EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES
SCS Quadra 9, Edifício Parque Cidade Corporate, Torre C, 1° ao 3° andares - Bairro Asa Sul
Brasília-DF, CEP 70308-200
(61) 3255-8900 - http://www.ebserh.gov.br

Norma Operacional - SEI nº 6/2022/SGTI/DTI-EBSERH

Brasília, *data da assinatura eletrônica*.

NORMA OPERACIONAL DE USO SEGURO DE COMPUTAÇÃO EM NUVEM PELA REDE EBSERH

Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pela Rede Ebserh.

A **DIRETORA DE TECNOLOGIA DA INFORMAÇÃO** da Empresa Brasileira de Serviços Hospitalares - Ebserh, no uso das atribuições institucionais que lhe foram conferidas pelo art. 103 do Regimento Interno da Administração Central da Ebserh, aprovado na 137ª Reunião Extraordinária do Conselho de Administração, realizada no dia 14 de junho de 2022, RESOLVE:

Divulgar a presente Norma Operacional que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem no âmbito da Rede Ebserh.

CAPÍTULO I - DAS DISPOSIÇÕES INICIAIS

Seção I - Do Objeto e Âmbito de Aplicação

Art. 1º Esta Norma Operacional dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem no âmbito da Rede Ebserh.

Art. 2º Fica autoriza a utilização e migração de soluções de TI para ambiente de computação em nuvem pela Ebserh, desde que sejam atendidos os requisitos de segurança previstos nesta norma e nas demais legislações que tratam sobre a matéria.

§ 1º A contratação de soluções de computação em nuvem busca garantir benefícios de capacidade, segurança e eficiência em Tecnologia da Informação para a empresa, o que deve ser demonstrado em Estudo Técnico Preliminar, nos termos do Regulamento de Licitações e Contratos da Ebserh (RLCE).

§ 2º A utilização de soluções de TI em ambiente de computação em nuvem deve ser precedida de regular processo de contratação pública, com celebração de contrato, ou de regular processo para celebração de convênio, acordo ou instrumento congênere.

Seção II - Dos Objetivos

Art. 3º O objetivo desta Norma Operacional é definir as diretrizes em relação à computação em nuvem, que são aplicáveis à Rede Ebserh, para garantir a eficiência, o nível de segurança da informação,

privacidade e proteção aos dados pessoais determinados pela legislação competente.

§ 1º Deverão ser observados os requisitos da legislação competente para que a Rede Ebserh adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

§ 2º Esta norma atende ao disposto na Política de Segurança da Informação da Ebserh e nas legislações correlatas, e define as medidas técnicas e administrativas que deverão ser observadas pelos agentes públicos vinculados à Ebserh e por organizações fornecedoras de computação em nuvem.

§ 3º As medidas técnicas e administrativas devem ser aptas a proteger as informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos em legislação.

Seção III - Das Definições

Art. 4º Para fins desta Norma, consideram-se os conceitos constantes no Dicionário de Referência de TI da Ebserh, o Glossário de Segurança da Informação GSI/PR e os que seguem:

I - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN) e é composta pelos:

a) modelos de implantação:

1. nuvem privada (ou interna): infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

2. nuvem comunitária: infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

3. nuvem pública (ou externa): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas; e

4. nuvem híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.

b) tipos de serviço:

1. infraestrutura as a Service (IaaS): tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de criar redes virtuais em seu ambiente de computação, permitindo-lhe selecionar os sistemas operacionais a serem instalados em máquinas virtuais, bem como a estrutura da rede, incluindo o uso de switches virtuais, roteadores e firewalls. O IaaS também fornece total liberdade quanto ao software ou código personalizado executado nas máquinas virtuais.

2. plataforma as a Service (PaaS): tipo de serviço de computação em nuvem, em que o provedor de serviço de nuvem oferece ao cliente a capacidade de operar códigos ou aplicativos personalizados, determinando previamente quais sistemas operacionais ou ambientes de execução são oferecidos, não sendo permitido ao cliente modificar os sistemas operacionais (mesmo patches de segurança) ou alterar o espaço da rede virtual.

3. software as a Service (SaaS): tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de usar um aplicativo fornecido, cabendo ao usuário tão somente usar o aplicativo oferecido e fazer pequenos ajustes de configuração e ao provedor a responsabilidade pela manutenção da aplicação.

II - escritório digital: plataforma para trabalho colaborativo disponibilizada pela Diretoria de Tecnologia da Informação - DTI aos usuários de rede da Ebserh com o objetivo de facilitar a gestão do trabalho e a

interação entre os membros das equipes, independentemente de onde as pessoas estejam localizadas, podendo ser acessado inclusive fora das dependências da Ebserh a partir de computadores ou smartphones.

III - medida administrativa: controle organizacional, físico ou procedimental, obtido por processo que possibilite a conformidade legal e normativa e a confidencialidade, disponibilidade e integridade dos dados pessoais;

IV - medida técnica: controle relacionado à segurança cibernética, obtido por processo que possibilite a conformidade legal e normativa e a confidencialidade, disponibilidade e integridade dos dados pessoais.

CAPÍTULO II - DAS COMPETÊNCIAS E ATRIBUIÇÕES

Seção I - Das Competências

Art. 5º A Diretoria de Tecnologia da Informação compete:

I - monitorar a implantação da norma na Rede Ebserh;

II - definir revisões do ato normativo de uso seguro de computação em nuvem;

III - estabelecer as diretrizes técnicas para utilização de computação em nuvem; e

IV - encaminhar para aprovação da Diretoria Executiva as minutas de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Art. 6º Ao Comitê de Segurança da Informação da Administração Central, mediante apoio técnico da DTI, compete:

I - estabelecer os países nos quais dados e informações custodiados pela Ebserh poderão ser armazenados em soluções de computação em nuvem;

II - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela rede Ebserh, em soluções de computação em nuvem;

III - analisar, em caráter conclusivo, as minutas de revisões do ato normativo sobre o uso seguro de computação em nuvem; e

IV - apoiar o Gestor de Segurança da Informação da Administração Central nas atribuições previstas no art. 12 incisos II, III, IV e V.

Art. 7º Ao Comitê de Segurança da Informação de cada HUF, mediante apoio técnico da área técnica da TI, compete:

I - apoiar nas revisões do ato normativo sobre o uso seguro de computação em nuvem;

II - apoiar o Gestor de Segurança da Informação da Administração Central e do HUF nas competências previstas nos incisos II, III, IV e V do art. 12 e nos incisos II, III, IV e V do art. 13;

Art. 8º Na avaliação sobre a possibilidade de contratação de solução de computação em nuvem competirá à Equipe de Planejamento da Contratação:

I - durante a elaboração do Estudo Técnico Preliminar verificar se a solução pretendida está em conformidade com a presente norma;

II - elaborar e atualizar o mapa de riscos, conforme situações previstas no art. 33, § 2º, do RLCE; e

III - se após a conclusão do Estudo Técnico Preliminar a solução pretendida for baseada em computação em nuvem a Equipe de planejamento da contratação deverá:

a) prever a capacitação da equipe responsável pelo gerenciamento da solução nas tecnologias utilizadas pelo provedor de serviço de nuvem; e

b) enviar o processo de planejamento da contratação para conhecimento do comitê de segurança da informação do HUF e da Administração Central através de despacho contendo relatório de conformidade dos requisitos da presente norma.

Parágrafo único. A avaliação da solução de computação em nuvem será coordenada pelo integrante técnico da área de TI.

Art. 9º À Equipe de Fiscalização do Contrato de solução de computação em nuvem compete:

I - aplicar checklist de verificação de cumprimento dos requisitos da presente norma junto à contratada, pelo menos, uma vez a cada período de 12 meses de contrato;

II - atualizar o mapa de riscos do contrato, caso haja eventos relevantes, durante a fase de Gestão do Contrato;

III - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem ao Comitê de Segurança da Informação ao qual está diretamente vinculada;

IV - enviar via processo relatório de conformidade dos requisitos da presente norma para conhecimento do Comitê de Segurança da Informação da Administração Central; e

V - monitorar e controlar os recursos de computação em nuvem de modo a garantir a continuidade dos serviços.

Parágrafo único. O monitoramento da solução de computação em nuvem será coordenado pelo fiscal técnico da área de TI.

Art. 10. À área responsável por convênios, acordos ou instrumentos congêneres que envolva solução de computação em nuvem, sob supervisão técnica da área de TI, compete:

I - aplicar checklist de verificação de cumprimento dos requisitos da presente norma, pelo menos, anualmente;

II - elaborar mapa de riscos na fase de planejamento da formalização do Convênio, Acordo ou instrumento congênere;

III - atualizar o mapa de risco, caso haja eventos relevantes, durante a fase de Gestão do Convênio, Acordo ou instrumento congênere;

IV - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem ao Comitê de Segurança da Informação ao qual está diretamente vinculada;

V - enviar via processo relatório de conformidade dos requisitos da presente norma para conhecimento do Comitê de Segurança da Informação do HUF e da Administração Central; e

VI - monitorar e controlar os recursos de computação em nuvem de modo a garantir a continuidade dos serviços.

Art. 11. À Diretoria Executiva compete aprovar o ato normativo sobre o uso seguro de computação em nuvem e suas revisões, bem como divulgá-los às partes interessadas.

Seção II - Das Atribuições

Art. 12. São atribuições do Gestor de Segurança da Informação da Administração Central, mediante apoio técnico da DTI:

I - instituir e coordenar a equipe responsável pelas revisões do ato normativo sobre uso seguro de computação em nuvem;

II - supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços a Ebserh, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;

V - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida; e

VI - encaminhar para aprovação da Diretoria de Tecnologia da Informação as minutas de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Art. 13. São atribuições do Gestor de Segurança da Informação de cada Hospital Universitário Federal – HUF, mediante apoio técnico da DTI:

I - sugerir revisões do ato normativo sobre uso seguro de computação em nuvem para o Gestor de Segurança da Informação da Administração Central;

II - supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem no âmbito do HUF;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao HUF, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem no âmbito do HUF, em casos de eventuais desvios;

V - comunicar incidentes cibernéticos, no âmbito do HUF, informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida; e

VI - comunicar incidentes cibernéticos, no âmbito do HUF, informados pelo provedor de serviço de nuvem para o Gestor de Segurança da Informação da Administração Central.

Art. 14. São atribuições dos usuários dos serviços de computação em nuvem:

I - zelar para que as informações que se enquadram no inciso II do caput do Art. 23 não sejam armazenadas serviço de nuvem;

II - zelar para que as informações que se enquadram no inciso III do caput Art. 23 sejam tratadas de forma adequada no ambiente de computação em nuvem; e

III - comunicar a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da Ebserh, caso identifique ou sofra algum incidente cibernéticos no ambiente de nuvem.

CAPÍTULO III - DOS REQUISITOS PARA A ADOÇÂO SEGURA DE COMPUTAÇÂO EM NUVEM

Art. 15. Deverão ser observados os requisitos mínimos deste Capítulo para que a Rede Ebserh adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Seção I - Da transferência de serviços para um provedor de serviço de nuvem

Art. 16. Antes de transferir serviços ou informações para um provedor de serviço de nuvem, a equipe responsável deverá, no mínimo:

I - garantir que as seguintes operações estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros e à Política de Proteção de Dados Pessoais da Ebserh:

a) de coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e

b) de comunicações realizada por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional;

II - realizar o gerenciamento de riscos**,** precedido por análise e relatório de impacto de dados pessoais, em conformidade com a Política de Gestão de Riscos e Controles Internos da Ebserh e a legislação, dos seguintes itens:

a) o tipo de informação a ser migrada;

b) o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;

c) o valor dos ativos envolvidos; e

d) os benefícios da adoção de uma solução de computação em nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro;

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas da Ebserh;

V - avaliar quais informações serão hospedadas na nuvem, considerando:

a) o processo de classificação da informação de acordo com a legislação;

b) o valor do ativo de informação;

c) os controles de acessos físico e lógico relativos à segurança da informação; e

d) o modelo de serviço e de implementação de computação em nuvem;

VI - as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução; e

VII - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

Seção II - Da capacidade do provedor de serviço de nuvem para implementar atualizações

Art. 17. Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a equipe responsável pela solução em nuvem deverá, no mínimo:

I - definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem; e

II - revisar e atualizar periodicamente o mapa de gestão de riscos de segurança da informação.

Seção III - Do gerenciamento de identidades e de registros (logs)

Art. 18. Em relação ao gerenciamento de identidades e de registros, a Rede Ebserh deverá, no mínimo:

I - adotar um padrão de identidade federada para permitir o uso de tecnologia single sign-on no processo de autenticação de seus usuários no provedor de serviço de nuvem;

II - negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação da Ebserh;

III - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia single sign-on , o qual deve ser acompanhado:

a) de autenticação multifator; ou

b) de outra alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem;

IV - exigir do provedor de serviço de nuvem que:

a) registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações; e

b) armazene, pelo período de um ano ou permita o download, de todos os registros de que trata a alínea a.

V - manter em ambiente próprio controlado, pelo período de cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem;

VI - capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem; e

VII - implementar a utilização de senhas fortes.

Seção IV - Do uso de recursos criptográficos

Art. 19. Em relação à necessidade do uso de recursos criptográficos, a equipe responsável pela solução de computação em nuvem deverá, no mínimo:

I - verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação;

II - analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios;

III - utilizar, sempre que possível, chaves de encriptação baseadas em hardware; e

IV - levar em consideração às orientações relacionadas a criptografia da Estratégia Nacional de Segurança da Informação, de que trata o Decreto n.º 9.637, de 26 de dezembro de 2018.

Seção V - Da segregação de dados e da separação lógica

Art. 20. Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, a Rede Ebserh, em conjunto com o provedor de serviço de nuvem, deverá estabelecer, no mínimo, as seguintes ações:

I - garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelos diferentes órgãos ou entidades da administração pública federal e por outros usuários do serviço em nuvem;

II - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

III - garantir a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela administração interna do órgão ou da entidade; e

IV - avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

Seção VI - Do gerenciamento da nuvem

Art. 21. Em relação ao gerenciamento da nuvem, a Rede Ebserh deverá, no mínimo:

I - capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;

II - exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;

III - elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias; e

IV - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Seção VII - Do tratamento da informação

Art. 22. Em relação ao tratamento da informação em ambiente de computação em nuvem, a Rede Ebserh, além de cumprir as orientações contidas na Política De Proteção De Dados Pessoais Da Ebserh, na Política de Classificação de Informação, Sigilo e Temporalidade da Ebserh e na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e

III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) a informação com restrição de acesso prevista na legislação, especialmente na Política de Classificação de Informação, Sigilo e Temporalidade da Ebserh;

b) o material de acesso restrito regulado pela Ebserh;

c) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e

d) o documento preparatório não previsto no inciso II do caput.

Art. 23. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela Ebserh, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia atualizada de segurança, deve ser mantida em território brasileiro e, se possível, em infraestrutura própria da Rede Ebserh;

II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;

III - a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do caput art. 22, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e

IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, na Política de Proteção de Dados Pessoais da Ebserh e demais legislações sobre o assunto;

Seção VIII - Das cláusulas contratuais específicas

Art. 24. O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos estabelecidos nos Art. 16 a Art. 23 além de, no mínimo, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações da Ebserh para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte da Ebserh, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III - proibição do uso de informações da Ebserh pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV - conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem à Ebserh, ao término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema da Ebserh sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e

VII - garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 - LGPD.

CAPÍTULO IV **- DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM**

Art. 25. Para que esteja habilitado a prestar serviços de computação em nuvem para a Rede Ebserh, o provedor de serviço de nuvem deverá cumprir, no mínimo, os seguintes requisitos:

I - possuir metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas e com a legislação, bem como realizar o gerenciamento de riscos descrito no inciso II do art. 9º;

II - implementar práticas de fortalecimento dos mecanismos de virtualização, que devem incluir, no mínimo, os seguintes procedimentos:

a) desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;

b) configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;

c) estabelecer limites para a utilização dos recursos de máquina virtual (Virtual Machine - VM);

d) manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;

e) validar a integridade das operações de gerenciamento de chaves criptográficas;

f) possuir controles que permitam aos usuários autorizados da Ebserh acessarem os registros de acesso administrativo do monitor de máquina virtual - Hypervisor;

g) habilitar o registro completo do Hypervisor; e

h) suportar o uso de máquinas virtuais confiáveis (Trusted VM) fornecidas pela Ebserh, que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem;

III - em relação ao gerenciamento de identidades e registros:

a) possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;

b) impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

c) suportar tecnologia single sign-on para autenticação;

d) suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários da Ebserh no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

e) permitir à Ebserh gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e

f) atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pela Ebserh em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso);

IV - em relação à segurança de aplicações web disponibilizadas no ambiente de nuvem:

a) utilizar firewalls especializados na proteção de sistemas e aplicações;

b) desenvolver código web em conformidade com as melhores práticas de desenvolvimento seguro e com os normativos existentes;

c) utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;

d) realizar periodicamente testes de penetração de redes e de aplicações; e

e) possuir um programa de correção de vulnerabilidades;

V - possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes e com as melhores práticas nessas áreas;

VI - possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;

VII - estabelecer um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS);

VIII - utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelas equipes da Ebserh;

IX - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria da Ebserh;

X - em relação à segregação de dados:

a) isolar, utilizando separação lógica, todos os dados e serviços da Ebserh de outros clientes de serviço em nuvem;

b) segregar o tráfego de gerenciamento do tráfego de dados da Ebserh; e

c) implementar dispositivos de segurança entre zonas;

XI - possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

a) sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;

b) destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction - CEED) e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição; e

c) armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos;

XII - notificar, imediatamente, à Ebserh incidente cibernético contra os serviços ou dados sob sua custódia;

XIII - possuir procedimentos necessários para preservação de evidências, conforme legislação; e

XIV - demonstrar estar em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual Service and Organization Controls 2 (SOC 2), conduzida por um auditor independente, com a apresentação dos relatórios de tipo I e tipo II.

CAPÍTULO V - DA UTILIZAÇÃO DE CLOUD BROKERS

Art. 26. O cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre a Ebserh e dois ou mais provedores de serviço de nuvem.

Art. 27. Caso a Ebserh contrate por meio do cloud broker plataforma de gestão multinuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

I - em relação às funcionalidades de provisionamento e orquestração de multinuvem:

a) um único portal integrado de provisionamentos para o usuário final;

b) utilização de modelos de provisionamento;

c) automação segura de provisionamento simultâneo e utilização, no que couber, de ferramentas de código aberto e interoperáveis;

d) fluxos de trabalho de orquestração baseada em eventos; e

e) soluções seguras integradas de criação de infraestrutura por código - IaaC;

II - em relação às funcionalidades de monitoramento e análise em multinuvem:

a) relatórios de monitoramento de desempenho de recursos na nuvem;

b) coleta e monitoramento de registros; e

c) procedimentos de monitoramento de alertas;

III - em relação às funcionalidades de inventário e classificação em multinuvem:

a) inventário de recursos na nuvem;

b) procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem; e

c) detecção de recursos sem etiqueta; e

IV - em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade:

a) mecanismos de single sign-on e de autenticação multifator das plataformas em nuvem;

b) gerenciamento seguro de usuários e de grupos de usuários;

c) gerenciamento de segurança dos recursos;

d) notificações de eventos de alerta multicanal;

e) gerenciamento de identidade e acesso - IAM; e

f) registros de atividade da plataforma em nuvem.

Parágrafo único. O cloud broker poderá utilizar ferramenta de Software as a Service (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

Art. 28. O cloud broker é o responsável por garantir que os provedores de serviço de nuvem que ele representa:

I - cumpram todos os requisitos previstos nesta Norma e na legislação brasileira; e

II - operem de acordo com as melhores práticas de segurança.

Parágrafo único. À Ebserh deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

CAPÍTULO VI - DISPOSIÇÕES GERAIS

Art. 29. A apresentação dos relatórios de tipo I e tipo II da auditoria SOC 2, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem com à Ebserh.

Parágrafo único. Na hipótese de utilização de cloud broker, esse será o responsável por apresentar os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa.

Art. 30. As áreas da Rede Ebserh que já estiverem utilizando os serviços de provedor de serviço de nuvem terão um prazo de 12 meses, após a entrada em vigor desta Norma, para adequação de seus contratos.

Art. 31. A solução de Escritório Digital da Ebserh utilizará solução de computação em nuvem.

§ 1º Informações compartilhadas ou armazenadas na solução de Escritório Digital pelos usuários da rede devem considerar o disposto nos art. 22 e art. 23.

§ 2º Informações que se enquadram no inciso II do caput art. 22 não poderão ser compartilhadas ou armazenadas na solução de Escritório Digital.

§ 3º Informações que referidas no inciso III do caput art. 22 devem utilizar recurso de criptografia e, caso compartilhadas, deve utilizar a funcionalidade que permite a especificação do(s) usuário(s) com as quais o compartilhamento será realizado.

Art. 32. A solução de e-mail corporativo da Ebserh utilizará solução de computação em nuvem.

§ 1º Informações compartilhadas ou armazenadas na solução de e-mail pelos usuários da rede devem considerar o disposto nos art. 22 e art. 23.

§ 2º Informações que se enquadram no inciso II do caput art. 22 não poderão ser compartilhadas ou armazenadas na solução de e-mail corporativo.

§ 3º Informações referidas no inciso III do caput art. 22, não devem ser expostas no corpo do e-mail e, se anexadas, devem ser criptografadas.

CAPÍTULO VII - DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 33. Para garantir a segurança de que trata esta Norma, a Rede Ebserh poderá adotar outras diretrizes complementares, desde que não confrontem as previsões da legislação.

Art. 34. Esta norma deverá ser revisada, no máximo, a cada dois anos, ou a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

Art. 35. As determinações desta norma aplicam-se a contratações em andamento, contratos existentes e novas contratações de soluções de computação em nuvem e precisam estar adequados a essas

determinações.

Art. 36. O não cumprimento desta norma poderá resultar em apuração de responsabilidade.

Art. 37. Esta norma entra em vigor na data de sua publicação.

(assinado eletronicamente)
SIMONE HENRIQUETA COSSETIN SCHOLZE
Diretora de Tecnologia da Informação

Documento assinado eletronicamente por **Simone Henriqueta Cossetin Scholze**, **Diretor(a)**, em 21/12/2022, às 14:50, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ebserh.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **26499478** e o código CRC **AA5DD0A7**.

Referência: Processo nº 23477.010458/2021-17 SEI nº 26499478