RESOLUÇÃO Nº 06/2021

Estabelece a Política de Segurança da Informação no âmbito da Universidade Federal do Sul da Bahia.

O CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DO SUL DA BAHIA, no uso de suas atribuições,

CONSIDERANDO o Decreto nº 9.637 de 26 de dezembro de 2018, do Gabinete de Segurança Institucional da Presidência da República que institui a Política Nacional de Segurança da Informação no âmbito da administração pública federal;

CONSIDERANDO o Decreto nº 10.332 de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

CONSIDERANDO o Decreto nº 10.641, de 2 de março de 2021 que Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

CONSIDERANDO a Instrução Normativa Nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República que Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO a Instrução Normativa Nº 2 de 24 de julho de 2020 do Gabinete de Segurança Institucional da Presidência da República que Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO a deliberação do plenário em Reunião Ordinária realizada no dia 24 de março de 2021,

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação (POSIN) no âmbito da Universidade Federal do Sul da Bahia, anexa a esta Resolução.

Art. 2º A POSIN entra em vigor na data de sua publicação, revogando-se quaisquer disposições em contrário.

Itabuna, 26 de março de 2021

JOANA ANGELICA GUIMARAES DA LUZ:57521239091

Assinado de forma digital por JOANA ANGELICA GUIMARAES DA LUZ:57521239091
DN: c=BR, o=ICP-Brasil, ou=presencial, ou=34028316000103, ou=Secretaria da Receita Federal do Brasil - RFB, ou=ARCORREIOS, ou=RFB e-CPF A3, cn=JOANA ANGELICA GUIMARAES DA LUZ:57521239091
Dados: 2021.03.26 11:31:07 -03'00'

JOANA ANGÉLICA GUIMARÃES DA LUZ
PRESIDENTE DO CONSELHO UNIVERSITÁRIO
REITORA

SUMÁRIO

1. Escopo

1.1. Esta Política de Segurança da Informação (POSIN), elaborada pelo Comitê de Segurança da Informação (CSI), e aprovada pelo Conselho Universitário (CONSUNI) da Universidade Federal do Sul da Bahia (UFSB), define as diretrizes gerais de Segurança da Informação (SI) no âmbito desta instituição, visando a preservação da disponibilidade, integridade, confidencialidade e autenticidade dos seus ativos de informação bem como atitudes adequadas para gestão, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso da UFSB contra ameaças e vulnerabilidades;

1.2. O escopo da Política de Segurança da Informação (POSIN) da UFSB envolve aspectos estratégicos, estruturais, organizacionais e humanos, bem como elementos físicos e lógicos, preparando a base para elaboração dos demais documentos normativos e não se limitam apenas a aspectos de Tecnologia da Informação (TI);

1.3. O objetivo desta política é estabelecer diretrizes e responsabilidades no que diz respeito a gestão, tratamento, controle e proteção dos ativos mencionados, servindo de apoio à alta direção na implementação do Sistema de Gestão de Segurança da Informação (SGSI) da UFSB, buscando assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

1.4. As diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta política devem ser observados e cumpridos em todo o âmbito da UFSB, nas suas diversas instâncias;

1.5. Esta política, assim como o disposto nas normas e procedimentos complementares, aplica-se a servidores, alunos, bolsistas, estagiários, visitantes, colaboradores externos que prestam serviço em razão de contratos administrativos firmados na forma da Lei e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres; e

1.6. Todos aqueles mencionados no item anterior são responsáveis pela proteção dos ativos de informação de propriedade ou custodiados pela UFSB, e devem estar comprometidos com o cumprimento desta política e suas normas complementares.

2. Conceitos e definições

2.1. **Reitoria:** é o órgão executivo superior, ao qual compete dirigir, administrar, planejar, coordenar, estabelecer parcerias e fiscalizar as atividades da Universidade;

2.2. **Unidade:** qualquer instância administrativa e acadêmica da UFSB a exemplo dos campi, unidades ligadas aos campi, núcleos de pesquisa e centros com funcionalidades específicas;

2.3. **Pró-Reitoria de Tecnologia da Informação e Comunicação (PROTIC):** instância administrativa responsável pelo desenvolvimento, implantação e manutenção dos recursos de Tecnologia da Informação e Comunicação (TIC);

2.4. **Coordenação de Segurança da Informação e Comunicação (CoSIC):** instância administrativa responsável por elaborar e revisar planos e a política de segurança da informação, implementar controles que possam proteger as informações contra acesso não autorizado e evitar que elas sejam danificadas, adotar medidas de contenção de ameaças, prevenir e responder a incidentes de segurança, disseminar a cultura de segurança da informação na UFSB, entre outras atividades relacionadas a SI;

2.5. **Pró-Reitoria de Gestão de Pessoas (PROGEPE):** instância administrativa responsável por orientar, coordenar e acompanhar as atividades referentes as políticas de pessoal, o que inclui atividades como a preparação para a seleção e contratação de novos servidores efetivos e substitutos, bem como a gestão da vida funcional, como capacitação, licenças, afastamentos, saúde, segurança do trabalho, saídas e registros como inativos; e

2.6. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC):** O Plano Diretor de Tecnologia da Informação (PDTI), é um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação de um órgão ou entidade para um determinado período. Também é o instrumento que permite nortear e acompanhar a atuação da área de TIC, definindo estratégias e o plano de ação para implementá-las.

2.7. Os demais termos utilizados nesta política foram retirados do Glossário de Segurança da Informação publicado pelo Gabinete de Segurança Institucional (GSI) através da portaria Nº 93, de 26 de setembro de 2019.

3. Referências Legais e Normativas

3.1. As Referências Legais e Normativas aplicáveis à Segurança da Informação estão relacionadas no Anexo I – Referências Legais e Normativas aplicáveis à Segurança da Informação.

4. Princípios

4.1. Esta política segue os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal e ainda considera os preceitos básicos da Segurança da Informação como: integridade, confidencialidade,

disponibilidade, autenticidade e não repúdio, bem como a proteção dos dados, informações e conhecimentos produzidos na UFSB;

4.2. Em complemento, a Política de Segurança da Informação (POSIN) da UFSB é regida pelos seguintes princípios adicionais:

4.2.1. Criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

4.2.2. Celeridade: as ações de segurança da informação devem fornecer respostas rápidas a incidentes e falhas;

4.2.3. Responsabilidade: as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todo usuário dos ativos de informação da UFSB é responsável pela sua apropriada utilização, devendo zelar e contribuir com a preservação da sua segurança e pelo cumprimento das Normas de Segurança da Informação advindas desta política;

4.2.4. Ciência: todos os usuários da informação devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

4.2.5. Ética: todos os direitos e interesses legítimos dos usuários da informação devem ser respeitados;

4.2.6. Proporcionalidade: ao se tomar qualquer decisão que envolva o tema Segurança da Informação (SI) na UFSB o nível, a complexidade e os custos das ações serão adequados ao entendimento administrativo e ao valor do ativo a proteger;

4.2.7. Privilégio mínimo: a atribuição dos acessos deve ser concedida ao estritamente necessário ao exercício das funções;

4.2.8. Clareza: as determinações relacionadas à SI devem ser suficientemente concisas e de fácil entendimento, de modo que todos aqueles envolvidos com os ativos de informação da UFSB possam compreender as suas responsabilidades, direitos e limites;

4.2.9. Conscientização: deve-se promover, em todas as instâncias da UFSB, a contínua conscientização e capacitação dos usuários dos ativos de informação, visando o desenvolvimento de uma cultura de preservação da SI no meio institucional, bem como o aprimoramento das competências relacionadas;

4.2.10. Privacidade: a utilização dos ativos de informação da UFSB deve ocorrer em conformidade com a preservação da intimidade, da vida privada e da honra dos seus usuários, conforme disposto na Constituição Federal e legislações

correlatas, sem prejuízo das auditorias de acesso aos sistemas que se fizerem necessárias para a condução de investigações de violações de segurança; e

4.2.11. 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 SI no âmbito da UFSB, que possa comprometer os seus ativos de informação, ou esteja em desacordo com as determinações de SI, extrapola o princípio da livre expressão, deverá ser evitado.

5. Competências

5.1. A Segurança da Informação é disciplina fundamental da boa governança corporativa, sendo de responsabilidade da alta administração da UFSB;

5.2. Para assessorar a alta administração da UFSB nas atividades de definição e implementação de diretrizes, políticas, normas e procedimentos relativos à SI, fica instituída a Estrutura de Gestão de Segurança da Informação da UFSB, em conformidade com a Instrução Normativa Nº 1, de 27 de maio de 2020 do GSI;

5.3. A Estrutura de Gestão de Segurança da Informação da UFSB é composta por:

5.3.1. Comitê de Governança Digital (CGD);

5.3.2. Comitê de Segurança da Informação (CSI);

5.3.3. Gestor de Segurança da Informação;

5.3.4. Coordenação de Segurança da Informação e Comunicação (CoSIC); e

5.3.5. Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT).

5.4. Ficam definidas nesta política as atribuições destas estruturas administrativas no que tange a SI na UFSB;

5.5. Comitê de Governança Digital

5.5.1. Cabe ao CGD:

5.5.1.1. tomar decisões administrativas, em instância superior ao CSI, referentes ao descumprimento desta política e das suas normas complementares.

5.6. Comitê de Segurança da Informação

5.6.1. Cabe ao CSI:

5.6.1.1. propor, avaliar e revisar, regularmente, a Política de Segurança da Informação (POSIN) e seus planos de ação;

5.6.1.2. assessorar o Comitê de Governança Digital e o Gabinete da Reitoria na implementação das ações de SI no âmbito da UFSB;

5.6.1.3. constituir grupos de trabalho para realizar verificações de conformidade na área de SI e legislações e normas vigentes;

5.6.1.4. instituir o Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT);

5.6.1.5. elaborar as diretrizes de SI, por meio dessa política e propor as suas alterações;

5.6.1.6. elaborar, aprovar e publicar normas e procedimentos relativos à SI, em conformidade com esta política;

5.6.1.7. avaliar, quando necessário, os incidentes de segurança causados pela ação ou omissão de usuários dos ativos de informação da UFSB, e recomendar as sanções administrativas cabíveis, nos termos da lei;

5.6.1.8. propor projetos e iniciativas relacionados à melhoria da SI;

5.6.1.9. solicitar ao CSIRT apurações quando da suspeita de ocorrências de quebras de SI; e

5.6.1.10. avaliar, analisar criticamente e, quando for o caso, revisar esta política e suas normas complementares, visando à sua aderência aos objetivos institucionais da UFSB e à legislação vigente;

5.7. Gestor de Segurança da Informação

5.7.1. Cabe ao Gestor de Segurança da Informação:

5.7.1.1. coordenar e organizar as questões administrativas do CSI;

5.7.1.2. promover e disseminar a cultura de SI;

5.7.1.3. coordenar a elaboração desta política e suas revisões;

5.7.1.4. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à CGD, após análise do CSI, os resultados consolidados de tais investigações e avaliações;

5.7.1.5. propor recursos necessários às ações de SI;

5.7.1.6. realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na SI;

5.7.1.7. propor normas e procedimentos relativos à SI;

5.7.1.8. manter contato permanente com o Departamento de Segurança da Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional (GSI) da Presidência da República, para o trato de assuntos relativos à SI, quando necessário;

5.7.1.9. consolidar em relatórios anuais os resultados dos trabalhos de auditoria de SI;

5.7.1.10. prover os meios necessários para capacitação e aperfeiçoamento técnico dos membros do CSIRT, bem como prover a infraestrutura necessária para o seu funcionamento; e

5.7.1.11. providenciar a divulgação institucional desta política e de suas normas complementares.

5.8. **Coordenação de Segurança da Informação e Comunicação (CoSIC)**

5.8.1. Cabe a CoSIC:

5.8.1.1. coordenar o Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT);

5.8.1.2. planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança;

5.8.1.3. promover a cultura de SI na UFSB;

5.8.1.4. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

5.8.1.5. propor os recursos necessários às ações de SI;

5.8.1.6. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;

5.8.1.7. atuar como instância de interlocução com grupos e órgãos de segurança da informação nacionais e internacionais para o trato de assuntos relativos à SI;

5.8.1.8. propor ao CSI diretrizes, normas e procedimentos relativos à SI no âmbito da UFSB;

5.8.1.9. promover ampla divulgação dos documentos relevantes à comunidade UFSB relacionados à SI, e garantir que sejam fornecidos orientações e treinamentos relacionados;

5.8.1.10. fornecer informações relativas a incidentes de segurança, em atendimento a demandas judiciais;

5.8.1.11. nos casos de violação das diretrizes, normas e procedimentos de SI, notificar a sua origem e reportar às autoridades competentes, quando cabível; e

5.8.1.12. nos casos de violação acima referidos, notificar o autor, quando identificado, dando ciência ao seu superior hierárquico.

5.9. **Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT)**

5.9.1. Cabe ao CSIRT:

5.9.1.1. facilitar e executar as atividades de tratamento e resposta a incidentes de segurança;
5.9.1.2. coordenar a recuperação de serviços de TIC quando de sua quebra de segurança buscando apoio dos órgãos envolvidos;
5.9.1.3. agir de modo proativo com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SI e avaliando condições de segurança de redes por meio de auditorias e verificações de conformidade;
5.9.1.4. 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;
5.9.1.5. analisar ataques e intrusões na rede da UFSB;
5.9.1.6. executar as ações necessárias para tratar quebras de segurança;
5.9.1.7. gerar informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
5.9.1.8. cooperar com as equipes de Tratamento e Resposta a Incidentes de outras instituições; e
5.9.1.9. participar em fóruns, redes nacionais e internacionais relativos à SI.

5.10. **Gestores dos Ativos de Informação**

5.10.1. Cabe aos Gestores dos Ativos de Informação:

5.10.1.1. garantir a segurança dos ativos de informação sob sua responsabilidade;
5.10.1.2. definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta POSIN e normas complementares;
5.10.1.3. conceder e revogar acessos aos ativos de informação;
5.10.1.4. comunicar o CSIRT a ocorrência de incidentes de SIC;
5.10.1.5. designar custodiantes de ativos de informação, quando aplicável; e
5.10.1.6. realizar o tratamento e a classificação da informação sob sua responsabilidade.

5.11. **Custodiante de Ativos de Informação**

5.11.1. Cabe ao Custodiante de Ativos de Informação:

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

5.12. **Titulares das Unidades da UFSB**

5.12.1. Cabe aos Titulares das Unidades da UFSB:

5.12.1.1. corresponsabilizar-se pelas ações realizadas por usuários sob sua supervisão;
5.12.1.2. colaborar com as ações desenvolvidas pelo CSI, bem como garantir o cumprimento das diretrizes, normas e procedimentos de SI na unidade sob sua responsabilidade;
5.12.1.3. incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI;
5.12.1.4. tomar as medidas administrativas necessárias para que sejam apurados os casos de descumprimento da SI por parte dos usuários sob sua supervisão;
5.12.1.5. informar a PROGEPE e os gestores dos ativos de informação a respeito de mudanças no quadro de pessoal de sua unidade;
5.12.1.6. autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;
5.12.1.7. comunicar ao CSIRT a respeito de casos de quebra de segurança; e
5.12.1.8. manter lista atualizada dos ativos de informação sob sua responsabilidade, com seus respectivos gestores.

5.13. **Pró-Reitoria de Gestão de Pessoas (PROGEPE)**

5.13.1. Cabe a Pró-Reitoria de Gestão de Pessoas (PROGEPE):

5.13.1.1. obter anuência do Termo de Responsabilidade e Sigilo (Anexo II) dos usuários dos ativos de informação da UFSB, indicando ciência e pleno acordo com esta POSIN, bem como normas e procedimentos complementares; e
5.13.1.2. informar imediatamente aos gestores dos ativos de informação pertinentes a respeito de todas as movimentações de pessoal, para que sejam revisadas ou revogadas as respectivas permissões de acesso.

5.14. **Terceiros, Fornecedores e Prestadores de Serviço**

5.14.1. Cabe aos terceiros, fornecedores e prestadores de serviço:

5.14.1.1. tomar conhecimento desta POSIN; e

5.14.1.2. fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

5.15. **Usuários da UFSB**

5.15.1. Cabe a todos os Usuários da UFSB:

5.15.1.1. tomar conhecimento desta POSIN, suas normas e procedimentos, bem como suas eventuais atualizações;

5.15.1.2. indicar, por meio da anuência do Termo de Responsabilidade e Sigilo (Anexo II), a ciência e o pleno acordo com a POSIN e suas normas complementares, além de assumir a responsabilidade pelo seu cumprimento;

5.15.1.3. cumprir todos os princípios, diretrizes e responsabilidades desta POSIN, bem como os demais normativos e resoluções relacionados à SI;

5.15.1.4. 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;

5.15.1.5. comunicar imediatamente ao CSIRT a respeito de qualquer descumprimento ou violação a esta POSIN ou às suas normas e procedimentos de que tiver conhecimento; e

5.15.1.6. em caso de dúvidas ou questionamentos, buscar imediato esclarecimento junto ao CSI, de modo a dirimi-las.

6. Diretrizes Gerais

6.1. São diretrizes gerais da Política de Segurança da Informação (POSIN) da UFSB:

6.1.1. Estar alinhada aos objetivos estratégicos, processos, requisitos legais e estrutura da UFSB, bem como ao Plano Diretor de Tecnologia da Informação (PDTI);

6.1.2. Adoção de medidas proativas que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que compõem o ativo da informação da UFSB;

6.1.3. As diretrizes desta política constituem os principais pilares do Sistema de Gestão de Segurança da Informação da UFSB, sendo norteadoras da elaboração das normas de SI;

6.1.4. Além de seguir as diretrizes estabelecidas nesta política, a UFSB também deve se orientar pelas melhores práticas e procedimentos de SI recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões;

6.1.5. A UFSB, como usuária dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatária de suas Políticas e Normas de Segurança. Portanto, todos os serviços que são disponibilizados pela UFSB por meio desse convênio será regulado pelas políticas e normas da RNP, sem prejuízo do cumprimento desta política e suas normas complementares;

6.1.6. O Comitê de Segurança da Informação (CSI), com o apoio da PROGEPE e demais instâncias pertinentes da UFSB, deve propor programas permanentes e regulares de conscientização, sensibilização e capacitação em SI, buscando parcerias com outras unidades, órgãos e entidades;

6.1.7. A CoSIC deve possuir um sistema de registro de incidentes de SI, que torne possível o fornecimento de relatórios gerenciais periódicos ao CSI e à alta administração da UFSB;

6.1.8. Os membros do Sistema de Gestão de Segurança da Informação (SGSI) da UFSB (CSI, CoSIC e CSIRT) devem receber, regularmente, capacitação especializada nas disciplinas relacionadas à SI, de acordo com suas funções;

6.1.9. O CSI deverá auxiliar a alta administração da UFSB 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;

6.1.10. 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;

6.1.11. Os contratos, convênios, acordos e instrumentos congêneres firmados pela UFSB devem conter cláusulas que determinem a observância desta política e seus respectivos documentos complementares;

6.1.12. É vedado a todo e qualquer usuário comprometer a disponibilidade, integridade, a confidencialidade ou a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela UFSB;

6.1.13. É vedado a todo e qualquer usuário da UFSB o uso dos recursos de TIC da instituição para fins pessoais (próprios ou de terceiros) relacionados à veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética, ou que prejudiquem o cidadão ou a imagem da instituição; e

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

6.2. Tratamento da Informação

6.2.1. As informações existentes no âmbito da UFSB apresentam diferentes níveis de confidencialidade e devem ser classificadas de acordo com a legislação vigente;

6.2.2. Toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelos agentes públicos da UFSB, no exercício de suas atividades, ou terceirizados e prestadores de serviços por meio de contrato firmado com a UFSB, é de propriedade da UFSB e são classificadas e protegidas segundo as diretrizes descritas nesta política e nas regulamentações em vigor;

6.2.3. As informações classificadas conforme a legislação vigente, produzida, armazenada e transportada em meios eletrônicos, utilizará criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos usuários das aplicações;

6.2.4. Toda informação institucional, se eletrônica, estará armazenada nos servidores de arquivo e bases de dados sob gestão e administração da PROTIC com mecanismo de cópia de segurança a fim de garantir sua recuperação em caso de perda da informação original;

6.2.5. Toda informação institucional, se não eletrônica, deverá ser mantida em local que a proteja adequadamente;

6.2.6. A cessão de bases de dados, informação custodiada ou de propriedade da UFSB a terceiros, deverá ser autorizada pelo CSI que providenciará a documentação formal relativa à cessão ou autorização de acesso às informações em conformidade com a legislação vigente antes da sua disponibilização;

6.2.7. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deverá providenciar junto à concedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso em conformidade com a legislação vigente;

6.2.8. Todos os servidores, fornecedores e terceiros devem assinar o Termo de Confidencialidade e Sigilo em relação as informações que irão ter acesso, antes mesmo que tenham acesso;

6.2.9. O CSI elaborará normas complementares e procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança.

6.3. Segurança Física e do Ambiente

6.3.1. O CSI deve estabelecer normas de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências;

6.3.2. As normas de proteção devem estar alinhadas e serem proporcionais aos riscos identificados;

6.3.3. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis;

6.3.4. As máquinas fotocopiadoras ou outras formas de reprodução devem possuir mecanismo de autenticação, e se possível, com múltiplos fatores. Documentos com informações classificadas na forma da lei no grau secreto ou reservado não devem ser abandonados após a sua cópia, impressão ou utilização; e

6.3.5. Deverá ser adotada a política de mesa limpa, de acordo com os seguintes procedimentos básicos:

6.3.5.1. Os papéis, mídias eletrônicas, ou qualquer outro meio onde informações possam ser gravadas, que forem importantes, críticos, devem ser guardados em um móvel trancado; e

6.3.5.2. Os computadores e terminais devem contar com uma proteção de tela com senha, ou outra forma de autenticação que impeça a visualização não autorizada, quando estiverem sem uso.

6.4. Gestão de Incidentes em Segurança da Informação

6.4.1. A UFSB manterá permanentemente um Grupo de Tratamento de Incidentes de Segurança em Computadores (da sigla em inglês CSIRT), sob gestão da Coordenação de Segurança da Informação e Comunicação com a responsabilidade de receber, filtrar, classificar e responder às solicitações e alertas, além de realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa;

6.4.2. Todos que fazem uso dos ativos de informação da UFSB são responsáveis por notificar ao CSIRT, imediatamente, incidentes que afetem a segurança da informação por meio de recursos de TIC ou o descumprimento desta política, ou dos demais documentos que a complementam, para que as providências sejam devidamente tomadas no sentido de minimizar o impacto negativo a Instituição;

6.4.3. Os incidentes de segurança da informação devem ser identificados, registrados, adequadamente tratados e monitorados por meio de um processo formalizado e que deve observar as regras a serem definidas em uma norma específica sobre o tema; e

6.4.4. O CSI deve aprovar metodologias e normas que estabeleçam processos de gestão para tratamento e resposta a incidentes de segurança da informação, conforme definido pela CoSIC;

6.5. Gestão de Ativos

6.5.1. A gestão de ativos de informação da UFSB deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua;

6.5.2. O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação;

6.5.3. Os ativos de informação devem:

6.5.3.1. ser inventariados e protegidos;

6.5.3.2. ter identificados os seus gestores e custodiantes;

6.5.3.3. ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

6.5.3.4. ter a sua entrada e saída nas dependências da UFSB autorizadas e registradas por autoridade competente;

6.5.3.5. 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; e

6.5.3.6. ser regulamentados por norma específica quanto à sua utilização.

6.5.4. O CSI 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;

6.5.5. Os ativos de informação devem ser protegidos contra quebra de segurança, independente do meio de armazenamento, processamento ou transmissão utilizado;

6.5.6. O acesso dos usuários aos ativos de informação e sua utilização deve ser condicionado ao aceite e assinatura do Termo de Responsabilidade, sem prejuízo do princípio do consentimento tácito;

6.5.7. Todo e qualquer dispositivo de armazenamento de dados que tenha sua custódia modificada deverá passar por análise da equipe da PROTIC ou equipe por ela delegada. As informações restritas ou privadas que dizem respeito a UFSB deverão ser analisadas, verificadas, devidamente transferidas para repositório adequado e sua posterior exclusão. Este processo será detalhado em norma específica. Esse tratamento não será realizado com os dados do usuário que estiverem salvaguardados nestes dispositivos. O próprio usuário deverá realizar o tratamento das suas informações individuais antes da devolução do ativo;

6.5.8. A documentação dos ativos deverá fornecer subsídios para a sua recuperação após um desastre;

6.5.9. As regras de documentação dos ativos serão definidas em normas específicas;

6.5.10. Os ativos de informação são de responsabilidade do seu gestor, ou de alguém por ele designado, que ficará encarregado pela operação adequada e observância desta política e de suas normas complementares, bem como pela notificação de qualquer evento que aconteça a eles;

6.5.11. Os ativos de TIC são de responsabilidade da PROTIC, ou de alguém por ela designado, que ficará encarregada pela sua alocação, documentação e manutenção;

6.5.12. A instituição deverá adotar as medidas necessárias para que os responsáveis pelos ativos possam geri-los adequadamente, cabendo ao gestor do ativo solicitar os recursos necessários para tal;

6.5.13. Os ativos de informação armazenados nos equipamentos utilizados pelos usuários (computadores, dispositivos móveis, dispositivos de armazenamento externo, entre outros) são de sua responsabilidade, cabendo aos mesmos adotar as medidas necessárias para realizar as cópias de segurança desses ativos de informação e proceder à sua recuperação em caso de perda; e

6.5.14. As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da UFSB devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo a esta política, e devem ser regidas por normas específicas, as quais contemplarão recomendações sobre o uso desses dispositivos.

6.6. Ativos de Software

6.6.1. A instalação de ativos de software em equipamentos da instituição deve ser notificada a PROTIC, que manterá um inventário de ativos de software a fim de controlar as licenças de uso, avaliar os requisitos de segurança e emitir alertas sobre atualizações críticas;

6.6.2. Antes da utilização de um novo ativo de software no ambiente do Centro de Dados da UFSB a CoSIC identificará os responsáveis pela definição e validação dos requisitos de segurança que o software deverá atender;

6.6.3. Os requisitos de segurança deverão ser definidos logo no início de qualquer projeto de desenvolvimento ou aquisição de software;

6.6.4. Deverá ser definida a execução de testes de segurança pela contratada e/ou pela equipe de desenvolvimento da PROTIC sob supervisão da CoSIC antes da utilização do software em ambiente de produção;

6.6.5. Fica estabelecida a obrigatoriedade da monitoração antes da implantação de qualquer software no ambiente do Centro de Dados da instituição, não sendo permitido que passe a operar enquanto perdurar qualquer falha de segurança considerada crítica;

6.6.6. O tratamento das vulnerabilidades constitui um dos requisitos para a aceitação do software;

6.6.7. É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir esta política, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes; e

6.6.8. Será permitida mediante solicitação formal ao CSI a administração do inventário por parte de unidades da Instituição que atendam a requisitos a serem determinados por norma específica.

6.7. Ativos Físicos

6.7.1. Cabe ao gestor do ativo físico a supervisão da utilização em conformidade com os procedimentos para o uso e controle elaborados pela equipe da PROTIC ou equipe por ela delegada;

6.7.2. Cabe ao custodiante de ativo físico zelar pelo cumprimento dos procedimentos operacionais padrão recomendados pela equipe da PROTIC ou equipe por ela delegada;

6.7.3. Todos os ativos de informação que possua a funcionalidade de registro de históricos de eventos (logs), devem ser configurados para armazená-los em formato que permita a identificação das operações mais críticas;

6.7.4. Os registros devem ser armazenados pelo período mínimo de 1 (um) ano, sem prejuízo de outros prazos previstos em normativos específicos; e

6.7.5. Quando possível os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio de tecnologia aplicável.

6.8. Segurança em Recursos Humanos

6.8.1. Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação;

6.8.2. Os usuários devem ter ciência:

6.8.2.1. das ameaças e preocupações relativas à SI; e

6.8.2.2. de suas responsabilidades e obrigações no âmbito desta política e normas que a complementam.

6.8.3. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em SI que alcancem todos os usuários da UFSB, de acordo com suas competências funcionais;

6.8.4. Os usuários devem ser sensibilizados e conscientizados para apoiar esta política no exercício das suas atribuições;

6.8.5. Não se deve discutir ou comentar assuntos confidenciais ou sensíveis da UFSB em locais públicos ou por meio de mensagens de qualquer tipo em redes sociais ou qualquer outro meio que não garanta sigilo.

6.9. Utilização de Equipamentos Pessoais

6.9.1. Equipamentos pessoais, como computadores ou quaisquer dispositivos que possam armazenar e/ou processar dados, não devem ser usados para armazenar e/ou processar informações que sejam classificadas como sensíveis para a atividade da UFSB, sem prévia autorização expressa do gestor do ativo de informação ou autoridade diretamente superior.

6.10. Termo de Responsabilidade e Sigilo

6.10.1. O Termo de Responsabilidade e Sigilo é o documento oficial de comprometimento com a SI e deve ser firmado por todos os usuários dos ativos de informação na UFSB;

6.10.2. Como linhas gerais para a confecção do Termo de Responsabilidade e Sigilo, seus signatários devem assumir o compromisso de:

6.10.2.1. declarar o conhecimento e aceitação dos termos desta política de segurança da informação e de suas políticas e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

6.10.2.2. declarar estar ciente que os acessos realizados por meio da estrutura de Tecnologia da Informação e Comunicação da UFSB são passíveis de auditoria; e

6.10.2.3. manter a confidencialidade de suas credenciais, notificando o Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT) sempre que existir qualquer indício de possível comprometimento, para que sejam tomadas as providências cabíveis.

6.10.3. A assinatura do Termo de Responsabilidade e Sigilo deve preceder do consentimento livre e esclarecido; e

6.10.4. O modelo do Termo de Responsabilidade e Sigilo pode ser localizado no Anexo II desta política.

6.11. Gestão do Uso dos Recursos Operacionais e de Comunicações

6.11.1. O CSI deve estabelecer parâmetros adequados, relacionados à SI, 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 UFSB;

6.11.2. Os acordos de nível de serviço firmados pela UFSB devem ser compatíveis com padrões de governança digital e requisitos de SI;

6.11.3. E-mail

6.11.3.1. Todo servidor docente e/ou técnico-administrativo membro da comunidade acadêmica da UFSB terá o direito de possuir uma, e somente uma, conta de e-mail no domínio @ufsb.edu.br;

6.11.3.2. Fica estabelecido por esta política o *e-mail* sob o domínio @ufsb.edu.br a ferramenta de TIC para comunicações oficiais;

6.11.3.3. O serviço de *e-mail* será usado para atividades acadêmicas e administrativas dos usuários da informação no âmbito da UFSB. As responsabilidades, direitos e penalidades referentes ao uso do *e-mail* serão especificadas por meio de normas complementares.

6.11.4. Acesso à Internet

6.11.4.1. O acesso à Internet no âmbito da UFSB é fornecido para fins diretos e complementares às atividades da instituição, sendo, portanto, passível de registro e auditoria;

6.11.4.2. O acesso à rede mundial de computadores (*Internet*) a partir da infraestrutura de telecomunicações da UFSB deve ser utilizado prioritariamente para atender às atividades acadêmicas e administrativas da instituição, obedecendo à legislação vigente, ficando autorizado, em momentos de picos de uso e degradação do serviço, a aplicação de controles para o alcance desta finalidade;

6.11.4.3. 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;

6.11.4.4. Os serviços de rede no ambiente da UFSB também constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem definidos através de norma específica.

6.11.5. Mídias Sociais

6.11.5.1. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações da UFSB, deve ser regida por normas internas específicas e deve estar em consonância tanto com esta política quanto com os objetivos estratégicos da instituição não sendo permitida a sua utilização em substituição aos meios oficiais de comunicação com o público;

6.11.5.2. Perfis de redes sociais, usuário administrador de sites e portais específicos, pertencentes a alguma das unidades organizacionais da UFSB, devem ser criados, atualizados e descontinuados sob a anuência da Assessoria de Comunicação Social (ACS) da UFSB, sendo o conteúdo publicado nestes canais de responsabilidade do autor da respectiva atualização;

6.11.5.3. Sites e portais específicos, pertencentes a alguma das unidades organizacionais da UFSB, devem ser criados, atualizados e descontinuados sob a anuência da PROTIC devendo estar obrigatoriamente registrado em um domínio da UFSB, sendo o conteúdo publicado nestes canais de responsabilidade do autor da respectiva atualização;

6.11.5.4. O conteúdo acessado ou publicado não pode possuir elementos que possam ser considerados ofensivos, destrutivos, difamatórios ou

pejorativos, incluindo, mas não limitado a comentários ou imagens sexuais, calúnias raciais, ou outros comentários ou imagens que possam ofender alguém por sua raça, classe social, nacionalidade, gênero, orientação sexual, crença religiosa, orientação política ou condição de deficiência; e

6.11.5.5. Não é permitida a utilização de conteúdos de terceiros, sujeitos às leis de direito autoral ou classificadas como informação sensível e/ou confidencial, sem autorização expressa, em qualquer tipo de publicação *on-line* pertencente a alguma das unidades organizacionais da UFSB.

6.11.6. Computação em Nuvem

6.11.6.1. O uso de recursos de Computação em Nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo a determinações desta politica, e demais orientações governamentais e legislação em vigor, com vistas a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas na nuvem, em especial aquelas sob custódia e gerenciamento de terceiros;

6.12. Controles de Acesso

6.12.1. Todos os sistemas de informação da UFSB, automatizados ou não, devem possuir um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso aos ativos de informação;

6.12.2. As atribuições de acesso devem seguir o princípio de privilégio mínimo;

6.12.3. 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 pelo ativo de informação;

6.12.4. O controle de acesso ao ativo de 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;

6.12.5. Devem ser registrados eventos relevantes, previamente definidos, para fins de segurança e rastreamento de acesso às informações;

6.12.6. Devem ser criados mecanismos para garantir a exatidão das trilhas de auditoria nos ativos de informação;

6.12.7. Os usuários da UFSB são responsáveis por todos os atos praticados com suas identificações, tais como: credenciais de acesso, crachás, carimbos, correio eletrônico e assinaturas digitais;

6.12.8. É de responsabilidade do usuário notificar o CSIRT da UFSB ao perceber que possui nível de acesso mais amplo do que o estritamente necessário para o exercício de suas atividades;

6.12.9. Sempre que houver mudança de lotação ou cargo de determinado usuário, a PROGEPE deverá notificar a CoSIC para que os privilégios de acesso às informações e aos recursos computacionais sejam readequados imediatamente, devendo ser cancelados em caso de desligamento da função ou cargo mesmo que ainda na UFSB, ou bloqueados em caso de afastamento;

6.12.10. Os ativos de software de uso institucional da UFSB 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, e quais forem necessários para a devida proteção dos ativos de informação;

6.12.11. O CSI definirá o Plano de Controle de Acesso que estabeleça procedimentos para a identificação dos ativos de informação com acesso controlado, assim como dos usuários que devem ter privilégio de acesso, e às áreas físicas protegidas contra o acesso de pessoas não autorizadas.

6.13. Classificação da Informação

6.13.1. O usuário apenas acessará os ativos de informação os quais são permitidos ao seu nível de acesso; e

6.13.2. Se por algum motivo houver falha no controle de segurança e for disponibilizado ao usuário algum ativo de informação ao qual ele não deveria ter acesso, o ativo não deve ser acessado e o CSIRT deve ser notificado.

6.14. Criptografia

6.14.1. O usuário é responsável pelo recurso criptográfico que receber; e

6.14.2. O CSI deve normatizar o uso de recursos criptográficos no âmbito das informações produzidas e custodiadas pela UFSB, com as orientações contidas em norma específica;

6.15. Gestão de Riscos

6.15.1. O CSI deve estabelecer um processo de Gestão de Riscos de Segurança da Informação (GRSI) que possibilite identificar ameaças e reduzir vulnerabilidades e impactos aos ativos de informação, alinhado com a Gestão de Riscos Institucional;

6.15.2. A GRSI é um processo contínuo e deve ser aplicado na implantação e operação do Sistema de Gestão de Segurança da Informação (SGSI), levando em consideração o planejamento, a execução, a análise crítica e a melhoria da SI na instituição;

6.15.3. As unidades administrativas e acadêmicas da UFSB devem colaborar com o CSI, fornecendo as informações por ele solicitadas, de modo a viabilizar o processo de GRSI;

6.15.4. Um Plano de Gestão de Riscos de Segurança da Informação deve ser elaborado e mantido pelo CSI, com base na legislação vigente, contendo necessariamente uma lista das ameaças mais prováveis e suas ocorrências, uma classificação dos riscos e alternativas para mitigá-los.

6.16. Gestão de Continuidade

6.16.1. Faz-se necessária a adoção de um conjunto de procedimentos emergenciais, através da definição de um Sistema de Gestão de Continuidade de Negócios (SGCN), para a eventualidade da ocorrência de algum incidente de segurança da informação que possa causar interrupção na continuidade de processos organizacionais da UFSB, decorrentes de desastres ou falhas em recursos de TIC;

6.16.2. O CSI deve manter atualizado um Plano de Continuidade do Negócio, cujas medidas visem minimizar os impactos sofridos pelos ativos de informação da UFSB diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que retornem à normalidade;

6.16.3. A resiliência contra possíveis interrupções na capacidade de atingir os principais objetivos institucionais deve ser prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional da UFSB.

6.17. Auditoria e Conformidade

6.17.1. A CoSIC 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 UFSB;

6.17.2. Deve ser realizada, periodicamente, a verificação de conformidade das práticas de SI da UFSB e de suas unidades com esta política e suas normas complementares, bem como com a legislação específica de SI, conforme diretrizes definidas em normas específicas;

6.17.3. O CSI manterá um Plano de Auditoria e Conformidade que deverá incluir métodos, técnicas, procedimentos, normas e responsabilidades para o efetivo cumprimento do estabelecido por esta Política de Segurança da Informação no âmbito da UFSB;

6.17.4. Todos os ativos de informação no âmbito da UFSB são passíveis de auditoria técnica a cargo da PROTIC, ou equipe por ela designada, segundo Plano de Auditoria e Conformidade; e

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

6.18. Propriedade Intelectual

6.18.1. Os ativos de informação produzidos no âmbito da UFSB por usuários internos, colaboradores e prestadores de serviço, no exercício de suas funções, são patrimônio intelectual da UFSB;

6.18.2. É vedada a utilização de informações produzidas para uso exclusivo da UFSB em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela instituição, salvo com autorização específica pelos gestores dos ativos de informação, nos processos e documentos de sua competência; e

6.18.3. Todos os usuários devem atentar-se a legislação vigente no país sobre direitos autorais, propriedade industrial e a política institucional de inovação e normas relacionadas.

7. Penalidades

7.1. As ações que violem os princípios desta POSIN ou quaisquer de suas diretrizes, normas e procedimentos, ou que quebrem os controles de SI, serão devidamente apuradas pelo CSI e encaminhadas ao CGD para que sejam aplicadas as sanções administrativas, sem prejuízo das sanções civis e penais a serem aplicadas pelos órgãos competentes;

8. Política de Atualização

8.1. A Política de Segurança da Informação da UFSB deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

9. Divulgação e acesso à estrutura normativa

9.1. Esta política e suas normas complementares devem ser amplamente divulgadas a todos os usuários de ativos de informação da UFSB e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

10. Disposições finais

10.1. Ficam instituídos os seguintes e-mails como canais oficiais de comunicações sobre o tema de Segurança da Informação na UFSB:

10.1.1. comite.si@ufsb.edu.br, para as comunicações de gestão do programa de segurança da informação da instituição. O acesso de administrador desta conta deverá ser atribuído ao Gestor de Segurança da Informação que coordenará o CSI, e compartilhado com os demais membros do comitê em modo de somente leitura. Na ocorrência de qualquer mudança na constituição deste comitê, os acessos deverão ser imediatamente revisados; e

10.1.2. csirt@ufsb.edu.br, para comunicações de ocorrência de incidentes de segurança da informação no âmbito da UFSB. O acesso de administrador desta conta deverá ser atribuído ao titular da Coordenação de Segurança da Informação e Comunicação que coordenará o CSIRT, e compartilhado com os demais membros do grupo em modo de somente leitura. Na ocorrência de qualquer mudança na constituição deste grupo, os acessos deverão ser imediatamente revisados.

11. Vigência

11.1. Esta política entra em vigor na data de sua publicação e tem prazo de validade de 3 anos ou até a edição de outro marco normativo que a atualize ou a revogue.

Anexo I - Referências Legais e Normativas

- Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências;
- Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;
- Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco Civil da Internet;
- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências;
- Decreto nº 7.724, de 16 de maio de 2012 que Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § do art. 216 da Constituição;
- Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento; Decreto nº 7.845, de 14 de novembro de 2012 que regulamenta os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Decreto nº 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação no âmbito da administração pública federal;
- Decreto nº 9.832, de 12 de junho de 2019 que Altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação;
- Decreto nº 10.160 de dezembro de 2019, que Institui a Política Nacional de Governo Aberto e o Comitê Interministerial de Governo Aberto;
- Decreto nº 10.222 de 5 de fevereiro de 2020 institui a Estratégia Nacional de Segurança Cibernética - E-Ciber que é orientação manifesta do Governo federal à sociedade brasileira

sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023;

- Decreto nº 10.332 de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;
- Decreto nº 10.641, de 2 de março de 2021 que altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.
- Instrução Normativa nº 01 da Secretaria de Governo Digital/ME, de 04 de Abril de 2019, que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;
- Instrução Normativa nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- Instrução Normativa nº 2 de 24 de julho de 2020 do Gabinete de Segurança Institucional da Presidência da República que Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- Norma ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. ABNT, 2013;
- Norma ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2013;
- Norma ABNT NBR ISO/IEC 27005 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. ABNT, 2011;
- Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01) Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicação - GRSIC nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 37, de 25 Fev. 2013 - Seção 1;

- Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 Ago. 2009 - Seção 1;

- Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicação, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 223, de 23 Nov. 2009 - Seção 1;

- Norma Complementar nº 07/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicação, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 Jul. 2014 - Seção 1;

- Norma Complementar nº 08/IN01/DSIC/GSIPR, estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 162, de 24 Ago. 2010 - Seção 1;

- Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 02) Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicação, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 Jul. 2014 - Seção 1;

- Norma Complementar nº 10/IN01/DSIC/GSIPR, estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicação (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1;

- Norma Complementar nº 11/IN01/DSIC/GSIPR, estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicação (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1;

- Norma Complementar nº 12/IN01/DSIC/GSIPR, estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicação (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1;

- Norma Complementar nº 13/IN01/DSIC/GSIPR, estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicação (SIC) nos

órgãos e entidades da Administração Pública Federal, direta e indireta (APF). Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1;

- Norma Complementar nº 14/IN01/DSIC/GSIPR, estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicação (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1;
- Norma Complementar nº 15/IN01/DSIC/GSIPR, estabelece diretrizes de Segurança da Informação e Comunicação para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 119, de 21 Jun. 2012 - Seção 1;
- Norma Complementar nº 16/IN01/DSIC/GSIPR, estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. Publicada no DOU Nº 224, de 21 Nov. 2012 - Seção 1;
- Norma Complementar nº 17/IN01/DSIC/GSIPR, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicação (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Publicada no DOU Nº 68, de 10 Abr. 2013 - Seção 1;
- Norma Complementar nº 18/IN01/DSIC/GSIPR, estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicação (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Publicada no DOU Nº 68, de 10 abril 2013 - Seção 1;
- Norma Complementar nº 19/IN01/DSIC/GSIPR, Estabelece Padrões Mínimos de Segurança da Informação e Comunicação para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 Jul. 2014 - Seção 1;
- Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicação para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 242, de 15 Dez 2014 - Seção 1;
- Norma Complementar nº 21/IN01/DSIC/GSIPR, estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1;
- Política de Uso da Rede IPÊ, elaborada pelo Comitê Gestor da RNP, em outubro de 2007.

Anexo II - Termo de Responsabilidade e Sigilo

Eu, _____, usuário (a) dos ativos de informação da Universidade Federal do Sul 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 – POSIN, publicada eletronicamente em https://ufsb.edu.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 administrativas, bem como em responsabilização administrativa, civil e criminal, quando aplicável.

Declaro também ciência de que os meus dados pessoais presentes neste documento serão registrados e operados com a finalidade de identificação do usuário no caso de violação de qualquer dos termos da POSIN e/ou de suas normas complementares e legislações ou da ocorrência de incidente de segurança que esteja relacionado ao meu usuário e/ou ativos de informação da UFSB sob os meus cuidados.

_____, _____de _____ de 20_____.

_____

Assinatura