UNIVERSIDADE FEDERAL DE MINAS GERAIS
GABINETE DA REITORA

OFÍCIO Nº 1117/2022/GAB-REI-UFMG

Belo Horizonte, 11 de outubro de 2022.

Ao Senhor

Prof. Dorgival Olavo Guedes Neto

Diretor de Tecnologia da Informação da UFMG (DTI/UFMG)

Assunto: Política de Segurança da Informação da UFMG.

Senhor Diretor,

Com nossos cordiais cumprimentos, comunicamos a V.Sa. que o Comitê de Governança Digital aprovou a Política de Segurança da Informação da Universidade Federal de Minas Gerais (UFMG), na reunião realizada no dia 26 de setembro de 2022.

Agradecendo a sua constante colaboração, despedimo-nos.

Atenciosamente,

Profa. Sandra Regina Goulart Almeida

Reitora

Documento assinado eletronicamente por **Sandra Regina Goulart Almeida**, **Reitora**, em 13/10/2022, às 19:08, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1826550** e o código CRC **3C19D580**.

Política de Segurança da Informação (POSIN-UFMG)

Documento elaborado pela Diretoria de Tecnologia da Informação, a pedido do Comitê de Governança Digital da Universidade Federal de Minas Gerais, e aprovado pelo comitê em reunião realizada no dia 26 de setembro de 2022, conforme o Ofício nº 1.117 do Gabinete da Reitoria, de 11 de outubro de 2022.

1. Introdução

A segurança da informação visa proteger as informações, sistemas, recursos e outros ativos contra desastres, problemas e manipulação indevida, para reduzir as chances e impactos de incidentes de segurança, envolvendo diversas áreas do conhecimento.

Para garantir a segurança da informação, além da área de tecnologia da informação e comunicações, também é necessário o envolvimento das demais estruturas organizacionais, pessoas, processos, regulamentações, ambiente e sua cultura, entre outros.

Para fins da Política Nacional de Segurança da Informação, instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018 e suas alterações, a segurança da informação no âmbito da Administração Pública Federal abrange:

I. segurança cibernética;
II. defesa cibernética;
III. segurança física;
IV. proteção de dados organizacionais; e
V. ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Para atender aos requisitos de segurança da informação, os órgãos e entidades da Administração Pública Federal devem planejar e realizar continuamente a gestão da segurança da informação, mantendo o alinhamento com a evolução da tecnologia e de seus riscos e identificando os fatores internos e externos que possam impactar no alcance dos objetivos institucionais.

Com o objetivo de manter uma gestão da segurança da informação eficaz, possuem extrema relevância o planejamento estratégico eficiente e, principalmente, o patrocínio da alta gestão.

2. Estrutura da Política de Segurança da Informação da UFMG

A Política de Segurança da Informação da UFMG (POSIN-UFMG) é integrada pelos seguintes tipos de instrumentos normativos, de níveis hierárquicos distintos:

I. Política de Segurança da Informação: define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
II. Normas de Segurança da Informação: identificam obrigações e procedimentos em conformidade com as diretrizes gerais da Política de Segurança da Informação; e
III. Procedimentos de Segurança da Informação: detalham a implementação dos controles de segurança da informação necessários previsos na Política e nas Normas de Segurança da Informação.

Poderão integrar a POSIN-UFMG outros documentos, manuais, orientações, planos, políticas e demais instrumentos normativos que complementem a matéria.

3. Finalidade

A POSIN-UFMG provê orientação e apoio para a segurança da informação na UFMG de acordo com as necessidades da instituição, conforme as leis, normas técnicas e regulamentações vigentes.

Este documento estabelece finalidade, conceitos, princípios, estrutura, diretrizes gerais, competências e responsabilidades dentre outras orientações acerca da segurança da informação na universidade, além de fornecer subsídios e direcionamento para a complementação normativa da matéria.

4. Escopo

As obrigações dispostas na POSIN-UFMG regem as ações quanto à segurança da informação no âmbito da Universidade Federal de Minas Gerais, devendo ser observada por todas as pessoas e entidades envolvidas nas atividades da instituição.

5. Conceitos e definições

Os conceitos utilizados neste documento constam, predominantemente, no Glossário de Segurança da Informação, aprovado, publicado e atualizado pelo Gabinete de Segurança Institucional da Presidência da República.

- Acesso à informação: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
- Ativo: qualquer coisa que tenha valor para a organização, material ou não;
- Ativo de informação: meios de armazenamentos, transmissão e processamento da informação ou equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
- Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;
- Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
- Avaliação de conformidade em segurança da informação: exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação com legislações específicas;
- Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov): organização inserida no Departamento de Segurança de Informação (DSI) do

Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

- Classificação da informação: processo para definir a sensibilidade da informação e quem tem acesso a essa informação, permitindo assim definir níveis e critérios de acesso que garantam a segurança da informação;
- Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;
- Conformidade em segurança da informação: cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;
- Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;
- Controles de segurança da informação: medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de *hash*, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros;
- Defesa cibernética: ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente;
- Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
- Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação da instituição;

- Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo 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, a marca da organização e suas atividades de valor agregado;
- Gestão de incidentes: processo voltado a restaurar, em caso de eventos adversos, a operação normal dos serviços com a devida agilidade para garantir os níveis adequados de qualidade e disponibilidade
- Gestão de mudanças: processo voltado a mitigar eventuais resistências e obter mudanças eficazes e eficientes em decorrência da evolução de processos e de tecnologias da informação, considerando a análise crítica de consequências em alterações, independentemente de terem sido planejadas;
- Gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
- Gestão da segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;
- Incidente: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- Incidente de segurança (ou incidente cibernético): qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores ou ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de

informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

- Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- Mapeamento de ativos de informação: processo de estruturação e manutenção de um registro de ativos de informação que contenha proprietários e custodiantes, informações básicas sobre requisitos de segurança, contêineres, interface e interdependência de cada ativo;
- Membro da comunidade UFMG: pessoa física autorizada a acessar os ativos de informação da instituição, incluindo servidores ou equiparados, terceirizados e discentes;
- Mudança: alteração ou transformação nos processos do negócio, recursos de processamento da informação ou nos sistemas da organização;
- Não repúdio: propriedade pela qual se previne uma origem ou destino de negar a transmissão de mensagens, isto é, quando dada mensagem é enviada, o destino pode provar que esta foi realmente enviada por determinada origem, e vice-versa;
- Partes externas: pessoas físicas e jurídicas externas à UFMG autorizadas a acessar ativos de informação da instituição;
- Política de Segurança da Informação da UFMG (POSIN-UFMG): este documento e os demais instrumentos normativos;
- Processamento da informação: submeter uma informação a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;
- Recurso humano: servidor, terceirizado ou equiparado, ou similar que desempenhe atividades de trabalho ou acadêmicas no âmbito da instituição;
- Rede Federal de Gestão de Incidentes Cibernéticos: organismo cuja finalidade é proporcionar a prevenção contra ameaças cibernéticas e de elevar o nível de resiliência em segurança cibernética dos ativos de informação, estimulando a integração e a cooperação institucional entre os órgãos e entidades da administração pública federal direta, autárquica e fundacional;

- Requisitos de segurança da informação: parâmetros definidos levando-se em consideração a análise e avaliação dos riscos na organização, legislação vigente, estatutos, regulamentações e cláusulas contratuais, princípios, objetivos e requisitos de negócio para o processamento de dados que a organização deve definir para dar suporte às suas operações;
- Segurança cibernética: ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;
- Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- Segurança física e do ambiente: ações que envolvem pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas; e
- Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

6. Princípios

6.1. estar em conformidade com as normas da legislação brasileira em vigência;

6.2. promover o respeito aos direitos humanos e às garantias fundamentais, de forma a assegurar a liberdade de expressão, o acesso à informação e a proteção dos dados e da privacidade;

6.3. subsidiar a condução e execução das ações de segurança da informação, em consonância com os objetivos estratégicos, processos internos, requisitos legais e estrutura da instituição;

6.4. observar as orientações fornecidas aos órgãos e entidades da Administração Pública Federal quanto a segurança da informação;

6.5. reforçar o compromisso da instituição no que se refere ao tratamento e a proteção da informação;
6.6. garantir à informação tratada os atributos de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade;
6.7. fomentar a cultura em segurança da informação;
6.8. propiciar o intercâmbio de conhecimentos relacionados à segurança da informação entre os órgãos e pessoas que atuam na universidade; e
6.9. estimular a integração e a cooperação entre os órgãos e as pessoas nas ações de segurança da informação.

7. Diretrizes gerais

7.1. Tratamento da Informação

Cabe à UFMG classificar a informação tratada no âmbito da instituição. O tratamento de toda e qualquer informação deve garantir os níveis de proteção adequados conforme sua classificação e as regras estabelecidas pela POSIN-UFMG.

7.2. Segurança Física e do Ambiente

Cabe à UFMG implementar os controles necessários para impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações, além de prevenir o acesso físico não autorizado, danos e interferências nas informações e em seus recursos de processamento da organização.

7.3. Gestão de Incidentes em Segurança da Informação

Cabe à UFMG regulamentar, planejar e realizar a gestão de incidentes em segurança da informação com o objetivo de implantar processos, disponibilizar recursos e executar ações de prevenção, tratamento e resposta a qualquer evento adverso relacionado à segurança da informação.

Os incidentes de segurança da informação devem ser comunicados à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), cujas responsabilidades e competências estão definidas em seção específica neste documento.

7.4. Gestão de Ativos de Informação

Cabe à UFMG regulamentar, planejar e executar o processo de mapeamento de ativos de informação com o objetivo de subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

7.5. Segurança em Recursos Humanos

Cabe à UFMG implementar os controles adequados para assegurar que os recursos humanos e partes externas estejam em conformidade com suas atribuições, estejam conscientes e cumpram com as suas responsabilidades pela segurança da informação, antes e durante a contratação.

Cabe à UFMG implementar os controles adequados para proteger os interesses da instituição em caso de mudança ou encerramento da contratação de recursos humanos e partes externas.

7.6. Gestão do Uso dos Recursos Operacionais e de Comunicações

Os recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros, devem ser destinados, exclusivamente, a fins diretos e complementares às atividades administrativas e acadêmicas da instituição.

A UFMG reserva-se o direito de monitorar e controlar o uso dos recursos operacionais e de comunicações disponibilizados, assim como revogar permissões de acesso caso sejam identificadas irregularidades.

7.7. Controles de Acesso

Cabe à UFMG regulamentar, planejar, implantar e gerenciar controles físicos e lógicos adequados para restringir o acesso à informação e aos recursos de processamento da informação às pessoas e entidades devidamente autorizadas, como forma de prevenção de incidentes de segurança.

7.8. Gestão de Riscos de Segurança da Informação

A gestão de riscos de segurança da informação tem a finalidade de adequar os riscos aos níveis aceitáveis pela instituição.

Cabe à UFMG elaborar o Plano de Gestão de Riscos de Segurança da Informação. Além disso, deve ser implementado e executado o processo de gestão de riscos de segurança da informação em compatibilidade com a gestão de riscos institucional, a missão e os objetivos estratégicos da universidade, os processos internos, os requisitos legais e a POSIN-UFMG.

7.9. Gestão de Continuidade de Negócios em Segurança da Informação

A gestão de continuidade de negócios tem a finalidade de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Cabe à UFMG elaborar o Plano de Gestão de Continuidade de Negócios em Segurança da Informação. Além disso, deve ser implementado e executado o processo de gestão de continuidade de negócios em segurança da informação com base nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio.

7.10. Gestão de Mudanças nos aspectos de Segurança da Informação

A gestão de mudanças nos aspectos de segurança da informação tem a finalidade de mitigar eventuais resistências e obter mudanças eficazes e eficientes em decorrência da evolução de processos e de tecnologias da informação.

Cabe à UFMG regulamentar, planejar e executar o processo de mudanças nos aspectos de segurança da informação, respaldando-se no processo de gestão de riscos de segurança da informação.

7.11. Auditoria e Conformidade

Cabe à UFMG propiciar e subsidiar as condições necessárias para a realização de auditoria e avaliação de conformidade nos aspectos de segurança da informação, de acordo com a legislação vigente e as diretrizes institucionais.

8. Competências e responsabilidades

8.1. Comitê de Governança Digital (CGD):

8.1.1. deve nomear, como seu subcomitê, o Comitê Gestor da Segurança da Informação (CGSI);

8.1.2. designar um gestor de segurança da informação; e

8.1.3. deliberar, quando necessário, sobre os casos encaminhados pelo CGSI.

8.2. Comitê Gestor da Segurança da Informação (CGSI):

8.2.1. assessorar a implementação das ações de segurança da informação;

8.2.2. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

8.2.3. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

8.2.4. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

8.2.5. deliberar sobre normas internas de segurança da informação; e

8.2.6. constituir, designar atribuições e escopo de atuação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares, com capacitação técnica compatível com as atividades dessa equipe, cuja participação na Rede Federal de Gestão de Incidentes Cibernéticos é obrigatória.

8.3. Gestor de Segurança da Informação:

8.3.1. coordenar o Comitê Gestor da Segurança da Informação ou estrutura equivalente;

8.3.2. 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;

8.3.3. assessorar a alta administração na implementação da Política de Segurança da Informação;

8.3.4. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

8.3.5. 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;

8.3.6. incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

8.3.7. propor recursos necessários às ações de segurança da informação;

8.3.8. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

8.3.9. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

8.3.10. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

8.3.11. 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.

8.4. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR):

8.4.1. receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

8.4.2. desenvolver as atividades de prevenção, tratamento e resposta a incidentes de segurança da informação;

8.4.3. notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) sobre a ocorrência de qualquer incidente de segurança, seguindo os formatos e procedimentos estabelecidos pelo CTIR Gov; e

8.4.4. trocar informações acerca de segurança da informação com as demais Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos existentes, seguindo os formatos e procedimentos estabelecidos pelo CTIR Gov.

8.5. Dirigentes e chefias da UFMG:

8.5.1. garantir que as atividades desempenhadas sob sua gestão estejam de acordo com a POSIN-UFMG;

8.5.2. promover a capacitação dos recursos humanos sob sua gestão em temas relacionados à segurança da informação;

8.5.3. alocar os recursos necessários às ações de segurança da informação no seu âmbito de atuação;

8.5.4. acompanhar a execução das ações de segurança da informação no seu âmbito de atuação;

8.5.5. garantir a transmissão e a guarda de dados exclusivamente em infraestrutura provida ou homologada pela UFMG;

8.5.6. garantir a utilização exclusiva dos recursos, serviços e sistemas de tecnologia da informação providos ou homologados pela UFMG, ainda que haja alternativas gratuitas;

8.5.7. estimular a cultura de segurança da informação; e

8.5.8. disseminar normas e boas práticas de segurança da informação.

8.6. Membros da comunidade UFMG, demais recursos humanos e partes externas:

8.6.1. estar ciente e cumprir diretrizes, princípios e regras estabelecidas pela POSIN-UFMG, incluindo suas atualizações;

8.6.2. guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades;

8.6.3. zelar pelo sigilo e integridade das informações e dos ativos aos quais tiver acesso;

8.6.4. adotar boas práticas de segurança da informação;

8.6.5. responder por seus atos e acessos que causem danos ou prejuízos às informações e aos ativos no âmbito da instituição, ou violem as regras dispostas na POSIN-UFMG ou em seus instrumentos complementares;

8.6.6. respeitar a legislação e as normas de propriedade intelectual pertinentes;

8.6.7. respeitar a legislação e as normas de proteção de dados e privacidade de informações pessoais pertinentes;

8.6.8. comunicar à UFMG sempre que tomar ciência de evento adverso que possa configurar incidente de segurança da informação; e

8.6.9. armazenar e preservar as informações em infraestrutura provida pela instituição, ou em nuvem, desde que aprovada e homologada pela UFMG;

8.6.10. utilizar exclusivamente os recursos, serviços e sistemas de tecnologia da informação providos ou homologados pela UFMG, ainda que haja alternativas gratuitas;

8.6.11. propor melhorias à segurança da informação no âmbito da instituição.

9. Penalidades

O descumprimento das regras da POSIN-UFMG implicará em sanções administrativas nos termos da lei, normas complementares, regimentos e resoluções internas, sem prejuízo de outras penalidades previstas nas esferas cível e penal.

10. Atualização

Este documento e os demais instrumentos normativos que integram a POSIN-UFMG devem ser revistos e atualizados sempre que necessário ou a cada 2 anos.

11. Disposições Finais

Os casos omissos devem ser encaminhados e avaliados pelo Comitê Gestor da Segurança da Informação.

12. Referências e fundamentação legal

- Constituição da República Federativa do Brasil de 1988;
- Decreto nº 9.637, de 26 de dezembro de 2018;
- Decreto nº 10.748, de 16 de julho de 2021;
- Instrução Normativa nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República;
- Instrução Normativa nº 2, de 24 de julho de 2020 do Gabinete de Segurança Institucional da Presidência da República;
- Instrução Normativa nº 3, de 28 de maio de 2021 do Gabinete de Segurança Institucional da Presidência da República;
- Portaria nº 93, de 18 de outubro de 2021 do Gabinete de Segurança Institucional da Presidência da República;
- Portaria nº 259, de 29 de novembro de 2018 do Gabinete da Reitoria da UFMG;
- Norma técnica ABNT NBR ISO IEC 27001:2013, lançada em 08 de novembro de 2013;
- Norma técnica ABNT NBR ISO IEC 27002:2013, lançada em 08 de novembro de 2013;
- Norma técnica ABNT NBR ISO IEC 27701:2019, lançada em 09 de dezembro de 2019; e
- Apostila *Gestão da Segurança da Informação: NBR 27001 e NBR 27002* (Escola Superior de Redes da Rede Nacional de Ensino e Pesquisa).