MARCELO HAGGE SIQUEIRA
Secretário Adjunto de Estado de Finanças
Matrícula nº. 300023998

Documento assinado eletronicamente por **Marcelo Hagge Siqueira**, **Secretário(a) Adjunto(a)**, em 05/12/2018, às 09:40, conforme horário oficial de Brasília, com fundamento no caput III, art. 12 do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.sistemas.ro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3942832** e o código CRC **2B2FC1CB**.

Portaria nº 947/2018/SEFIN-ASTEC

O SECRETÁRIO DE ESTADO DE FINANÇAS, no uso das atribuições legais que lhe confere o art. 41, I da Lei Complementar n. 965, de 20 de dezembro de 2017;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação - PSI nos termos dos anexos I e II da Presente Portaria.

Art. 2º Fica instituído, no âmbito da Secretaria de Estado de Finanças – SEFIN/RO, o Grupo de Segurança da Informação – GSI composto pelos seguintes membros:

I – Assessor de Infraestrutura da Gerência de Controle e Informações - GEINF;

II - Assessor de Desenvolvimento da Gerência de Controle e Informações - GEINF;

III - Um membro indicado pela Gerência de Fiscalização - GEFIS;

IV - Um membro indicado pela Gerência de Arrecadação - GEAR;

V - Chefe de TI da Superintendência Estadual de Contabilidade – SUPER;

VI – Um membro indicado pela Gerência de Tributação – GETRI.

Art. 3º Compete ao grupo de Segurança da Informação - GSI:

I - Assessorar na implementação das ações de Segurança da Informação;

II - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

III - Propor alterações na PSI;

IV - Propor Normas de Segurança da Informação - NSI;

V - Propor, solicitar e participar e/ou sugerir membros para Auditorias sobre possíveis descumprimentos da PSI da SEFIN/RO.

Art. 4º Fica instituída, no âmbito da Gerência de Controle e Informações - GEINF, a Equipe de Tratamento e Resposta a Incidentes – ETRI com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas à incidentes em rede de computadores, composto pelos seguintes membros:

I - Assessor de Infraestrutura da Gerência de Controle e Informações - GEINF;

II - Chefe de Suporte da Gerência de Controle e Informações - GEINF;

III - Chefe de Administração de Sistemas da Gerência de Controle e Informações - GEINF;

IV - Chefe de Banco de Dados da Gerência de Controle e Informações - GEINF;

Art. 5º Os usuários dos equipamentos de informática da SEFIN são responsáveis pela segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, tais como crachá, token, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

Art. 6º O titular da unidade administrativa deverá, de imediato, comunicar a GEINF todo incidente de Segurança da Informação - SI que ocorra no âmbito de suas atividades, mediante o envio de relatório circunstanciado.

Art. 7º É dever do servidor da SEFIN/RO conhecer e zelar pelo cumprimento desta PSI.

Art. 8º Todos os servidores da SEFIN/RO são responsáveis pelas ações de SI, observando de forma específica as atribuições pertinentes a cada cargo e /ou função.

Art. 9º Os casos omissos e as dúvidas surgidas na aplicação desta PSI serão analisados, dirimidos ou solucionados pelo Grupo de Segurança da Informação - GSI ou pela Gerência de Controle e Informações – GEINF, conforme o caso.

Art. 10. Esta Portaria entra em vigor na data de sua publicação.

Porto Velho, 05 de Dezembro de 2018.

ANEXO I
Política de Segurança da Informação - PSI

Apresentação da SEFIN/RO

A Secretaria de Estado de Finanças é um órgão do Poder Executivo do Estado de Rondônia responsável, dentre outras atribuições definidas na Lei Complementar Estadual 965/2017, pela formulação da política econômico-tributária, arrecadação e fiscalização dos tributos de competência Estadual, planejamento financeiro, processamento central de despesas públicas, tesouraria, administração da dívida pública, contabilidade geral do Estado, controle interno e prestação geral de contas.

Missão da SEFIN/RO

A Secretaria de Estado de Finanças tem como missão: Gerir as finanças públicas, assegurando a realização da Receita e controlando as Despesas para o desenvolvimento socioeconômico do Estado de Rondônia.

Visão de Futuro da SEFIN/RO

A visão estratégica da Secretaria, conforme exposto no Planejamento Estratégico da Secretaria é: “Ser referência em eficiência, eficácia e efetividade, no cumprimento das suas atribuições, dentre os órgãos que compõe a Administração Pública do Estado de Rondônia, até dezembro de 2017”.

Plano Diretor de Tecnologia da Informação (PDTI) 2015 -2017 e a PSI

O Plano Diretor de Tecnologia da Informação (PDTI) da SEFIN/RO é um instrumento base de planejamento estratégico da Secretaria de Estado de Finanças. Ele direciona a equipe de TI nas suas rotinas e projetos e também norteia os investimentos e orçamento para infraestrutura de TI da instituição, alinhando-os, continuamente, com os objetivos de negócio. Além disso, é uma ferramenta de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação para atender às necessidades de informação da SEFIN/RO realizadas através da área de TI e auxiliá-la no alcance dos seus objetivos e metas institucionais.

A elaboração da PSI está alinhada ao Planejamento Estratégico da SEFIN/RO, consignado no Plano Diretor de Tecnologia da Informação 2015 - 2017 do órgão, constituindo-se no objetivo estratégico 3 – Promover a Política de Segurança da Informação.

O referido objetivo é composto de três metas estratégicas, quais sejam: a) Sensibilizar a Administração Fazendária sobre a necessidade de criação do Comitê ou Grupo de Segurança da Informação; b) Auxiliar o Comitê ou Grupo de Segurança da Informação na criação de Atos Normativos relacionados à Segurança da Informação; e c) Criar no âmbito da Gerência de Controle e Informações – GEINF a Equipe de Tratamento e Respostas a Incidentes ETRI.

1. Escopo

1.1. A Política de Segurança da Informação (PSI) é uma declaração formal da SEFIN/RO acerca do compromisso com a proteção dos ativos de TI de sua propriedade e/ou sob sua guarda. Seu propósito é direcionar a instituição no que diz respeito à gestão dos riscos e do tratamento dos incidentes de Segurança da Informação (SI), por meio da adoção de procedimentos e mecanismos, que visem à eliminação e/ou à redução de incidentes relacionados à segurança da informação, bem como garantir a disponibilidade de recursos e sistemas críticos para assegurar a continuidade dos negócios da SEFIN/RO, em conformidade com a legislação vigente, normas complementares pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de Segurança da Informação.

2. Objetivo

2.1. A PSI objetiva instituir diretrizes estratégicas, responsabilidades e competências, com o objetivo de assegurar a disponibilidade, integridade, confidencialidade, autenticidade e proteção dos dados, salvaguardando informações e documentos produzidos, armazenados ou transmitidos, por meio dos sistemas de informação da SEFIN/RO, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional.

2.2.Orientar quanto ao uso adequado das informações e dos recursos de Tecnologia da Informação, evitando e/ou minimizando os impactos prejudiciais às atividades finalísticas e à Gestão da Instituição.

2.3. Estabelecer o comprometimento da alta direção organizacional da SEFIN/RO, com vistas a prover apoio para implementação da Gestão de Segurança da Informação, e estabelecer um ambiente seguro, proporcionando melhor qualidade nos processos de gestão e controle dos sistemas de informação e demais ativos de TI.

3. **Abrangência e vigência**
4.

3.1. A Política de Segurança da Informação (PSI) se aplica a todas as unidades administrativas, servidores, funcionários e 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.

3.2. A PSI tem prazo de validade indeterminado, portanto, sua vigência inicia em sua instituição e se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

4. Conceitos e Definições

4.1. Os conceitos e definições constantes deste item se aplicam de forma a auxiliar a interpretação da Política de Segurança da Informação da SEFIN/RO e também no estabelecimento de futuras normas complementares.

4.2. Para os fins desta Política, considera-se:

4.2.1. Comitê Estratégico de Tecnologia da Informação (CETI): comitê criado pelo Decreto 19.173/2015, responsável, dentre outras atribuições, por apreciar e aprovar o Plano Diretor de Tecnologia da Informação (PDTI), a Política de Segurança da Informação (PSI) e demais normas a estas relacionadas; analisar e aprovar os investimentos na área de Tecnologia da Informação e monitorar o estágio dos projetos e o nível dos serviços, recomendando ações para solução dos problemas de recursos e interesse da área;

4.2.2. Grupo de Segurança da Informação (GSI): grupo responsável por elaborar e revisar periodicamente a Política de Segurança da Informação (PSI) e normas relacionadas, submetendo à aprovação do Comitê Estratégico de Tecnologia da Informação - CETI, entre outras competências;

4.2.3. Gerência de Controle e Informações:

4.2.4. Equipe de Tratamento e Resposta a Incidentes - ETRI: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

4.2.5. Segurança da informação - SI: conjunto de políticas, normas e procedimentos que objetivam o controle de acesso, a preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade, integridade dos dados e responsabilidade das informações e dos recursos de TI;

4.2.6. Ameaça: Conjunto de fatores externos e internos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a SEFIN/RO.

4.2.7. Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição.

4.2.8. Ativo de Informação: dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados na SEFIN/RO. Exemplos desses ativos são: base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho entre outros.

4.2.9. Ativo de Tecnologia da Informação: composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações. Entre os ativos de software podemos citar os aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Nos ativos físicos estão incluídos os equipamentos computacionais fixos e móveis, equipamentos utilizados para comunicação de dados e mídias removíveis.

4.2.10. Contas de acesso: Permissões concedidas por autoridade competente da SEFIN/RO, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso.

4.2.11. Incidente de segurança: Qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação da SEFIN/RO.

4.2.12. Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que a SEFIN/RO mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

4.2.13. Plano de Recuperação de Desastres: documentação dos procedimentos e informações necessárias para que a SEFIN/RO operacionalize o retorno das atividades críticas a normalidade.

4.2.14. Quebra de segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da SI da instituição.

4.2.15. Tecnologia da Informação (TI): Conjunto de todas as atividades e soluções providas por recursos de computação. Serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. Este termo é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas.

4.2.16. Usuário(s): Servidores, agentes públicos, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada de acesso aos Ativos de Tecnologia da Informação da SEFIN/RO, formalizada por meio da assinatura de um Termo de Responsabilidade.

4.2.17. Dispositivos móveis: Consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória.

4.2.18. Computação em Nuvem: Modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, processamento, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

4.2.19. Redes Sociais: Estruturas sociais, disponíveis na rede mundial de computadores (Internet), compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

4.2.20. Sistemas de informação: sistemas codificados de propriedade ou em posse da SEFIN/RO, bem como seus conteúdos hospedados ou armazenados em máquinas servidoras ou em máquinas locais com cópias de segurança em máquinas servidoras, de responsabilidade da instituição. São partes integrantes do sistema de informação os componentes clientes instalados nas máquinas locais.

4.2.21. Serviços de rede: todos os serviços oferecidos aos usuários por meio da infraestrutura de rede interna e externa, tais como: correio eletrônico, websites (páginas individuais e institucionais de conteúdos para a Internet), aplicações web ou desktops (sistemas corporativos acessados via rede), repositórios de arquivos em rede, servidores de bancos de dados individuais e corporativos, sistemas de autenticação de usuários de rede, serviços de segurança e monitoração, entre outros; bem como seus conteúdos (mensagens de correio eletrônico, dados corporativos, documentos, arquivos de configuração) que são hospedados e armazenados em máquinas servidoras de responsabilidade da Gerência de Controle e Informações ou no Núcleo de TI da Superintendência de Contabilidade;

5. Estrutura da Política de Segurança da Informação

5.1. A PSI da SEFIN/RO é composta por um conjunto de documentos com 2 (dois) níveis hierárquicos distintos, relacionados a seguir:

5.1.1. Política de Segurança da Informação - PSI: constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação.

5.1.2. Normas de Segurança da Informação (NSI): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da PSI, a serem seguidos em diversas instâncias em que a informação é tratada. A cada Norma será associada a um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas na PSI.

6. Princípios da Política de Segurança da Informação

6.1. As ações relacionadas com a SI na SEFIN/RO são norteadas pelos seguintes princípios, assim definidos:

6.1.1. Autenticidade: Garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos, por pessoa física, por sistema, órgão ou entidade vinculado à SEFIN/RO.

6.1.2. Celeridade: As ações de Segurança da Informação devem oferecer respostas rápidas a incidentes e falhas de segurança.

6.1.3. Confidencialidade: Garantia de que a informação confidencial não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada pela SEFIN/RO.

6.1.4. Conhecimento: Os usuários devem conhecer e respeitar a PSI, NSI e demais regulamentações relativas a Segurança da Informação da SEFIN/RO.

6.1.5. Clareza: As regras de Segurança da Informação, documentação e comunicações devem ser precisas, concisas e de fácil entendimento.

6.1.6. Disponibilidade: Garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física, determinado sistema, órgão ou entidade vinculada à SEFIN/RO.

6.1.7. Ética: Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento da Segurança da Informação.

6.1.8. Integridade: Garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito ou no seu destino.

6.1.9. Legalidade: As ações de segurança devem levar em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais da SEFIN/RO.

6.1.10. Privacidade: Garantia ao direito pessoal e coletivo, à intimidade e ao sigilo da correspondência e das comunicações individuais.

6.1.11.Publicidade: Transparência no trato da informação, observados os critérios legais.

6.1.12. Responsabilidade: As responsabilidades primárias e finais pela segurança dos ativos da SEFIN/RO e pelo cumprimento de processos de segurança devem ser claramente definidas.

6.1.13. Não repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.

7. Diretrizes de Segurança

7.1. Esta PSI define as diretrizes para a Segurança da Informação da SEFIN/RO e descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

7.2. As diretrizes da PSI constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração das Normas Segurança da Informação (NSI).

7.3. Deverão ser mantidos Planos de Gerenciamento de Incidentes e Planos de Recuperação de Desastres formais e periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade.

7.4. Os sistemas, as informações e os serviços da SEFIN/RO utilizados pelos usuários, no exercício de suas atividades, são de exclusiva propriedade da instituição, não podendo ser interpretados como de uso pessoal e devem ser protegidos, segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

7.5. Todos os ativos de informação estão sujeitos à monitoração e auditoria, e os registros assim obtidos poderão ser utilizados para detecção de violações da PSI e demais regulamentações em vigor.

7.6. Os recursos de tecnologia da informação de propriedade da SEFIN/RO são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração. É considerada imprópria a utilização desses recursos para propósitos não profissionais ou não autorizados. Os usuários e visitantes que tomarem conhecimento dessa prática devem levá-la ao conhecimento do superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

7.7. Informações confidenciais da SEFIN/RO não podem ser transportadas em qualquer meio sem as devidas autorizações e proteções.

7.8. Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas.

7.9. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o reconhecimento do envolvido.

7.10. Qualquer tipo de dúvida sobre a PSI, as NSIs e demais regulamentações de Segurança da Informação deve ser imediatamente esclarecido com a Gerência de Controle e Informações.

8. Diretrizes Gerais

8.1. Gestão da Segurança da Informação

8.1.1. Todos os mecanismos de proteção utilizados para a SI devem ser mantidos com o objetivo de garantir a continuidade do negócio (regular exercício das funções institucionais).

8.1.2. As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido.

8.2. Gestão de Ativos

8.2.1. A gestão dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

8.2.2. Os ativos de informação da SEFIN/RO deverão ser inventariados, classificados, documentados atribuídos aos respectivos responsáveis, e seu uso deve estar em conformidade com os princípios e normas operacionais de SI e são destinados ao uso corporativo, sendo vedada a utilização para fins particulares ou em desconformidade com os interesses institucionais.

8.2.3 Os ativos de um setor deverão ser de responsabilidade do gestor ou alguém por ele designado, que ficará encarregado de exigir o uso adequado do ativo, e de notificar o usuário quando ocorrer mal uso. 8.2.4. A designação do responsável deverá constar de termo de responsabilidade assinado pelo gestor, definindo os cuidados e obrigações que o responsável deverá ter com o ativo, e assinado pelo responsável dando ciência de suas atribuições.

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

8.3. Tratamento da Informação

8.3.1. A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços da SEFIN/RO.

8.3.2. Os dados, as informações e os sistemas de informação da SEFIN/RO devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos egarantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

8.3.3. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade, elaborando-se, para tanto, sistema de classificação da informação.

8.4. Da Classificação da Informação

8.4.1. As informações criadas, armazenadas, manuseadas, transportadas ou descartadas na SEFIN/RO deverão ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas e legislação específica em vigor.

8.4.2. Todo usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pela SEFIN/RO e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

8.5. Do Material Impróprio

8.5.1. É expressamente proibido o acesso, uso, guarda e encaminhamento de material não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios e recursos de comunicações disponibilizados pela SEFIN/RO.

8.6. Gestão de Tratamento de Incidentes de Segurança em Redes

8.6.1. A GEINF deverá criar e manter Equipe de Tratamento e Resposta a Incidentes (ETRI), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança na rede de computadores da SEFIN.

8.6.2. Os eventos e incidentes de SI devem ser tratados de acordo com O Plano de Gerenciamento de Incidentes específico, devidamente disponibilizado para todos os servidores.

8.6.3 A ETRI apresentará planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Grupo de Segurança da Informação.

8.6.3. As normas e procedimentos para implantação e gerenciamento de riscos de Informação serão definidos em documento específico elaborado pela ETRI e aprovados pelo Grupo de Segurança da Informação.

8.7. Gestão de Riscos de Segurança da Informação

8.7.1. A Gestão de Riscos de Segurança da Informação é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

8.7.2. Após a implementação e operação da Gestão de Riscos de Segurança da Informação, todas as áreas responsáveis por ativos de informação deverão implementar processos contínuos de Gestão de Riscos.

8.7.3. A Gestão de Riscos de Segurança da Informação deve ser realizada no âmbito da SEFIN/RO, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizada periodicamente, no mínimo01 (uma) vez por ano, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades detectadas. Trata-se de um instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócio e um Plano de Gerenciamento de Incidentes.

8.7.4. O Plano de Continuidade de Negócio deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

8.7.5. O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SI.

8.8. Gestão de Continuidade de Negócios

8.8.1. A Gestão de Continuidade de Negócios é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da SEFIN/RO e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes de SI e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da SEFIN/RO, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, objetivando salvaguardar os interesses da SEFIN/RO e da sociedade.

8.8.2. As áreas da SEFIN/RO deverão manter processo de gestão de continuidade de negócios, visando não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

8.8.3. A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional da SEFIN/RO.

8.8.4. A área de Tecnologia da Informação da SEFIN/RO, responsável pela Gestão de Continuidade de Negócios, deverá criar um Plano de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

8.8.5. As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar a disponibilidade dos ativos de informação e o retorno de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

8.9. Auditoria e Conformidade

8.9.1. A área de Tecnologia da Informação deverá manter registros e procedimentos, como trilhas de auditoria e outros que assegurem a conformidade através do rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e rede interna da SEFIN/RO.

8.9.2. Auditoria

8.9.2.1. A Auditoria de conformidades será precedida de estudo de da cultura de conformidade de outros órgão e empresas privadas, bem como da análise do grau de comprometimento dos profissionais, a fim de que sejam adotadas como matrizes de auditoria procedimentos compatíveis com o grau de segurança necessário.

8.9.2.2. É uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e melhorar as operações da SEFIN/RO. Além disso, assiste à SEFIN/RO na consecução dos seus objetivos por meio de abordagem sistemática e disciplinada, na avaliação da eficácia da gestão de riscos, do controle e dos processos de Governança de TI.

8.9.2.3. A auditoria efetua verificação de forma aleatória e temporal por meio de amostragens para certificar-se do cumprimento das normas e processos instituídos.

8.9.2.4 Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a PSI e Normas de Segurança da Informação (NSI), será permitido à GEINF auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário, ao Grupo de Segurança da Informação e/ou à Administração Superior da SEFIN/RO, dependendo da gravidade. Sendo considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços.

8.9.3. Conformidade

8.9.3.1. A conformidade é o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as diretrizes, a PSI, as NSIs e os procedimentos estabelecidos para o negócio e para as atividades da SEFIN/RO, bem como para evitar, detectar e tratar qualquer desvio ou não conformidade que possa ocorrer, objetivando:

8.9.3.1.1. Evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações contratuais e de quaisquer requisitos de SI;

8.9.3.1.2. Executar atividades de verificações de forma rotineira e permanente, monitorando-as para assegurar,de maneira corporativa, que os departamentos e unidades estejam respeitando as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para a prevenção e controle dos riscos envolvidos em cada atividade;

8.9.3.1.3. Ser independente quanto à auditoria, reportando-se à administração para informá-la de eventos que representem riscos que possam afetar a reputação da SEFIN/RO;

8.9.3.1.4. Englobar o acompanhamento dos pontos falhos identificados pela auditoria até que sejam regularizados, configurando interseção das duas áreas;

8.9.3.1.5. Auxiliar os usuários na resolução de situações não cobertas pela legislação especifica.

8.9.3.2. Metodologias voltadas à boa conduta e de conformidade devem estar integradas, pois se baseiam em valores e responsabilidade morais, bem como no cumprimento e conformidade das leis e políticas internas.

8.10. Controle de Acesso

8.10.1. As regras de controle de acesso a todo sistema corporativo, Intranet, Internet, informações, dados e às instalações físicas da SEFIN/RO deverão ser definidas e regulamentadas, através de Normas de Segurança da Informação (NSI), com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da SEFIN/RO.

8.10.2. Todas as contas de acesso aos ativos de informação e as instalações físicas da SEFIN/RO deverão ser revogadas ou suspensas quando não mais necessárias, conforme normas e legislação específica em vigor.

8.10.3. Todo acesso às informações e aos ambientes lógicos da SEFIN/RO deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação contemplando:

8.10.3.1 Controle de Acesso Lógico: Permite que os sistemas de TI verifiquem a identidade dos usuários que tentam utilizar seus serviços. Deve ainda utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

8.10.3.2 Controle de Acesso Físico: Limitação e controle do acesso físico aos Ativos de Tecnologia da Informação, segundo o grau de criticidade do ativo.

8.10.4. Todos os usuários deverão, por meio de um termo de responsabilidade específico, assumir o compromisso de:

8.10.4.1. Declarar o conhecimento e aceitação dos termos desta PSI e de suas normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância.

8.10.4.2. Declarar estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria.

8.10.4.3. Manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da GEINF.

8.11. Uso de e-mail

8.11.1. O correio eletrônico é um recurso de comunicação corporativa da SEFIN/RO. As regras de acesso e utilização de e-mail devem atender a todas as orientações desta PSI e das Normas Internas (NIs) específicas, além das demais diretrizes do Governo.

8.11.2 Norma de Segurança da Informação disciplinará o uso do correio eletrônico no âmbito da SEFIN/RO.

8.12. Acesso a Internet

8.12.1. Todos os servidores têm o direito de acesso à internet, conforme as permissões de acesso estipuladas na Norma de Segurança da Informação. Esse acesso deverá ser feito exclusivamente para fins diretos e complementares às atividades da instituição, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

8.12.2. Todos os acessos à Internet devem ser registrados e, a critério da SEFIN/RO, pode ser monitorado todo e qualquer dado transmitido ou recebido através de seus ativos de tecnologia da informação. Este acesso pode ser revogado nos casos de ameaça iminente a qualquer ativo, por desrespeito à PSI e/ou por necessidade de serviço.

.

8.13. Uso das Redes Sociais

8.13.1. O uso das Redes Sociais disponíveis na rede mundial de computadores (Internet), com o objetivo de prestar atendimento e serviços púbicos, divulgando ou compartilhando informações da SEFIN/RO, deve ser regido por Norma de Segurança da Informação (NSI) específica, atendendo às determinações desta PSI, e demais orientações governamentais e legislação em vigor.

8.14. Uso de Dispositivos Móveis

8.14.1. As diretrizes gerais de uso de dispositivos móveis para acesso a informações, sistemas e aplicações da SEFIN/RO, devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo a esta Política de Segurança da Informação e regidas por Normas de Segurança de Informação (NSI) específica, a qual contemplará recomendações sobre o uso desses dispositivos.

8.14.2. Fica sob a responsabilidade do Comitê ou Grupo de Segurança da Informação, a restrição ou liberação de acesso a dispositivos moveis solicitados por usuários da SEFIN/RO.

8.14.3. A liberação de acesso a dispositivos moveis se dará por meio de pedido, através de ordem de serviço, mediante autorização do gerente imediato e aprovação do GSI.

8.15. Uso de Computação em Nuvem

8.15.1. 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 de Segurança de Informação (NSI) específicas, atendendo às determinações desta PSI e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

8.16 Desenvolvimento e Aquisição de Sistemas

8.16.1 Os sistemas utilizados na SEFIN/RO devem dispor de 3 (três) ambientes segregados, voltados ao seu desenvolvimento (quando interno), à sua homologação e à sua execução em regime de produção.

8.16.2 O processo de desenvolvimento e aquisição de sistemas deve ser realizado em conformidade com as diretrizes, normas e padrões definidos internamente para este fim, bem como estar de acordo com a PSI.

8.16.3 Todos os produtos gerados durante o ciclo de vida de desenvolvimento de sistemas devem estar hospedados em repositórios sujeitos a mecanismos de controle de acesso, garantindo que somente agentes autorizados tenham acesso a estes produtos. Os códigos-fonte de programas devem ser armazenados utilizando sistemas de controle de fontes institucional.

8.16.4 Os contratos de desenvolvimento de software devem conter cláusula contratual que garanta a entrega do código fonte e da documentação no padrão exigido pela SEFIN/RO, de acordo com os marcos do projeto, garantindo-se a completa documentação ao término ou no momento da interrupção do contrato.

8.16.5 Será dispensada a cláusula contratual que garanta a entrega do código fonte, quanto autorizado pela Grupo de Segurança da Informação (GSI).

8.16.6 Com relação à aceitação do sistema e sua implantação em ambiente de produção é necessário que o mesmo possua um gestor responsável, e que tenha sido avaliado com sucesso em testes de vulnerabilidade e de carga. Além disso, deve existir um conjunto de documentos que descreva o sistema e/ou produto a ser implantado, que permita o seu gerenciamento e suporte.

9. Penalidades

9.1. O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação (PSI) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor, especialmente a Lei Complementar 68/1992, que dispõe sobre o Regime Jurídico dos Servidores Públicos Civis do Estado de Rondônia, das Autarquias e das Fundações Públicas Estaduais, bem como a suspensão ou limitações de uso dos recursos de tecnologia de informação.

9.2. O usuário responderá disciplinarmente, sem prejuízo das eventuais sanções civis e penais cabíveis, pelo dano que vier a ocasionar a SEFIN/RO.

10. Divulgação

10.1. As normas e orientações de segurança deverão ser publicadas no Diário Oficial do Estado de Rondônia e no portal Intranet Superativo.

10.2. A Gerência de Controle e Informações disponibilizará um canal eletrônico para pesquisa das normas relativas à Segurança da Informação no âmbito da SEFIN/RO.

11. Atualização

11.1. A PSI, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

11.2. Os instrumentos normativos gerados a partir desta PSI deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Conselho de Informática - COETIC, ou conforme definido pelo GSI em reuniões de ações de prevenção, em resposta e/ou recuperação, objetivando salvaguardar os interesses da SEFIN/RO e da sociedade.

ANEXO II

TERMO DE USO E RESPONSABILIDADE

Nome Completo: (COLETAR AS INFORMAÇÕES DO ACTIVE DIRECTORY)

CPF: (COLETAR AS INFORMAÇÕES DO ACTIVE DIRECTORY)

Cargo/Função: (COLETAR AS INFORMAÇÕES DO ACTIVE DIRECTORY)

Empresa: SECRETARIA DE FINANÇAS DO ESTADO DE RONDONIA

Doravante nomeado **PARTE COMPROMETIDA**, pelo presente **TERMO DE USO E RESPONSABILIDADE**, relativo ao uso de EQUIPAMENTO DE INFORMÁTICA DA SECRETARIA DE FINANÇAS DO ESTADO DE RONDONIA, compromete-se

CONDIÇÕES DE USO EQUIPAMENTO DE INFORMÁTICA E RECURSOS DE INFORMÁTICA

A PARTE COMPROMETIDA tem como OBRIGAÇÃO:

1. Todos os equipamentos de informática, programas, vias ou condições de acesso à internet, inclusive correio eletrônico, são de propriedade Secretaria de Finanças – SEFIN/RO e são colocados à disposição dos USUÁRIOS apenas e tão-somente como ferramentas de trabalho e para uso no desempenho de suas atividades profissionais, sendo vedado o seu uso nas seguintes condições:

a) durante os períodos de afastamento (licença-maternidade, férias, afastamento previdenciário, etc);

b) para fins de ordem pessoal sem expressa autorização do superior imediato responsável;

c) para a transmissão, o acesso ou a reprodução de material de conteúdo sexualmente ofensivo, agressivo, difamatório, discriminatório ou que seja proibido por lei ou não recomendado pelo costume ou pela moral média, inclusive o acesso a redes de relacionamentos, fóruns, blogs, correios eletrônicos ou qualquer forma similar que promova a discriminação de raça, origem, idade, estado civil, sexo, filiação política ou religiosa, inaptidão ou preferência sexual e pedofilia;

d) para atividades ilegais ou que interfiram no trabalho alheio;

e) para obter acesso não autorizado a qualquer outro computador, rede, banco de dados ou informações armazenadas eletronicamente;

f) para reproduzir, instalar, alterar, copiar, distribuir programas de computador (softwares), conteúdos literários, fonográficos e/ou audiovisuais entre outros, protegidos por direitos autorais, sem a expressa autorização do autor;

g) para o envio de mensagens eletrônicas de conteúdo abusivo, obsceno, difamatório, correntes, propagandas, angariação de fundos ou qualquer material que possa violar a legislação vigente, regulamentos internos ou código de ética e conduta definia na PSI – Politica de Segurança da Informação;

h) para a transferência de arquivos da SEFIN/RO para sites, repositórios e qualquer outra forma de tecnologia de armazenamento de dados físico, lógico ou virtual, de origem desconhecida, sem expressa autorização do superior imediato responsável;

i) cadastrar o e-mail profissional em listas de discussão, redes de relacionamento, fóruns e/ou formas similares de comunicação, bem como a manifestação de opinião em nome da SEFIN/RO, sem expressa autorização do superior imediato responsável;

j) para uso, cópia, instalação ou transmissão de quaisquer programas de computador (softwares) não autorizados previamente pela área de suporte da SEFIN/RO, ainda que tais programas sejam de legítima propriedade do USUÁRIO;

k) desinstalação de programas (softwares), a alteração de configuração de equipamentos ou a desabilitação de quaisquer mecanismos de controle ou verificação que estejam instalados nos recursos que forem colocados à sua disposição para o exercício de suas atividades profissionais, sem prévia autorização da área de suporte;

l) abertura dos equipamentos de informática, bem como a remoção ou alteração de quaisquer partes de tais equipamentos, sem a devida autorização da área de suporte da SEFIN/RO;

m) divulgação de sua senha pessoal de acesso aos equipamentos de informática, programas, vias e condições de acesso à internet, a terceiros e a outros USUÁRIOS;

n) divulgação fora e dentro do âmbito profissional, de fatos ou informações de qualquer natureza, a que os USUÁRIOS tenham acesso em decorrência de suas atribuições, salvo por meio judicial ou com o pedido e expressa autorização do superior imediato responsável;

2. A SEFIN/RO a é proprietária de todas as mensagens e dos conteúdos dos acessos feitos com o uso das ferramentas por ele fornecidas;

3. A SEFIN/RO, através da GEINF (Gerencia de Informatica) tem o pleno direito de monitorar, interceptar, copiar, transmitir ou eliminar as comunicações eletrônicas e os acessos à internet feitos por meio das ferramentas ora mencionados, salvo os acessos relacionados à internet banking e webmail pessoal, sem qualquer aviso prévio e sem que isto implique qualquer forma de violação da privacidade, intimidade ou imagem do USUÁRIOS envolvidos;

4. Os USUÁRIOS devem atender integral e prontamente a todas as orientações e diretivas emanadas pela SEFIN/RO e que tenham relação com o uso de equipamentos de informática, programas, vias ou condições de acesso à internet;

5. Os USUÁRIOS devem empenhar-se no sentido de manter em boas condições todos os equipamentos de informática tanto nas condições físicas (correto uso de periféricos, como teclado, mouse, scanners, impressoras, etc) e programas, vias e condições de acesso à internet que lhes sejam fornecidos para o desempenho de suas atividades profissionais, devendo reportar de imediato qualquer tipo de problema técnico ou ocorrência anormal (através de abertura de chamado técnico – Ordem de Serviço);

6. É de responsabilidade do USUÁRIO manter as informações sigilosas e/ou confidenciais em áreas seguras (de acesso exclusivo do usuário mediante logon e senha), desta forma, evitando acesso indevido por parte de outros usuários não autorizados.

7. Os USUÁRIOS serão trabalhista, civil e penalmente responsáveis pelo uso indevido das ferramentas ora mencionadas, pela não obediência às presentes regras e por quaisquer prejuízos que estes comportamentos possam causar a SEFIN/RO ou a terceiros;

8. A SEFIN/RO - através de políticas definidas na PSI - poderá alterar as presentes regras, no todo ou em parte, sempre que houver tal necessidade, sem prévio aviso.

Declaro que Li todas condições citadas no documento, e aceito as condições de uso.

NOME DO SERVIDOR

MATRÍCULA N.

Documento assinado eletronicamente por **Marcelo Hagge Siqueira**, **Secretário(a) Adjunto(a)**, em 05/12/2018, às 10:14, conforme horário oficial de Brasília, com fundamento no caput III, art. 12 do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.sistemas.ro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3943837** e o código CRC **ACBA8680**.

Portaria nº 948/2018/SEFIN-GRH

Porto Velho, 05 de dezembro de 2018.

O SECRETÁRIO ADJUNTO DE ESTADO DE FINANÇAS, no uso de suas atribuições legais e considerando o Termo de Posse, datado em 01/11/2018.

RESOLVE:

I – **LOTAR** a contar de 1 de dezembro de 2018, o servidor **VILMAR VACARI**, ocupante do cargo Técnico Tributário, matrícula 300138356, na Agência de Rendas de São Miguel do Guaporé - AGSMG/5ªDRRE/Rolim de Moura/RO.

II – Esta portaria entra em vigor na data de sua publicação, retroagindo seus efeitos a partir de 01/11/2018.

MARCELO HAGGE SIQUEIRA
Secretário Adjunto de Estado de Finanças
Matrícula nº. 300023998

Documento assinado eletronicamente por **Marcelo Hagge Siqueira**, **Secretário(a) Adjunto(a)**, em 05/12/2018, às 17:23, conforme horário oficial de Brasília, com fundamento no caput III, art. 12 do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.sistemas.ro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3948026** e o código CRC **DDF96C0F**.
