UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2022-2024

COMITÊ DE GOVERNANÇA DIGITAL

# 1. ESCOPO

A Política de Segurança da Informação (POSIN) é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Esta POSIN deve direcionar a Universidade Federal do Espírito Santo (Ufes) na gestão dos riscos e no tratamento dos incidentes de segurança, por meio da adoção de procedimentos e mecanismos, que visam a eliminação ou redução de ocorrência de modificações não autorizadas garantindo confidencialidade, integridade e autenticidade, bem como a disponibilidade de recursos e sistemas críticos para garantir a continuidade do funcionamento da Ufes.

Esta POSIN está em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de Segurança da Informação (SI) e aplica-se a todas as unidades e entidades vinculadas à Universidade Federal do Espírito Santo, bem como a todos os membros da comunidade universitária (incluindo alunos, docentes, servidores técnico-administrativos, estagiários, terceirizados, dentre outros) e qualquer pessoa (agente público ou particular) que, oficialmente, execute atividade vinculada à atuação institucional da Ufes.

# 2. CONCEITOS E DEFINIÇÕES

A Segurança da Informação (SI) visa a preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas, transmitidas ou custodiadas pela Ufes. Adicionalmente, outras propriedades, tais como irretratabilidade (não repúdio), privacidade e primariedade deverão ser observadas.

A POSIN visa estabelecer princípios, normas, procedimentos e recomendações a serem seguidos na abordagem de SI da Ufes, orientando e esclarecendo os seus princípios e controles, no que concerne à sua regulamentação e conscientização na Universidade.

Nesse contexto, devem ser considerados o armazenamento, o processamento e a transmissão destas informações com o uso de quaisquer meios, incluindo papel e telefonia.

Os órgãos e as entidades da administração pública federal deverão utilizar o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI/PR Nº 93, de 18 de outubro de 2021, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos.

# 3. PRINCÍPIOS

A Constituição Brasileira garante em seu artigo 5º, inciso XII ser inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

A publicidade é um princípio a ser observado para a Administração Pública (art. 37 da Constituição Federal), porém determinadas informações cuja guarda está a cargo da Ufes devem ter circulação restrita. Entre elas constam: informações pessoais sobre discentes, docentes, servidores técnico-administrativos e, no caso do Hospital Universitário (HUCAM), pacientes. Também existem informações cuja divulgação pode acarretar prejuízos à União ou à sociedade como, por exemplo, entre outras, o preço esperado em licitações, questões de provas e exames etc.

A SI deve ser entendida como uma responsabilidade coletiva e suas diretrizes devem considerar, prioritariamente, os objetivos estratégicos, os requisitos legais, a estrutura e finalidade da Universidade Federal do Espírito Santo.

Sinteticamente, portanto, o conjunto de documentos que compõe esta POSIN guiar-se-á pelos seguintes princípios gerais:

- **Menor privilégio**: Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.
- **Segregação de função**: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.
- **Auditabilidade**: Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial.
- **Rastreabilidade**: Todas as ações devem poder ser atribuídas a uma pessoa.
- **Mínima dependência de segredos**: Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam.
- **Controles automáticos**: Sempre que possível, controles de segurança automáticos deverão ser utilizados.
- **Resiliência**: Os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre.

- **Defesa em profundidade**: Controles devem ser desenhados em camadas de tal forma que, quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança.
- **Exceção aprovada**: Exceções à POSIN deverão sempre ter aprovação superior.
- **Substituição da segurança em emergências**: Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em emergências.

Esta POSIN deve estar também em conformidade com os princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como com os demais dispositivos legais.

Devido à natureza das universidades onde, por princípio, deve haver um livre fluxo de informação e livre intercâmbio de ideias dentro da comunidade universitária e com a comunidade externa, a Ufes não implementará nenhum sistema de censura, devendo, no entanto, serem respeitados os preceitos éticos e a legislação vigente.

Portanto, os usuários devem ser responsáveis pelas informações que distribuírem ou acessarem. Por haver a possibilidade de uso destes recursos de informação e comunicação para atos ilícitos, a Ufes deverá manter registros de manipulação das informações para fins de auditoria e estar assim em condições de determinar o responsável por algum ilícito.

# 4. DIRETRIZES GERAIS

As instituições de ensino e pesquisa, como a Ufes, necessitam de acesso livre à informação e de mecanismos rápidos, eficientes, seguros e confiáveis para comunicação entre si ou com outros membros da comunidade e da sociedade.

A implantação de mecanismos invasivos de filtros de conteúdo impõe restrições à comunicação, e impede a livre circulação da informação. Por outro lado, a total falta de controle da infraestrutura existente pode ser usada para atividades ilícitas que podem prejudicar não só o funcionamento da rede e dos sistemas computacionais da Ufes, como também os externos, e mesmo causar danos a pessoas. Portanto, deve haver um sistema de identificação e de registro de informações que, sem violar o sigilo das comunicações, permita a identificação de usuários que executem atividades ilícitas ou criminosas.

De outra parte e com o intuito de garantir a qualidade de serviço prestado reserva-se a prerrogativa de garantir a limitação de banda para certos tipos de serviço e/ou usuários.

## 5. DIRETRIZES ESPECÍFICAS

A aplicação de cada uma das diretrizes constantes na relação abaixo deverá ser realizada após a elaboração e publicação das respectivas Instruções Normativas.

- Tratamento da Informação
- Segurança Física e do Ambiente
- Gestão de Incidentes em Segurança da Informação
- Gestão de Ativos
- Gestão do Uso dos Recursos Operacionais e de Comunicações
- Controles de Acesso Lógico
- Gestão de Riscos
- Gestão de Continuidade
- Auditoria e Conformidade
- Segurança em Recursos Humanos
- Desenvolvimento de Software Seguro
- Licenciamento de Software
- Cópias de Segurança (Backup)

## 6. COMPETÊNCIAS E RESPONSABILIDADES

A estrutura de suporte à Gestão de Segurança da Informação (GSI) será composta pelo Gestor de Segurança da Informação, pelo Comitê de Segurança da Informação (CSI) e pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

O Comitê de Segurança da Informação (CSI) será composto pelo Gestor de Segurança da Informação, que o coordenará, e pelos dirigentes das unidades abaixo relacionadas, ou seus representantes designados:

- Gestor de Segurança da Informação (coordenador);
- Reitoria;
- Pró-Reitoria de Administração;
- Pró-Reitoria de Assuntos Estudantis e Cidadania;
- Pró-Reitoria de Extensão;
- Pró-Reitoria de Gestão de Pessoas;
- Pró-Reitoria de Graduação;
- Pró-Reitoria de Pesquisa e Pós-Graduação;

- Pró-Reitoria de Planejamento e Desenvolvimento Institucional;
- Ouvidoria; e
- Diretoria de Documentação Institucional (DDI/PROAD).

A composição e funcionamento da ETIR está a cargo de Instrução Normativa específica.

## Compete ao Gestor de Segurança da Informação:

- Coordenar o Comitê de Segurança da Informação ou estrutura equivalente;
- Coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
- Assessorar a alta administração na implementação da Política de Segurança da Informação;
- Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;
- Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- Propor recursos necessários às ações de segurança da informação;
- Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);
- Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e
- Manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

## Comitê de Segurança da Informação (CSI):

- Assessorar a implementação das ações de segurança da informação;

- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
- Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;
- Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação; e

  Deliberar sobre normas internas de segurança da informação.

## Compete à Alta Administração:

- Designar um Gestor de Segurança da Informação;
- Instituir Comitê de Segurança da Informação (CSI) ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;
- Promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação; e

  Garantir os recursos necessários para a execução da POSIN no âmbito da Ufes.

## Compete aos setores da Ufes:

- Detectar e encaminhar ao Gestor de Segurança da Informação os casos de quebra da SI e das comunicações ocasionadas por riscos não identificados ou riscos que não foram tratados por usuários;
- Realizar análise, avaliação e tratamento de riscos dos ativos de informação sob sua administração a partir das diretrizes estabelecidas em instruções normativas, legislação e orientações do CSI;
- Contribuir para o processo de melhoria contínua da GSI monitorando e realizando análises críticas dos ativos do setor;
- Indicar responsáveis pelo gerenciamento de atividades relacionadas à GSI no setor;
- Comunicar às partes interessadas os riscos dos ativos de informação sob a administração do setor; e
- Comunicar ao Gestor de Segurança da Informação situações que comprometam à GSI.

## Compete aos Usuários:

- Cumprir a GSI da Universidade;

- Comunicar ao chefe imediato situações de riscos que comprometam a segurança das informações da Universidade.

# 7. PENALIDADES

O não cumprimento desta POSIN e suas Instruções Normativas sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos da Ufes, caracterizando infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos desta POSIN e suas Instruções Normativas, fica sujeito à aplicação das penalidades previstas na Lei Nº 8.112/90 e na legislação pertinente.

# 8. POLÍTICA DE ATUALIZAÇÃO

Esta POSIN e as Instruções Normativas derivadas devem ser revistas periodicamente, em intervalo não superiores a 3 (três) anos. Para esta revisão, deve ser instituída uma comissão específica.

O CSI está autorizado a promover alterações na POSIN em caso de alteração/criação de princípios constitucionais, administrativos ou do arcabouço legislativo vigente que rege a Administração Pública Federal. Contudo, tais alterações devem ser homologadas pelo Comitê de Governança Digital (CGD).

# 9. DISPOSIÇÕES FINAIS

Os casos omissos e as dúvidas com relação a esta Política de Segurança da Informação (POSIN) serão submetidos ao Comitê de Segurança da Informação (CSI) da Ufes.

# 10. REFERÊNCIAS LEGAIS E NORMATIVAS

## 10.1 LEIS

LEI Nº 8.666 DE 21 DE JUNHO DE 1993

LEI Nº 9.610 DE 19 DE FEVEREIRO DE 1998

LEI Nº 10.098 DE 19 DE DEZEMBRO DE 2000

LEI Nº 10.436 DE 24 DE ABRIL DE 2002

LEI Nº 10.520 DE 17 DE JULHO DE 2002

LEI Nº 12.527 DE 18 DE NOVEMBRO DE 2011

LEI Nº 12.682 DE 9 DE JULHO DE 2012

LEI Nº 12.965 DE 23 DE ABRIL DE 2014

LEI Nº 13.146 DE 06 DE JULHO DE 2015

LEI Nº 13.460 DE 26 DE JUNHO DE 2017

LEI Nº 13.709 DE 14 DE AGOSTO DE 2018

LEI Nº 13.874 DE 20 DE SETEMBRO DE 2019

## 10.2 DECRETOS

DECRETO Nº 5.296 DE 02 DE DEZEMBRO DE 2004

DECRETO Nº 5.626 DE 22 DE DEZEMBRO DE 2005

DECRETO Nº 6.949 DE 25 DE AGOSTO DE 2009

DECRETO Nº 7.174 DE 12 DE MAIO DE 2010

DECRETO Nº 7.579 DE 11 DE OUTUBRO DE 2011

DECRETO Nº 7.724 DE 16 DE MAIO DE 2012

DECRETO Nº 7.892 DE 23 DE JANEIRO DE 2013

DECRETO Nº 8.777 DE 11 DE MAIO DE 2016

DECRETO Nº 8.936 DE 19 DE DEZEMBRO DE 2016

DECRETO Nº 9.094 DE 17 DE JULHO DE 2017

DECRETO Nº 9.319 DE 21 DE MARÇO DE 2018

DECRETO Nº 9.637 DE 26 DE DEZEMBRO DE 2018

DECRETO Nº 9.723 DE 11 DE MARÇO DE 2019

DECRETO Nº 9.756 DE 11 DE ABRIL DE 2019

DECRETO Nº 9.854 DE 25 DE JUNHO DE 2019

DECRETO Nº 9.903 DE 08 DE JULHO DE 2019

DECRETO Nº 10.024 DE 20 DE SETEMBRO DE 2019

DECRETO Nº 10.046 DE 09 DE OUTUBRO DE 2019

DECRETO Nº 10.278 DE 18 DE MARÇO DE 2020

DECRETO Nº 10.332 DE 28 DE ABRIL DE 2020

DECRETO Nº 10.403 DE 19 DE JUNHO DE 2020

DECRETO-LEI Nº 200 DE 25 DE FEVEREIRO DE 1967

## 10.3 PORTARIAS

PORTARIA CONJUNTA Nº 6 DE 14 DE MARÇO DE 2019

PORTARIA INTERMINISTERIAL MP-MC-MD Nº 141 DE 02 DE MAIO DE 2014

PORTARIA INTERMINISTERIAL Nº 1 DE 12 DE JANEIRO DE 2017

PORTARIA INTERMINISTERIAL Nº 176 DE 25 DE JUNHO DE 2018

PORTARIA INTERMINISTERIAL SEME-SGPR SGD-SEDGG-ME Nº 1 DE 7 DE AGOSTO DE 2020

PORTARIA MCOM Nº 2.382 DE 9 DE ABRIL DE 2021 - GUIA DE ESTILO

PORTARIA NORMATIVA Nº 5 DE 14 DE JULHO DE 2005

PORTARIA Nº 1 DE 4 DE ABRIL DE 2019

PORTARIA Nº 1.914 SEI-MCOM DE 28 DE JANEIRO DE 2021 – MANUAL DA MARCA

PORTARIA Nº 1.915 SEI-MCOM DE 28 DE JANEIRO DE 2021 – GUIA DE TRANSFORMAÇÃO DIGITAL

PORTARIA Nº 3 DE 7 DE MAIO DE 2007

PORTARIA Nº 6.432 DE 11 DE JULHO DE 2018

PORTARIA Nº 8 DE 7 DE MAIO DE 2007

PORTARIA Nº 11 SLTI DE 30 DE DEZEMBRO DE 2008

PORTARIA Nº 11.551 DE 8 DE MAIO DE 2020

PORTARIA Nº 13.420 DE 2 DE JUNHO DE 2020

PORTARIA Nº 23 DE 4 DE ABRIL DE 2019

PORTARIA Nº 39 DE 9 DE JULHO DE 2019

PORTARIA Nº 41 DE 3 DE SETEMBRO DE 2019

PORTARIA Nº 482 DE 28 DE AGOSTO DE 2020 - MANUAL DE PUBLICAÇÃO

PORTARIA Nº 483 DE 28 DE AGOSTO DE 2020 - MANUAL DE DIRETRIZES

PORTARIA Nº 484 DE 28 DE AGOSTO DE 2020 - MANUAL DE MIGRAÇÃO

PORTARIA Nº 485 DE 28 DE AGOSTO DE 2020 - MANUAL DE SEO

PORTARIA Nº 540 DE 8 DE SETEMBRO DE 2020 - PADRÃO DIGITAL DE GOVERNO DOS ÓRGÃOS E ENTIDADES DO PODER EXECUTIVO FEDERAL

PORTARIA Nº 778 DE 4 DE ABRIL DE 2019

PORTARIA SLTI-MPOG Nº 92 DE 24 DE DEZEMBRO DE 2014

PORTARIA STI-MP Nº 4 DE 6 DE MARÇO DE 2017

PORTARIA STI-MP Nº 20 DE 14 DE JUNHO DE 2016

## 10.4 RESOLUÇÕES

RESOLUÇÃO Nº 1 DE 23 DE OUTUBRO DE 2012

RESOLUÇÃO Nº 2 DE 24 DE MARÇO DE 2017

RESOLUÇÃO Nº 3 DE 13 DE OUTUBRO DE 2017

## 10.5 INSTRUÇÕES NORMATIVAS

INSTRUÇÃO NORMATIVA 01-2009 GSI DE 13 DE JUNHO DE 2008

INSTRUÇÃO NORMATIVA Nº 1 DE 17 DE JANEIRO DE 2011

INSTRUÇÃO NORMATIVA Nº 1 DE 19 DE JANEIRO DE 2010

INSTRUÇÃO NORMATIVA Nº 3 DE 27 DE MARÇO DE 2012

INSTRUÇÃO NORMATIVA Nº 4 DE 13 DE ABRIL DE 2012

INSTRUÇÃO NORMATIVA Nº 5 DE 18 DE JUNHO DE 2018

INSTRUÇÃO NORMATIVA Nº 8 DE 27 DE NOVEMBRO DE 2018

INSTRUÇÃO NORMATIVA SECOM-PR Nº 8 DE 19 DE DEZEMBRO DE 2014

INSTRUÇÃO NORMATIVA SEGES-MP Nº 1 DE 10 DE JANEIRO DE 2019

INSTRUÇÃO NORMATIVA SEGES-MP Nº 5 DE 26 DE MAIO DE 2017

INSTRUÇÃO NORMATIVA SGD-ME Nº 1 DE 4 DE ABRIL DE 2019

INSTRUÇÃO NORMATIVA SGD-ME Nº 2 DE 4 DE ABRIL DE 2019

INSTRUÇÃO NORMATIVA SGD-ME Nº 128 DE 28 DE DEZEMBRO DE 2020

INSTRUÇÃO NORMATIVA SGD-ME Nº 202 DE 18 DE SETEMBRO DE 2019

## 10.6 NORMAS COMPLEMENTARES

NORMA COMPLEMENTAR 04-2009 DE 14 DE AGOSTO DE 2009