das ações de SIC no âmbito da UFBA;
- b) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 20 / 37            |

- c) elaborar as diretrizes de Segurança da Informação e Comunicações, através desta PoSIC e propor as suas alterações;
- d) elaborar, aprovar e publicar normas e procedimentos relativos à SIC, em conformidade com esta PoSIC;
- e) avaliar, quando necessário, os incidentes de segurança causados pela ação ou omissão de usuários dos ativos de informação da UFBA, e recomendar as sanções administrativas cabíveis, nos termos da lei;
- f) propor projetos e iniciativas relacionados à melhoria da Segurança da Informação e Comunicações;
- g) indicar ao Gabinete da Reitoria a relação dos Ativos de Informação da UFBA, para nomeação dos seus Gestores;
- h) solicitar à GSIC apurações quando da suspeita de ocorrências de quebras de SIC;
- i) avaliar, analisar criticamente e, quando for o caso, revisar a PoSIC e suas normas complementares, visando à sua aderência aos objetivos institucionais da UFBA e à legislação vigente;
- j) constituir grupo de trabalho para realizar verificações de conformidade na área de SIC e legislações e normas vigentes;
- k) elaborar o plano de investimentos em SIC da UFBA;
- l) monitorar e avaliar periodicamente o plano de investimentos em SIC, assim como determinar os ajustes cabíveis; e
- m) definir e atualizar seu Regulamento Interno.

#### **9.4 Cabe à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:**


- a) facilitar e executar as atividades de tratamento e resposta a incidentes de segurança;
- b) coordenar a recuperação de serviços de TIC quando de sua quebra de segurança buscando apoio dos órgãos envolvidos;

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 21 / 37            |

- c) agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de auditorias e verificações de conformidade;
- d) realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
- e) analisar ataques e intrusões na rede da UFBA;
- f) executar as ações necessárias para tratar quebras de segurança;
- g) gerar informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
- h) cooperar com as equipes de Tratamento e Resposta a Incidentes de outras instituições; e
- i) participar de fóruns, redes nacionais e internacionais relativos à SIC.
- j) As atividades de tratamento e resposta a incidentes de segurança devem estar de acordo com as regras estabelecidas em norma específica da instituição.

#### **9.5 Cabe aos gestores dos ativos de informação:**

- a) garantir a segurança dos ativos de informação sob sua responsabilidade;
- b) definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC e normas complementares;
- c) conceder e revogar acessos aos ativos de informação;
- d) comunicar à ETIR a ocorrência de incidentes de SIC;
- e) designar custodiantes de ativos de informação, quando aplicável; e
- f) realizar o tratamento e a classificação da informação sob sua responsabilidade.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 22 / 37            |

#### **9.6 Cabe aos custodiantes de ativos de informação:**


- a) proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor do ativo de informação, e de acordo com esta PoSIC e normas complementares.

#### **9.7 Cabe aos titulares das unidades da UFBA:**

- a) corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;
- b) colaborar com as ações desenvolvidas pela GSIC, bem como garantir o cumprimento das diretrizes, normas e procedimentos de SIC na unidade sob sua responsabilidade;
- c) incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;
- d) tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de descumprimento da SIC por parte dos usuários sob sua supervisão;
- e) informar aos gestores de pessoal e dos ativos de informação a respeito de mudanças no quadro de pessoal de sua unidade;
- f) autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;
- g) comunicar à GSIC a respeito de casos de quebra de segurança; e
- h) manter lista atualizada dos ativos de informação sob sua responsabilidade, com seus respectivos gestores.

#### **9.8 Cabe aos terceiros, fornecedores e prestadores de serviço, conforme previsto em contrato:**

- a) tomar conhecimento desta PoSIC;
- b) fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 23 / 37            |


- c) fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

#### **9.9 Cabe aos gestores de pessoal:**

- a) obter anuência do Termo de Responsabilidade (Anexo III) dos usuários dos ativos de informação da UFBA, indicando ciência e pleno acordo com esta PoSIC, bem como normas e procedimentos complementares; e
- b) informar imediatamente aos gestores dos ativos de informação pertinentes a respeito de todas as movimentações de pessoal de que trata o capítulo 7.7, para sejam revisadas ou revogadas as respectivas permissões de acesso.

#### **9.10 Cabe a todos os usuários dos ativos de informação da UFBA:**

- a) tomar conhecimento desta PoSIC, suas normas e procedimentos, bem como suas eventuais atualizações;
- b) indicar, por meio da anuência do Termo de Responsabilidade (Anexo III), a ciência e o pleno acordo com a PoSIC e seus documentos complementares, além de assumir a responsabilidade pelo seu cumprimento;
- c) cumprir todos os princípios, diretrizes e responsabilidades desta PoSIC, bem como os demais normativos e resoluções relacionados à SIC;
- d) obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;
- e) assegurar que os ativos de informação à sua disposição ou sob sua custódia sejam protegidos contra acesso, modificação, destruição ou divulgação não autorizados, e utilizados apenas dentro da finalidade para a qual foram concebidos;
- f) comunicar imediatamente à GSIC a respeito de qualquer descumprimento ou violação a esta POSIC ou às suas normas e procedimentos de que tiver conhecimento; e
- g) em caso de dúvidas ou questionamentos, buscar imediato esclarecimento junto à GSIC, de modo a dirimi-las.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 24 / 37            |


## 10 Divulgação e Atualização

- 10.1 Esta PoSIC deverá ser amplamente divulgada em todos os *campi*, unidades e setores da UFBA, devendo o seu conteúdo, assim como das normas e procedimentos complementares, constar permanentemente em endereço eletrônico específico, acessível publicamente através da Internet.
- 10.2 Esta PoSIC deverá ser revisada e atualizada periodicamente, não devendo exceder o período máximo de 3 (três) anos a partir da data da sua publicação, ou de acordo com determinação do CSIC.
- 10.3 O CSIC formalizará a proposta de revisão da PoSIC por meio de Resolução, a qual deve ser, sucessivamente, apreciada e aprovada.

## 11 Disposições Finais

- 11.1 Os casos omitidos por esta PoSIC que não forem tratados por norma complementar serão analisados e deliberados pelo Comitê de Segurança da Informação e Comunicações, observando-se a legislação em vigor.
- 11.2 Esta PoSIC entra em vigor na data da sua publicação.



|   |   |                                   |
|---|---|-----------------------------------|
|  | <p align="center"> <b>Universidade Federal da Bahia</b><br/> <b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br/> <b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> </p> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 25 / 37            |

**Universidade Federal da Bahia**  
**Comitê de Segurança da Informação e Comunicações – CSIC**


**Anexo I – Referências Legais e Normativas aplicáveis à  
Segurança da Informação e Comunicações da UFBA**

Código: P.POSIC.001.Anexo.I

Revisão: 1.3.0

|   |
|---|
| <p align="center"> <b>Classificação:</b><br/> <b>Uso Interno</b> </p> |
|---|

**Salvador – BA**

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 26 / 37            |


## 1 **Apresentação**

2 Este documento relaciona e referencia o arcabouço legal vigente representado pelas leis, regulamentações e normas aplicáveis à segurança da informação e comunicações na UFBA.


## 3 **Referências Legais e Normativas**

### 3.1 **Dispositivos legais de caráter federal, aplicáveis à segurança da informação:**


- Constituição Federal, art. 5º, inciso X. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
- Constituição Federal, art. 5º, inciso XII. Sigilo dos dados telemáticos e das comunicações privadas.
- Constituição Federal, art. 5º, inciso XIV. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
- Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II. Disponibilidade das informações constantes nos órgãos públicos.
- Constituição Federal, art. 5º, inciso XXXIV. Disponibilidade das informações constantes nos órgãos públicos.
- Constituição Federal, art. 23, incisos III e IV. Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
- Constituição Federal, art. 216, § 2º. Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
- Constituição Federal, art. 37, caput. Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
- Constituição Federal, art. 37, § 6º e Código Civil, art. 43. Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 27 / 37            |


- Constituição Federal, art. 37, § 7º. Necessidade de regulamentação do acesso a informações privilegiadas.
- Consolidação das Leis do Trabalho - CLT, art. 482, alínea "g". Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).
- Código de Conduta da Alta Administração, art. 5º, § 4º. Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).
- Código de Conduta da Alta Administração, art.14, inciso II. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II. Proteção da integridade das informações públicas.
- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II. Proteção da disponibilidade das informações públicas.
- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso X da Seção I. Proteção da disponibilidade das informações públicas.
- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso VII da Seção I. Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso IX da Seção I. Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.
- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II. Disponibilidade das comunicações.
- Código de Propriedade Industrial, art. 75. Sigilo das patentes de interesse da defesa nacional.
- Código de Defesa do Consumidor, arts. 43 e 44. Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 28 / 37            |

- Código Penal, art. 151. Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.
- Código Penal, art. 152. Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.
- Código Penal, art. 153. Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.
- Código Penal, art. 154. Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.
- Código Penal, art. 184, § 3º. Proteção da autenticidade.
- Código Penal, art. 297. Proteção da integridade e autenticidade dos documentos públicos.
- Código Penal, art. 298. Proteção da integridade e autenticidade dos documentos particulares. Código Penal, art. 305. Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
- Código Penal, art. 307. Proteção da autenticidade.
- Código Penal, art. 313-A. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
- Código Penal, art. 313-B. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
- Código Penal, art. 314. Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.
- Código Penal, art. 325. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
- Código Processo Penal, art. 20. Proteção de informações sigilosas.
- Código Processo Penal, art. 207. Proteção do sigilo profissional.
- Código Processo Penal, art. 745. Proteção de informações sigilosas relacionadas ao condenado.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 29 / 37            |

- Código Tributário Nacional, art. 198. Proteção do sigilo fiscal.
- Código de Processo Civil, art. 347, inciso II c/c art. 363, inciso IV. Proteção da privacidade de seus clientes.
- Código de Processo Civil, art. 406, inciso II c/c art. 414, § 2º. Proteção da privacidade de seus clientes.
- Instrução Normativa nº 4/2010 Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.
- Lei nº 6.538/1978, art. 41. Proteção da privacidade de correspondência.
- Lei nº 7.170/1983, art. 13. Proteção das informações sigilosas relacionadas à segurança nacional.
- Lei nº 7.232/1984, art. 2º, inciso VIII. Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.
- Lei nº 7.492/1986, art. 18. Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
- Lei nº 8.027/1990, artigo 5º, inciso I. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
- Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais(LGPD), legislação brasileira que regula as atividades de tratamento de dados pessoais, e que também altera os artigos 7º e 16 do Marco Civil da Internet.
- Lei nº 12.965/2014, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <p align="center"> <b>Universidade Federal da Bahia</b><br/> <b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br/> <b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> </p> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 30 / 37            |

**Universidade Federal da Bahia**  
**Comitê de Segurança da Informação e Comunicações – CSIC**


**Anexo II – Termos e Definições do Sistema Normativo de  
Segurança da Informação e Comunicações da UFBA**

Código: P.POSIC.001.Anexo.II

Revisão: 1.3.0

|   |
|---|
| <p align="center"> <b>Classificação:</b><br/> <b>Uso Interno</b> </p> |
|---|

**Salvador – BA**

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 31 / 37            |


## 1 **Apresentação**

- 2 Este documento apresenta os termos e definições utilizados nos documentos do sistema normativo de segurança da informação da UFBA.
- 3 Este anexo poderá ser atualizado de acordo com a necessidade e de forma independente da revisão da Política de Segurança da Informação.

## 4 **Conceitos e Definições**


No âmbito desta PoSIC, são considerados os seguintes conceitos e definições:

- 4.1 **Agente Público** – todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na Universidade Federal da Bahia, e abrange também os empregados de empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no âmbito da UFBA;
- 4.2 **Ameaça** – conjunto de fatores com potencial para comprometer os objetivos da instituição, seja trazendo danos diretos aos seus ativos, ou prejuízos decorrentes de situações inesperadas;
- 4.3 **Área de Gestão de Segurança da Informação e Comunicações (GSIC)** – área pertencente à Superintendência de Tecnologia da Informação da UFBA, responsável pela gestão das ações envolvendo Segurança da Informação e Comunicações no âmbito da instituição;
- 4.4 **Ativo** – qualquer coisa que tenha valor para a instituição;
- 4.5 **Ativos de informação** – meios de armazenamento, transmissão e processamento de informações, sistemas de informação, dispositivos móveis, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- 4.6 **Capacitação em SIC** – criação, atualização e/ou ampliação das competências necessárias à preservação da Segurança da Informação e Comunicações, por meio da aplicação dos seus conceitos e procedimentos na rotina pessoal e profissional, e possibilitando a atuação de agentes multiplicadores do tema;


|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 32 / 37            |

- 4.7 **Classificação da informação** – identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
- 4.8 **Comitê de Segurança da Informação e Comunicações (CSIC)** – grupo de pessoas com a responsabilidade de assessorar a implementação das ações de Segurança da Informação e Comunicações no âmbito da UFBA;
- 4.9 **Controle de acesso** – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou retirar privilégios de acesso aos ativos de informação;
- 4.10 **Custodiante de ativo de informação** – aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que, embora não lhe pertençam, estão sob sua custódia;
- 4.11 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)** – grupo técnico com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito da UFBA;
- 4.12 **Gestão de Ativos** – processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- 4.13 **Gestão de Continuidade do Negócio** – processo abrangente de gestão que identifica ameaças potenciais para uma instituição e os possíveis impactos nas suas operações, caso essas ameaças se concretizem. Fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a imagem da instituição, e suas atividades de valor agregado;
- 4.14 **Gestão de Operações e Comunicações** – atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;
- 4.15 **Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;




|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 33 / 37            |


- 4.16 **Gestor de ativo de informação** – servidor da UFBA nomeado em processo próprio como responsável pela concessão, manutenção, revisão e cancelamento de privilégios de acesso a determinadas informações e demais ativos a elas relacionados;
- 4.17 **Gestor de pessoal** – pessoa ou unidade responsável pela gestão de pessoas no seu âmbito de atuação. São gestores de pessoal:
- a) a Pró-Reitoria de Desenvolvimento de Pessoas, em se tratando de servidor;
  - b) a Pró-Reitoria de Graduação, Pós-graduação e Extensão, em se tratando de aluno;
  - c) as Pró-Reitorias responsáveis pela concessão de bolsas, ou o responsável por projeto de pesquisa, em se tratando de bolsista ou estagiário; e
  - d) a Pró-Reitoria de Administração, no que diz respeito às informações de recursos humanos das empresas prestadoras de serviço que desenvolvem atividades na UFBA, em se tratando de empregado terceirizado.
- 4.18 **Gestor de SIC** – servidor da UFBA nomeado pelo Gabinete da Reitoria como responsável pela gestão da SIC no âmbito da UFBA;
- 4.19 **Incidente de SIC** – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos de informação da UFBA;
- 4.20 **Informação** – conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- 4.21 **Política de Segurança da Informação e Comunicações (PoSIC)** – documento aprovado pelo Comitê de Governança Digital (CGD) com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação e Comunicações na UFBA. É complementado por duas categorias de documento:
- 4.21.1 **Normas** – concebidas no nível tático, detalham situações, fornecem orientações e estabelecem obrigações a respeito do uso adequado das informações, em conformidade com as diretrizes da PoSIC; e

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 34 / 37            |

- 4.21.2 **Procedimentos** – concebidos no nível operacional, instrumentalizam o disposto nas diretrizes e normas previamente publicadas, permitindo a direta aplicação da SIC nas atividades da Universidade.
- 4.22 **Risco de SIC** – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo para a UFBA;
- 4.23 **Segurança da Informação e Comunicações (SIC)** – conjunto de ações que objetivam viabilizar e assegurar as propriedades de disponibilidade, integridade, confidencialidade e autenticidade – “DICA” das informações:
- 4.23.1 **Disponibilidade** – propriedade de que a informação esteja sempre acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade legítimos;
- 4.23.2 **Integridade** – propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;
- 4.23.3 **Confidencialidade** – propriedade que garante acesso à informação somente às partes autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, seja de forma proposital ou acidental; e
- 4.23.4 **Autenticidade** – propriedade que assevera que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso.
- 4.24 **Segurança física e do ambiente** – processo que trata da proteção de todos os ativos físicos da UFBA, englobando instalações físicas, internas e externas, em todas as localidades em que a instituição está presente;
- 4.25 **Sistema de informação de uso institucional** – conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas e acadêmicas da instituição com eficácia e eficiência;

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 35 / 37            |

- 4.26 **Terceiro** – qualquer pessoa, física ou jurídica, de natureza pública ou privada, externa à UFBA;
- 4.27 **Tratamento da informação** – conjunto de ações referentes à produção, recepção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as de caráter sigiloso;
- 4.28 **Tratamento de incidentes** – processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas de SIC, realizando análises dos incidentes de segurança e procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação da sua origem, bem como de tendências;
- 4.29 **Usuário** – indivíduo com acesso autorizado aos ativos de informação, de acordo com as restrições e permissões definidas. Compreende o grupo de servidores (técnico-administrativos e docentes), alunos, bolsistas, estagiários, prestadores de serviços e visitantes que utilizam os ativos de informação da UFBA;
- 4.30 **Violação ou quebra de segurança** – ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC em uma ou mais propriedades de segurança; e
- 4.31 **Vulnerabilidade** – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

|   |   |                                   |
|---|---|-----------------------------------|
|  | <p align="center"> <b>Universidade Federal da Bahia</b><br/> <b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br/> <b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> </p> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 36 / 37            |


**Universidade Federal da Bahia**  
**Comitê de Segurança da Informação e Comunicações – CSIC**

**Anexo III – Termo de Responsabilidade**

Código: P.POSIC.001.Anexo.III

Revisão: 1.3.0

|   |
|---|
| <p align="center"> <b>Classificação:</b><br/> <b>Uso Interno</b> </p> |
|---|

|   |   |                                   |
|---|---|-----------------------------------|
|  | <b>Universidade Federal da Bahia</b><br><b>Comitê de Segurança da Informação e Comunicações – CSIC</b><br><b>Proposta da Política de Segurança da Informação e Comunicações – PoSIC</b> | <b>Código:</b> P.POSIC.001        |
|   |   | <b>Revisão:</b> 1.3.0             |
|   |   | <b>Classificação:</b> Uso Interno |
|   |   | <b>Data:</b> 11/06/2021           |
|   |   | <b>Página:</b> 37 / 37            |

**Salvador – BA**

### **Anexo III – Termo de Responsabilidade**

Eu, \_\_\_\_\_, usuário (a) dos ativos de informação da Universidade Federal da Bahia, portador (a) da matrícula nº \_\_\_\_\_, RG \_\_\_\_\_, CPF \_\_\_\_\_, residente e domiciliado (a) na

\_\_\_\_\_, cidade de \_\_\_\_\_/\_\_\_\_\_, CEP \_\_\_\_\_,

declaro estar ciente do disposto na sua Política de Segurança da Informação e Comunicações – PoSIC, publicada eletronicamente em <http://www.gsic.ufba.br>, bem como nas normas e procedimentos complementares ali presentes, e comprometo-me a cumprir todas as suas determinações, bem como a manter-me periodicamente atualizado (a) a respeito de eventuais modificações que estes documentos possam sofrer.

Estou ciente que o descumprimento deste termo poderá acarretar medidas, inclusive abertura de processo administrativo disciplinar, bem como a cabível responsabilização administrativa, civil e criminal, quando aplicável.

\_\_\_\_\_, \_\_\_\_\_ de \_\_\_\_\_ de 20\_\_\_\_.

\_\_\_\_\_  
Assinatura