Diário Oficial do Estado de Rondônia nº 116
Disponibilização: 09/06/2021
Publicação: 09/06/2021

Governo do Estado de
RONDÔNIA

Estado para Resultados - EPR

Portaria nº 97 de 09 de junho de 2021

Institui a Política de Segurança da Informação - PSI aplicável aos dados e informações trafegadas na rede de dados da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC, e dá outras providências.

O **SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, no uso de suas atribuições legais, conferidas pelo art. 114-A, especialmente os incisos I, II, IV e XII, da Lei Complementar nº 965, de 20 de dezembro de 2017, e pelo Decreto de 01.01.2019, publicado no DOE n. 001, de 03.01.2019;

CONSIDERANDO a Política Nacional de Segurança da Informação, instituída pelo artigo 4º do Decreto nº 9.637, de 26 de dezembro de 2018, no âmbito da administração pública federal, com a finalidade de assegurar a segurança da informação a nível nacional, acarretando a necessidade de disciplinar esse tema por meio de normas de observância obrigatória;

CONSIDERANDO as recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, e que atende fielmente às exigências legais vigentes em nosso país, servindo de base para a formulação da presente Política de Segurança da Informação;

CONSIDERANDO que compete à SETIC planejar, estruturar e manter a infraestrutura tecnológica e operacional do Governo do Estado de Rondônia, operando e controlando sua estrutura de data center e interconexão de redes, mantendo a disponibilidade de seus ativos e garantindo a segurança das credenciais de acesso, da comunicação de dados e voz, bem como elaborar, coordenar, apoiar a implantação pelos Órgãos e supervisionar a conformidade das políticas de segurança da informação e comunicação da Administração Pública Estadual;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação - PSI com a finalidade de assegurar a segurança das informações trafegadas na rede de dados da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC, regulando a proteção dos dados, informações e

conhecimentos.

Art. 2º Para os fins do disposto nesta PSI, a segurança da informação abrange:

I - a segurança cibernética;

II - a segurança física e a proteção de dados organizacionais;

III - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 3º A PSI é uma declaração formal acerca do compromisso da SETIC com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os envolvidos, internamente e externamente à Superintendência, sejam eles servidores, colaboradores, estagiários, prestadores de serviços, ou qualquer cidadão que tenha acesso a dados ou informações da rede de dados da SETIC.

Parágrafo único. O propósito da PSI é estabelecer diretrizes para as normas, procedimentos e instruções referentes à segurança da informação, atribuindo responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações.

Art. 4º São princípios da PSI:

I - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

II - visão abrangente e sistêmica da segurança da informação;

III - fortalecimento da cultura de segurança da informação na sociedade;

IV - responsabilidade da SETIC na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação;

V - intercâmbio científico e tecnológico relacionado à segurança da informação entre os órgãos e entidades da Administração Pública Estadual;

VI - educação como alicerce fundamental para o fomento da cultura em segurança da informação;

VII - articulação entre as ações de segurança cibernética, defesa cibernética, proteção de dados e ativos da informação;

VIII - dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das

informações imprescindíveis à segurança da sociedade e do Estado e à inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

IX - cooperação entre os órgãos de investigação, os demais órgãos e as entidades públicas no processo de credenciamento de pessoas para acesso às informações sigilosas;

X - integração e cooperação entre o Poder Público, o Setor Empresarial, a Sociedade e as Instituições Acadêmicas.

Art. 5º São objetivos da PSI:

I - contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;

II - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;

III - aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação;

IV - fomentar a formação e a qualificação dos recursos de pessoas necessários à área de segurança da informação;

V - definir o escopo da segurança da informação na SETIC;

VI - permitir a adoção de soluções de segurança integradas;

VII - servir de referência para auditoria, apuração e avaliação de responsabilidades.

VIII - orientar, por meio de suas diretrizes, todas as ações de segurança, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos tecnológicos;

IX - orientar ações relacionadas a:

a) segurança dos dados custodiados por entidades públicas;

b) segurança da informação das infraestruturas críticas;

c) proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica;

d) tratamento das informações com restrição de acesso.

Art. 6º A utilização dos recursos de Tecnologia da Informação e Comunicação - TIC pertencentes à SETIC destina-se estritamente às suas funções corporativas e será monitorada, tendo seus registros administrados e mantidos pelo setor interno de operações.

CAPÍTULO II
DAS REFERÊNCIAS NORMATIVAS

Art. 7º A presente PSI tem como fundamentos as seguintes referências legais e normativas:

I - Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

II - Lei Federal nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet;

III - Lei Federal nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI);

IV - Decreto Federal nº 9.637 de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

V - Lei Complementar Estadual nº 68, de 09 de dezembro de 1992 - Dispõe sobre o Regime Jurídico dos Servidores Públicos Civil do Estado de Rondônia;

VI - Decreto Estadual nº 9.832 de 12 de junho de 2019 - Dispõe sobre o Comitê Gestor da Segurança da Informação;

VII - NBR/ISO/IEC 27001/2006 - Estabelece os elementos de um Sistema de Gestão de Segurança da Informação;

VIII - NBR/ISO/IEC 27002/2013 - Institui o Código de Melhores Práticas para Gestão de Segurança da Informação;

IX - NBR/ISO/IEC 27005:2008 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação;

X - Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/;

XI - Instruções Normativas do Departamento de Segurança da Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR):

a. NC nº 01/IN01/DSIC/GSI/PR, de 13 de junho de 2008;

b. NC nº 02, de 14 de outubro de 2008;

c. NC nº 03, de 3 de julho de 2009;

d. NC nº 07, de 16 de julho de 2014;

e. NC nº 09, de 16 de julho de 2014;

f. NC nº 10, de 10 de fevereiro de 2012;

g. NC nº 11, de 10 de fevereiro de 2012;

h. NC nº 12, de 10 de fevereiro de 2012;

i. NC nº 13, de 10 de fevereiro de 2012;

j. NC nº 14, de 10 de fevereiro de 2012;

k. NC nº 16, de 21 de novembro de 2012;

l. NC nº 17, de 10 de abril de 2013;

m. NC nº 18, de 10 de abril de 2013;

n. NC nº 19, de 16 de julho de 2014.

Art. 8º Para os efeitos desta PSI, serão utilizados os conceitos e definições do Glossário de Segurança da Informação do Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI/PR, instituído pela Portaria nº 93, de 26 de setembro de 2019, publicada no Diário Oficial da União em 01/10/2019, edição 190, seção 1, página 3, e disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663 .

CAPÍTULO III
DA ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 9º. A SETIC estabelecerá uma estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação em seu âmbito.

Art. 10. Fica criada a Comissão Permanente de Segurança da Informação - CPSI no âmbito da SETIC, responsável pela gestão da segurança da informação, exercendo suas competências nos termos desta Portaria.

Art. 11. A CPSI será composta por 04 (quatro) servidores com formação técnica na área ou notório conhecimento, presidida por um servidor efetivo dentre estes, a serem designados por portaria própria, pelo Superintendente Estadual de Tecnologia da Informação e Comunicação.

Art. 12. É obrigação de todo servidor que tomar conhecimento de incidente que afete a segurança da informação registrar o ocorrido através de chamado no sistema GLPI (Gestionnaire Libre de Parc Informatique) mantido pela SETIC, para análise da CPSI.

CAPÍTULO IV
DOS DISPOSITIVOS MÓVEIS

Art. 13. Entende-se por "dispositivo móvel" qualquer equipamento eletrônico com atribuições de mobilidade, de propriedade da SETIC ou de propriedade particular, a exemplo de notebooks, smartphones, tablets, televisores e sistemas de assistentes virtuais inteligentes.

Art. 14. Os dispositivos móveis corporativos serão regidos pelas seguintes regras:

I - quando fornecidos pela SETIC, serão cadastrados, garantindo a sua identificação única, bem como a do usuário responsável pelo uso;

II - serão utilizados única e exclusivamente por aqueles usuários que assumiram a responsabilidade pelo seu uso;

III - será expressamente vedado aos usuários instalar aplicativos ou recursos não disponibilizados inicialmente no dispositivo sem permissão da CPSI;

IV - serão implementados mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis;

V - os usuários serão orientados a respeito dos procedimentos de segurança acerca dos dispositivos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

Art. 15. Os dispositivos móveis de propriedade de particulares serão regidos pelas seguintes regras:

I - o usuário proprietário de dispositivo móvel particular deverá solicitar ao seu chefe imediato a autorização para acesso aos recursos corporativos, conforme necessário;

II - o chefe imediato definirá a quais recursos ou dados corporativos o dispositivo móvel particular terá acesso;

III - serão individualmente autorizados pela CPSI, mediante solicitação expressa;

IV - serão cadastrados, garantindo a sua identificação única, bem como a do usuário responsável pelo uso;

V - serão utilizados mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis;

VI - os usuários serão orientados a respeito dos procedimentos de segurança para os recursos e acessos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

Art. 16. Os dispositivos móveis de visitantes serão regidos pelas seguintes regras:

I - a concessão de seu uso estará vinculada à conscientização do usuário acerca das normas internas de utilização da rede;

II - obedecerão a procedimentos de controle e concessão de acesso a serem estabelecidos para visitantes que, durante sua permanência nas instalações da SETIC, necessitem conectar seus dispositivos móveis à internet.

Parágrafo único. Considerar-se-á visitante todo e qualquer usuário de rede que não integre o quadro de servidores públicos da SETIC.

Art. 17. O uso indevido do dispositivo móvel caracteriza que o usuário assumiu todos os riscos por sua conduta, tornando-se o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha a causar à SETIC ou a terceiros.

Art. 18. É responsabilidade do usuário, no caso de furto, roubo, extravio ou danos materiais a um dispositivo móvel fornecido pela SETIC, notificar imediatamente seu chefe imediato e a CPSI, devendo simultaneamente procurar a ajuda das autoridades policiais registrando boletim de ocorrência policial, logo que possível, nos casos de furto ou roubo do dispositivo.

CAPÍTULO V

DAS REGRAS PARA UTILIZAÇÃO DO SERVIÇO DE ACESSO REMOTO EXTERNO

Art. 19. As regras para utilização do serviço de acesso remoto externo à rede de dados da SETIC visam à prevenção do acesso não autorizado às informações, evitando ameaças à integridade e sigilo das informações contidas na rede.

Art. 20. O acesso remoto externo à rede de dados da SETIC e a seus serviços corporativos somente será disponibilizado aos usuários que, oficialmente, executem atividade vinculada à atuação governamental e necessitam daquele acesso para execução de atividades externas, desde que devidamente autorizados pelo chefe imediato e certificados pela SETIC.

Art. 21. É vedada a utilização do acesso remoto para fins não relacionados às atividades corporativas.

§ 1º A SETIC irá monitorar e registrar toda conexão remota e de acesso à sua rede de dados.

§ 2º Os administradores de redes poderão ter permissão de acesso remoto aos recursos de TIC da SETIC, quando necessário para o desempenho de suas atribuições.

Art. 22. A solicitação de acesso remoto ocorrerá por meio de chamado registrado no sistema GLPI, contendo as seguintes informações do usuário e do serviço: nome completo; CPF; setor; e-mail e telefone de contato; IP de destino; porta do serviço; tempo de validade do acesso remoto e justificativa.

Art. 23. O serviço de acesso remoto será cancelado nas seguintes condições:

I - finalização do período especificado na solicitação;

II - perda da necessidade de utilização do serviço;

III - transferência ou exoneração do usuário;

IV - identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

Art. 24. As conexões remotas à rede de dados da SETIC cumprirão os seguintes requisitos:

I - utilização de certificado digital;

II - criptografia das senhas e das informações que trafegam entre a estação remota e a rede.

CAPÍTULO VI
DA GESTÃO DE PESSOAS

Art. 25. As responsabilidades pela segurança da informação devem ser mencionadas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da SETIC.

Parágrafo único. Os papéis e responsabilidades pela segurança dos ativos de informação deverão ser definidos conforme o cargo, função, estágio ou vínculo estabelecido com a SETIC.

Art. 26. Todos os usuários deverão ser sensibilizados e treinados acerca dos procedimentos de segurança da informação.

Parágrafo único. A SETIC implementará programa de sensibilização para disseminação das informações relativas à segurança da informação, a fim de assegurar que todos os administradores e/ou usuários de sistemas, redes e operações da SETIC estejam cientes dos potenciais riscos de segurança e exposição a que estão submetidos, dando especial ênfase às equipes que possuem tratativas e relações diretas com os usuários finais, e incluindo treinamentos de proteção contra ataques típicos de engenharia social.

Art. 27. O controle operacional de uma atividade crítica não poderá ser atribuição exclusiva de uma única pessoa.

Art. 28. Os procedimentos de segurança da informação serão documentados e implementados, garantindo que todos os servidores, pessoal contratado ou prestadores de serviços transferidos, remanejados, promovidos ou exonerados, tenham todos os seus privilégios de acesso aos sistemas, informações e recursos devidamente revistos, modificados ou revogados, conforme o caso.

§ 1º Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização será de responsabilidade do chefe imediato e do setor de Gestão de Pessoas respectivo a revisão imediata dos direitos de acesso e uso dos ativos.

§ 2º Quando da efetivação do desligamento de usuário, serão suspensos todos os direitos de acesso e uso dos ativos a ele atribuídos, e os ativos por ele produzidos serão mantidos pela SETIC, garantindo o reconhecimento e o esclarecimento da propriedade.

§ 3º Serão registrados e mantidos no sistema E-Estado relatórios sobre movimentações de entrada e saída de servidores.

CAPÍTULO VII
DA GESTÃO E CLASSIFICAÇÃO DE ATIVOS

Art. 29. Os ativos tecnológicos de propriedade da SETIC ou por esta mantidos, a exemplo de redes, sistemas, softwares, estações de trabalho, serviços de Internet, correio eletrônico, entre outros, serão utilizados exclusivamente para o trabalho e os interesses do Estado e da comunidade, e serão administrados e monitorados individualmente.

Art. 30. Equipamentos, tráfego de rede, hardware, softwares de terceiros e sistemas pertencentes a SETIC poderão ser auditados com o objetivo de manutenção preventiva e segurança.

Art. 31. Para todo ativo tecnológico da SETIC será designado um proprietário, assim entendido o servidor responsável pela guarda, manutenção e uso do ativo.

Parágrafo único. O proprietário poderá delegar para um custodiante as tarefas de rotina diária daquele ativo, mediante acordo formal, caso em que a responsabilidade pelo ativo permanece com o proprietário.

Art. 32. Todos os ativos tecnológicos da SETIC serão identificados e classificados quanto à sua importância e criticidade, contendo as informações que ajudem a assegurar a sua proteção efetiva: nome do ativo, proprietário, custodiante, patrimônio, localização, cópia de segurança, criticidade, dentre outros específicos.

Art. 33. A classificação quanto à criticidade dos ativos obedecerá aos seguintes critérios:

I - Muito Alta (prioridade 0) - quando a interrupção do ativo provoca parada total das atividades;

II - Alta (prioridade 1) - quando a interrupção do ativo provoca perda das atividades de um ou mais setores;

III - Média (prioridade 2) - quando a interrupção do ativo provoca perda das atividades de parte de um setor;

IV - Baixa (prioridade 3) - quando a interrupção do ativo provoca perdas de atividade secundárias.

Art. 34. Os ativos tecnológicos, principalmente os classificados como Muito Alta ou Alta criticidade, serão instalados em áreas protegidas contra acessos físicos indesejados.

Art. 35. A rede de dados da SETIC deverá possuir nobreaks e gerador de energia para alimentar eletricamente os equipamentos e os locais classificados como Muito Alta ou Alta criticidade.

Art. 36. O direito de administrador somente será concedido aos usuários de computador previamente autorizados pela CPSI.

Art. 37. Os arquivos com conteúdo de grande importância, cuja perda represente prejuízo para a SETIC ou para o Estado, serão submetidos a uma rotina de backup periódico, mantendo-se uma cópia de segurança em um servidor de rede e outra cópia na nuvem da SETIC.

Art. 38. Somente será permitido utilizar softwares que tenham sido aprovados pela CPSI, a fim de assegurar a integridade da rede corporativa e não permitir que as licenças de software sejam violadas.

§ 1º A instalação de softwares, inclusive navegadores e outros sistemas relacionados à internet, nos equipamentos computacionais da SETIC será feita apenas pelo setor de Service Desk, e desde que o software esteja autorizado pela CPSI, vedada a instalação pelo usuário.

§ 2º Havendo instalação de softwares e sistemas nos equipamentos computacionais da SETIC, sem autorização e/ou licença devida, o usuário se tornará o responsável exclusivo pela sua utilização, arcando com eventuais penalidades e multas de acordo com a legislação vigente.

§ 3º Somente serão instalados softwares e sistemas com suas licenças de uso em dia e devidamente registrados junto ao fabricante.

Art. 39. Os dados, as informações e os sistemas de informação da rede de dados da SETIC serão protegidos preventivamente contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses ativos e das atividades e serviços da rede de dados da SETIC.

Art. 40. As informações da rede de dados da SETIC serão classificadas por meio de um processo contínuo, determinando os controles e níveis de proteção adequados para as informações de natureza restrita ou sigilosa, de acordo com o valor, sensibilidade e criticidade de cada tipo de informação.

Art. 41. As informações criadas, editadas e/ou armazenadas nos dispositivos da SETIC são propriedade do Governo do Estado de Rondônia, serão controladas e geridas pela SETIC, podendo ser acessadas sempre que necessário com a preservação da sua integridade e confidencialidade, sendo adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades corporativas.

CAPÍTULO VIII
DO CONTROLE DE ACESSO

Art. 42. A conta de acesso é o instrumento para identificação do usuário na rede de dados da SETIC e caracteriza-se por ser de uso individual e intransferível, vedando-se a sua divulgação sob qualquer hipótese.

§ 1º Contas para terceiros e estagiários deverão ser criadas com prazo final de atividade, prorrogável em caso de necessidade, sendo imediatamente bloqueadas após o vencimento assinalado.

§ 2º Contas para terceiros e estagiários deverão ser mantidas em Unidades Organizacionais - OU separadas das contas relativas ao órgão de lotação, mesmo nos casos de possuírem os mesmos privilégios.

Art. 43. A solicitação de criação de conta de acesso de usuário aos serviços de rede de dados da SETIC será feita pelo chefe imediato, via chamado registrado no sistema GLPI.

§ 1º O chamado informará o nome completo do usuário, CPF, e-mail particular, setor no qual desempenha suas atividades, matrícula, justificativa da necessidade da conta de acesso e quais serviços serão necessários, como rede local, internet, correio eletrônico, sistemas e/ou dados.

§ 2º A SETIC efetuará a análise do cadastro e, caso aprovado, informará ao interessado o seu usuário e a senha inicial provisória, bem como encaminhará Termo de Compromisso para assinatura, acompanhado de cópia desta Política de Segurança da Informação, tudo através do e-mail particular informado.

Art. 44. A solicitação de exclusão de uma conta ou acesso a um sistema, será solicitada pelo chefe imediato à CPSI, por meio de memorando no Sistema de Processo Eletrônico Oficial do Estado, assinado, informando o nome completo do usuário, o acesso que deve ser removido e justificativa da exclusão.

Parágrafo único Quando da mudança de setor ou exoneração, o chefe imediato deverá comunicar ao setor de Data Center, via chamado no GLPI, para que o remanejamento ou bloqueio do usuário seja realizado.

Art. 45. A senha de acesso é confidencial, intransferível, individual, e não compartilhável, devendo ser trocada pelo usuário no primeiro acesso e, posteriormente, a cada 42 dias.

§ 1º A senha deverá conter no mínimo 7 (sete) caracteres, não sendo recomendados:

I - o mesmo nome do login de usuário para senha, por exemplo: Usuário: “maria”, Senha: “maria”;

II - o nome do usuário ou combinações deste;

III - nomes de familiares, animais de estimação, datas de aniversário ou número de telefone;

IV - nome de clubes de esportes;

V - informações pessoais ou fáceis de serem obtidas;

VI - repetição de números e/ou letras, por exemplo: “111111”, “aaabbb”;

VII - palavras que existam em dicionários, catálogos ou listas conhecidas, mesmo que escritas de trás para frente.

§ 2º São recomendados para uso em senhas:

I - caracteres alfanuméricos, por exemplo: “Ip253O4”;

II - caracteres mistos com maiúsculas e minúsculas, a exemplo de “IpSTmya”;

III - caracteres especiais, como “#”, “@”, “$”, “%”, “&”, “!”, “*”, “?”, “_”, “/”, “>”: “,”; “{“, “]”, “=”, “+”.

§ 3º Não será permitida a repetição das 4 (quatro) últimas senhas utilizadas.

§ 4º Não deverão ser reveladas senhas pelo telefone, e-mail ou por qualquer outro meio, mesmo que para o chefe, assistentes ou secretárias.

§ 5º Não deverão ser reveladas senhas para colegas de trabalho, nem mesmo quando o servidor estiver em férias ou licença.

Art. 46. A conta será bloqueada depois de 5 (cinco) tentativas inválidas de entrada, podendo o seu desbloqueio ser obtido por meio de chamado no GLPI.

Art. 47. As contas inativas por mais de 90 (noventa) dias corridos serão bloqueadas, podendo o seu desbloqueio ser obtido por meio de chamado no GLPI.

Art. 48. O chefe imediato será o responsável pelas contas de acesso à rede de dados pertencentes ao seu setor.

§ 1º O usuário é o responsável por qualquer acesso aos serviços realizados com sua conta.

§ 2º No caso de evidências de uso irregular dos recursos de acesso a serviços, o usuário terá seu acesso bloqueado para averiguação e, em sendo constatada irregularidade, será realizado o imediato cancelamento do acesso ao serviço e serão aplicadas as penalidades, de acordo com a legislação vigente.

§ 3º O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato, à diretoria correspondente e à CPSI.

CAPÍTULO IX
DO CORREIO ELETRÔNICO

Art. 49. O uso do correio eletrônico, também denominado e-mail, é limitado aos fins corporativos e relacionados às atividades do usuário como um instrumento de comunicação interna e externa, no desempenho de funções profissionais na SETIC.

Art. 50. O correio eletrônico corporativo oficial é unicamente aquele de domínio "@setic.ro.gov.br", com exclusão de qualquer outro, não sendo aceitas como oficiais mensagens enviadas por domínio diverso.

Art. 51. A nomenclatura de endereços eletrônicos deve obedecer à composição utilizada para login do usuário (<primeiro nome><último sobrenome>), seguido de "@setic.ro.gov.br".

Parágrafo único. É proibida a utilização de apelidos na nomenclatura de endereços eletrônicos.

Art. 52. O uso do correio eletrônico é pessoal e intransferível, sendo o titular da conta responsável por toda mensagem enviada pelo seu endereço de e-mail eletrônico.

§ 1º Para os grupos de endereços, ou e-mail de grupo, o criador do grupo será proprietário da conta e responsável por todas as mensagens enviadas.

§ 2º E-mails setoriais, quando necessários, serão de responsabilidade do chefe do setor, exigindo-se a apresentação de documento de nomeação do mesmo para a criação do e-mail.

Art. 53. O acesso às mensagens de correio eletrônico está restrito ao remetente e ao destinatário, sendo o seu conteúdo inviolável, salvo por determinação administrativa ou por motivo de segurança institucional, casos em que o acesso deverá ser expressamente autorizado pela CPSI.

Parágrafo único. A leitura indevida de mensagens de correio eletrônico alheias estará sujeita às sanções administrativas, cíveis e criminais previstas na legislação vigente.

Art. 54. As mensagens de correio eletrônico deverão ser escritas em linguagem profissional e impessoal, observando a norma padrão da língua portuguesa, zelando pela imagem da SETIC e do Governo do Estado, pelo pleno respeito à legislação vigente e pelos princípios éticos da organização.

Art. 55. Os usuários devem sempre verificar se a mensagem recebida é de fonte fidedigna, a fim de impedir a instalação de arquivos maliciosos e, em havendo alguma suspeita quanto à mensagem, seu teor ou origem, o usuário deve informá-la à CPSI.

Art. 56. O e-mail corporativo não deve ser considerado um ambiente seguro pois, considerando que as mensagens de e-mail são transmitidas através da internet, um meio não propriamente seguro, a SETIC não pode garantir que as mensagens sejam lidas somente pelo remetente e o destinatário final, ou que não sejam alteradas durante o percurso, ou ainda que tenham sido criadas pela fonte declarada.

Art. 57. São deveres, responsabilidades do usuário e recomendações para o uso do correio eletrônico:

I - o usuário é o responsável pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;

II - o mau uso de uma conta de correio por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades de acordo com a legislação vigente;

III - não enviar mensagens não autorizadas, divulgando informações sigilosas e/ou de propriedade da SETIC;

IV - não utilizar o e-mail corporativo para assuntos pessoais;

V - adotar o hábito de leitura dos e-mails diariamente;

VI - enviar e-mails apenas para destinatários que realmente precisam da informação;

VII - não acessar, quando não autorizado, a caixa postal de outro usuário e/ou ao Banco de Dados do correio eletrônico;

VIII - não enviar, armazenar nem manusear material que contrarie o disposto nesta PSI, a legislação vigente, a moral, os bons costumes e a ordem pública;

IX - não enviar, armazenar nem manusear material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente PSI, lesivos aos direitos e interesses da SETIC ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos, bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

X - não enviar, armazenar nem manusear material que caracterize:

a. promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas;

b. assuntos de caráter obsceno;

c. prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso;

d. distribuição de qualquer material que caracterize violação de direito autoral garantido por lei;

e. uso para atividades com fins comerciais e/ou o uso extensivo para assuntos pessoais ou privados;

XI - não utilizar o sistema de correio eletrônico para envio de mensagens do tipo “corrente”;

XII - não utilizar as listas e/ou caderno de endereços da SETIC para a distribuição de mensagens que não sejam de estrito interesse funcional e/ou sem a devida permissão do responsável;

XIII - evitar todo e qualquer procedimento de uso do correio eletrônico não previsto nesta PSI, que possa afetar de forma negativa a SETIC ou o Governo do Estado de Rondônia;

XIV - caso receba uma mensagem de correio eletrônico originada na internet de um remetente não confiável ou suspeito, esta deverá ser descartada, antes mesmo de ser aberta;

XV - garantir que cada um dos arquivos anexados possua o seu nível de confidencialidade, de acordo com a classificação da informação, em relação ao destinatário e aos copiados;

XVI - encaminhar arquivos anexados por correio eletrônico somente quando for imprescindível, principalmente, quando houver usuários externos envolvidos na troca de mensagens;

XVII - não enviar mensagens que representem sua opinião pessoal, colocando-a em nome da SETIC.

Art. 58. São deveres, responsabilidades e recomendações dos administradores do correio eletrônico:

I - verificar periodicamente a conta postmaster, para detectar eventuais problemas que possam estar ocorrendo no servidor e na entrega de e-mail dos usuários;

II - criar as contas “security” e “abuse” nos servidores de domínio;

III - configurar o servidor de correio para enviar e-mail só após a autenticação do Usuário, utilizando configurações do tipo “smtp auth”, “smtp after pop”, etc;

IV - implementar medidas para filtragem de vírus no sistema de correio eletrônico;

V - implementar medidas para filtragem de spam e e-mails indesejados (correntes, mensagens obscenas, propaganda, etc.) no sistema de correio eletrônico;

VI - monitorar o funcionamento do servidor de correio eletrônico, em termos de número de conexões, número de mensagens enviadas e recebidas, número de mensagens bloqueadas, banda consumida na rede, etc.

Art. 59. Os anexos serão utilizados quando estritamente necessários para as atividades relacionadas ao trabalho e devem ter tamanhos máximos de 25 MB por mensagem.

Parágrafo único. Não é permitido anexar arquivos classificados como de acesso restrito ou sigiloso.

Art. 60. Ficam limitadas ao tamanho máximo de 5 GB as caixas de e-mail, sendo dever dos usuários excluir e-mails considerados desnecessários para a sua atividade funcional.

CAPÍTULO X
DO ACESSO À INTERNET

Art. 61. O acesso à internet e sua utilização, no âmbito da SETIC, serão estritamente voltados para atividades inerentes aos trabalhos desenvolvidos.

Art. 62. Todas as contas com acesso à internet terão uma titularidade e serão vinculadas às contas de acesso à rede de dados da SETIC, determinando a responsabilidade sobre a sua utilização.

Art. 63. Todo acesso à internet através da rede de dados da SETIC será monitorado e registrado pelo setor de operações, por meio de ferramentas próprias para tal.

§ 1º Todos os registros de acesso à internet são passíveis de auditoria.

§ 2º É expressamente proibido o acesso à internet para violar leis e regras brasileiras ou de qualquer outro país, ou para outras práticas não aceitáveis.

Art. 64. O usuário deve desconectar-se imediatamente de um site que contenha conteúdo indevido e/ou acesso restrito, mesmo que tenha passado pelo controle de fluxo da rede.

Art. 65. São consideradas práticas inaceitáveis de acesso à internet, não se restringindo a estas:

I - elaborar, utilizar, propagar, acessar ou de qualquer maneira manusear material de propaganda política, racismo, terrorismo, hacker, assédio sexual, pornografia, pedofilia, incentivo a violência, discriminação e outros não condizentes com os objetivos de trabalho corporativo, as leis vigentes e a ética;

II - acessar ou fazer uso de sites de conversação (bate-papo) e redes sociais;

III - acessar ou fazer uso de sites de proxy online;

IV - acessar ou fazer uso de quaisquer tipos de jogos, inclusive online;

V - acessar ou fazer uso de programas que implementem P2P, onde o computador do usuário atua como servidor;

VI - acessar ou fazer uso de web rádio e web TV (sessões de transmissão contínua de vídeo e áudio);

VII - baixar arquivos (downloads) ou executar arquivos do tipo “.exe”, “.dat”, “.sys”, “.bat” e outros tipos de arquivos executáveis;

VIII - distribuir software ou conteúdo não autorizado (“pirataria”);

IX - disseminar vírus, worms, cavalos de tróia ou qualquer outro tipo de código malicioso.

CAPÍTULO XI

DAS ESTAÇÕES DE TRABALHO E DA REDE INTERNA

Art. 66. Entende-se por estação de trabalho qualquer computador de mesa, notebook, tablet ou afins, que seja utilizado por um usuário para desenvolver as atividades laborais da SETIC e que a esta pertença.

Art. 67. Cabe ao usuário o zelo pelo equipamento, mantendo o seu exterior limpo e evitando a ingestão de bebidas (água, sucos, refrigerantes, café, etc) e alimentos próximo a ele.

Art. 68. O acesso para uso da estação de trabalho será feito através de login e senha da conta de acesso à rede de dados da SETIC, devendo o usuário bloquear a estação de trabalho caso se afaste da mesma.

Art. 69. Os servidores de arquivos e estações de trabalho serão protegidos com:

I - proteção de tela com ativação automática e bloqueio da estação ou através de desconexão quando o usuário necessitar afastar-se do computador;

II - software de detecção e reparo contra software ou código malicioso, com atualização frequente.

III - programação para bloqueio em caso de inatividade após 5 minutos, efetuar logoff após 30 minutos e desligamento após 18 horas.

Parágrafo único. A CPSI estabelecerá e revisará periodicamente as configurações padrão das estações de trabalho e dos servidores de arquivos.

Art. 70. Todas as atualizações e correções de segurança de hardware, software, sistema operacional ou aplicativos somente poderão ser feitas após a devida validação em ambiente de teste pelo setor de Service Desk, depois de sua disponibilização pelo fabricante e/ou fornecedor.

Art. 71. A SETIC não se responsabiliza por estações de trabalho que não lhe pertençam, mesmo as utilizadas em atividades administrativas, e os seus técnicos não prestarão atendimento a dispositivos particulares.

Art. 72. Todas as estações de trabalho da SETIC devem estar adicionadas na ferramenta de gerenciamento de usuários de rede (AD - Active Directory).

§ 1º As estações de trabalho só poderão ser adicionadas/incluídas à rede de dados da SETIC após tombadas e cadastradas no sistema de gestão patrimonial.

§ 2º A nomenclatura das estações de trabalho seguirá o padrão: “XXX-00000000000”, onde XXX é a sigla da secretaria, conforme Anexo I, e os 11 (onze) dígitos numéricos serão relativos ao número do tombamento da estação.

Art. 73. O acesso aos recursos de impressão estará restrito aos usuários devidamente autorizados pelo chefe imediato.

Art. 74. A instalação e configuração de impressoras na rede de dados da SETIC será responsabilidade do setor de Service Desk.

§ 1º A aquisição e troca de toner ou cartucho e papel para impressão será responsabilidade do setor onde está instalada a impressora.

§ 2º No caso de impressoras locadas e/ou terceirizadas, a configuração e a manutenção ficarão a cargo da empresa responsável pelo contrato, devendo a respectiva instalação ser acompanhada por um técnico do setor de Service Desk.

Art. 74. Todas as informações relacionadas às atividades da administração da SETIC, serão armazenadas em servidores de rede, de acordo com os respectivos sistemas utilizados, e implementados pelo setor de Data Center.

Art. 75. Documentos imprescindíveis para as atividades corporativas dos usuários deverão ser armazenados nos servidores da rede, não sendo considerados para fins de backup os arquivos armazenados em estações de trabalho.

§ 1º Em caso de divergência de versões, os documentos salvos nos servidores de rede serão considerados vigentes, enquanto os salvos nas estações de trabalho serão desconsiderados.

§ 2º Fotos, músicas, vídeos e arquivos muito grandes (acima de 1GB) não deverão ser copiados ou movidos para os servidores de rede e/ou nuvem, podendo, caso identificados, ser excluídos definitivamente sem prévia comunicação ao usuário, salvo exceções definidas pela CPSI.

§ 3º Será autorizado o armazenamento, nos servidores de rede, somente de arquivos com as extensões “.doc”, “.docx”, “.xls”, “.xlsx”, “.ppt”, “.pptx”, “.pdf”, “.txt”, “.odt”, “.ods”, “.odp”, “.bmp”, “.jpg”, “.jpeg”, “.csv”, “.png”, “.rtf”, “.sh”, “.conf” e “.log”, com exceção feita aos setores organizacionais que, para fins de serviço, necessitam armazenar arquivos em formatos diferentes dos citados, caso em que providenciarão a autorização da CPSI.

§ 4º O nome do arquivo salvo nos servidores da rede deve possuir um tamanho máximo de 200 caracteres, contando com o caminho (pastas) para acessar o mesmo, usando a estrutura organizada pelos administradores dos servidores da rede de dados da SETIC.

Art. 76. Todas as informações acessadas pelos sistemas nos bancos de dados da SETIC serão registradas através de log de acesso, consignando data, hora, usuário e as alterações realizadas pelo usuário.

Art. 77. Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados, sendo considerado violação a esta PSI qualquer acesso ou tentativa de acesso a ambientes não autorizados.

Art. 78. É vedado o acesso direto aos bancos de dados para alteração de qualquer informação, exceto por técnicos devidamente identificados, autorizados e acompanhados pela CPSI, caso

em que será feito registro das alterações realizadas.

Art. 79. É absolutamente vedada a exclusão de dados armazenados nos bancos de dados ou aplicações, sob pena das sanções previstas na legislação vigente.

Art. 80. Quando constatada a necessidade de acesso a uma base de dados por terceiros, o interessado deverá solicitar autorização à CPSI.

Parágrafo único. O acesso do terceiro autorizado será bloqueado tão logo tenha terminado o trabalho devido, devendo ser solicitada nova autorização à CPSI caso haja, futuramente, uma nova necessidade de acesso.

Art. 90. A administração dos Bancos de Dados é exclusiva do setor responsável pelo Desenvolvimento de Software da SETIC, cabendo-lhe a manutenção, alteração e atualização de hardware e software.

CAPÍTULO XII
DA CRIPTOGRAFIA

Art. 91. Serão utilizados métodos de criptografia para proteger as informações classificadas como restritas ou sigilosas, armazenadas e transportadas nos diversos meios e formas.

§ 1º O processo de criptografia pode ser usado para cifrar ou decifrar informações, e serve para proteger a integridade, a confidencialidade e a autenticidade da informação, além de reduzir os riscos na sua utilização.

§ 2º A avaliação de risco é proveniente do algoritmo de criptografia utilizado, devendo o nível de proteção ser identificado para tanto, utilizando proteção nas chaves criptográficas e na recuperação de informações cifradas, e elencando os procedimentos quando houver perda, dano ou comprometimento dessas chaves.

Art. 92. O canal de comunicação seguro (Rede Privada Virtual - VPN) para interligar redes dos órgãos e entidades do Governo do Estado de Rondônia, de forma direta e indireta, objetivando a troca de informações classificadas, utilizará os requisitos mínimos de criptografia de dados AES-256 no modo CBC, com autenticação de dados SHA1 e “handshake” RSA-2048.

Art. 93. A transmissão de informações classificadas como restritas ou sigilosas por meio de sistemas de informação, deverá ser realizada no âmbito da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra da segurança.

Parágrafo único Os sistemas de informação terão níveis diversos de controle de acesso e utilizarão recursos criptográficos adequados para cada grau de sigilo ou restrição.

Art. 94. Os equipamentos e sistemas utilizados para a produção e/ou edição de documentos,

com informações classificadas como restritas ou sigilosas, deverão estar protegidos ou ligados a canais de comunicação seguros, estes, física ou logicamente isolados de qualquer outro.

CAPÍTULO XIII
DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 95. Os controles de acesso físico visam restringir o acesso aos ambientes, equipamentos, documentos e suprimentos, permitindo apenas pessoas devidamente autorizadas e registradas.

§ 1º Serão adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas do pessoal previamente autorizado.

§ 2º Todos os serviços envolvidos em trabalhos de apoio, como a manutenção e limpeza das instalações físicas, devem ser feitos por uma equipe já capacitada, que será orientada a manter as medidas de proteção ao acesso físico dos ambientes.

§ 3º O ingresso de visitantes deve ser controlado de forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo quando acompanhados e com autorização de um responsável.

§ 4º Deverá ser seguido o Regulamento Geral do Palácio Rio Madeira para solicitação de qualquer tipo de manutenção predial.

Art. 96. É proibido qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação dos ativos de rede da rede de dados sem o conhecimento prévio da SETIC, exigindo-se comunicação por escrito e o acompanhamento de um técnico da SETIC.

Parágrafo único A entrada ou retirada de quaisquer dispositivo tecnológico nas estruturas físicas do Governo do Estado de Rondônia exigirá uma requisição preenchida e autorizada de acordo com o Regulamento Geral do Palácio Rio Madeira.

Art. 97. O Regulamento Geral do Palácio Rio Madeira adotará mecanismos de controle de acesso físico, dentro ou fora do expediente, indicando a pessoa que terá acesso, o local, data, hora e quem o autorizou.

Art. 98. O acesso aos Data Centers somente será feito por sistemas de autenticação por biometria e cartão magnético registrados em software próprio mantido pela Casa Militar.

Parágrafo único. O acesso aos Data Centers por meio de chave ocorrerá apenas em situações de emergência, quando a segurança física for comprometida, por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Art. 99. O cabeamento elétrico e lógico que alimenta e interliga os Data Centers deverão ser

protegido em toda sua passagem e leito, desde a via pública até o interior dos ambientes de trabalho.

Art. 100. Os Data Centers deverão possuir mecanismos de proteção e combate a incêndio, controle das condições climáticas do ambiente e imagens de circuito interno, que serão monitorados e mantidos pelo setor de Data Center da SETIC.

Art. 101. Os Data Centers deverão ser mantidos permanentemente limpos e organizados.

§ 1º Qualquer procedimento que gere lixo ou sujeira nesse ambiente deverá ser realizado com a colaboração do pessoal da limpeza.

§ 2º Não é permitida a entrada de qualquer tipo de alimento, bebida, produto fumígeno ou inflamável nos Data Centers.

Art. 102. A SETIC adotará uma política de mesas "limpas", inclusive em relação a papéis e mídias de armazenamento removível e, igualmente, uma política de "telas limpas" nos dispositivos eletrônicos, para arquivos e/ou atalhos na área de trabalho, conforme descrito no Anexo II, visando reduzir riscos de acessos não autorizados, perda ou danos às informações durante e após o horário de expediente.

Parágrafo único. É vedado permitir que informações classificadas como restritas ou sigilosas fiquem "à vista", estejam elas em papel ou em quaisquer dispositivo eletrônico, a fim de se evitar a exposição indevida de informações ou mesmo o seu comprometimento.

CAPÍTULO XIV
DA SEGURANÇA NAS OPERAÇÕES

Art. 103. As operações de funcionamento dos ativos de rede da rede de dados da SETIC serão sempre documentadas, com detalhes de sua configuração e executadas de acordo com os procedimentos estabelecidos nessa documentação, utilizando instalações e equipamentos adequados e em condições seguras.

Art. 104. O gerenciamento das mudanças tem como objetivo prever e minimizar os riscos decorrentes do processo de mudança, fazendo com que os mesmos permaneçam dentro dos limites de aceitabilidade definidos no processo.

§ 1º Os processos de gestão de mudanças conterão, no mínimo, as fases de descrição, avaliação, aprovação, implementação e verificação, de forma a viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

§ 2º Mudanças, temporárias ou permanentes, físicas ou lógicas, serão avaliadas visando à eliminação e/ou minimização de riscos decorrentes de sua implantação.

§ 3º É função do gestor de mudanças assegurar-se de que o processo de mudanças contempla os seguintes procedimentos:

I - identificação e registro de todas as etapas das mudanças;

II - correta alocação dos recursos disponíveis;

III - planejamento e testes das mudanças;

IV - comunicação dos detalhes das mudanças para todas as pessoas envolvidas;

V - procedimentos de recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

Art. 105. O monitoramento dos recursos e serviços de TIC da rede de dados da SETIC, é de extrema importância para prover informações sobre como as atividades de negócio do dia a dia consomem os recursos e serviços e se os ativos de rede estão aguentando o fluxo das informações.

Parágrafo único. O gerenciamento de capacidade considera se a capacidade dos serviços e infraestrutura de TIC são capazes de atender em desempenho, acessibilidade e com baixo custo a rede de dados da SETIC, mantendo disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 106. A SETIC utilizará uma solução que permita que diversos dispositivos de armazenamento sejam monitorados simultaneamente, registrando em log todas as ações efetuadas e, em caso de detecção de código malicioso, interrompa a ação do usuário e dispare e-mail ao administrador da rede e à CPSI, assim assegurando que as informações e os recursos de processamento da informação estejam protegidos contra códigos maliciosos.

Art. 107. Será regulamentada, por normativo próprio, uma Política de Backup, realizada por um processo contínuo, definido de maneira formal, aplicado na implementação e operação de proteger as informações da rede contra a perda e/ou roubo de dados por meio de cópias de segurança das informações.

CAPÍTULO XV
DA SEGURANÇA NAS COMUNICAÇÕES

Art. 108. A rede de dados da SETIC utilizará serviços de controle de fluxo de dados, visando filtrar e ordenar todas as informações transitadas e garantir sua proteção.

§ 1º O setor de operações manterá e administrará firewalls em todos os segmentos da rede, gerenciando todo o tráfego de entrada e saída.

§ 2º Um firewall é uma passagem (“gateway”) que restringe e controla o fluxo do tráfego de dados entre redes, mais comumente entre uma rede interna e a internet e pode também estabelecer passagens seguras entre redes internas.

§ 3º Para manter o controle na entrada e saída de informações da rede, qualquer autorização ou bloqueio nos controles de fluxo de dados deverá ocorrer por meio de chamado no GLPI.

§ 4º Cada setor possui autonomia sobre o conteúdo acessado por seus usuários, mantendo controle de quais sites aqueles podem acessar e quais não podem, quem está autorizado a acessá-los e quem não está, além de estabelecer bloqueios comuns a todos.

Art. 109. Todo ativo de rede na rede de dados da SETIC, exceto as estações de trabalho, é monitorado, tanto nas interfaces onde transitam as informações quanto em seus componentes de hardware.

Parágrafo único. O monitoramento será feito via “agentes” instalados e/ou protocolos, juntamente com outras configurações, para que os dispositivos possam alimentar uma base de dados em um servidor de monitoramento, a qual será acessível via navegador, para que os administradores da rede possam acessá-la a partir de qualquer local e em qualquer horário.

Art. 110. Todo segmento de rede é uma VLAN com uma faixa de endereços específicos na rede de dados da SETIC, e cada VLAN necessita de serviços de controle de fluxo próprio.

Parágrafo único. As VLANs possibilitam a segmentação da rede não baseada em cabeamento físico, de modo que usuários em ambientes físicos distintos, mas que fazem parte do mesmo grupo de trabalho (e se comunicam frequentemente entre si), além de acessarem os mesmos servidores, podem participar da mesma VLAN e, portanto, do mesmo domínio de difusão, podendo haver entre eles comunicação direta.

CAPÍTULO XVI
DO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Art. 111. Todo desenvolvimento ou manutenção de sistemas deve ser precedido por uma análise de impacto e ser formalmente autorizado pelo chefe imediato do setor de desenvolvimento.

Art. 112. Toda alteração de escopo de desenvolvimento ou manutenção de software será documentada e formalmente autorizada pelo chefe imediato.

Art. 113. Todo projeto de sistema conterá um documento de especificação que descreva seus requisitos de segurança, os quais devem, entre outros, contemplar:

I - mecanismo de autenticação do usuário, que deve utilizar senhas com métrica mínima e exigir do usuário a troca periódica da senha, bem como bloquear o acesso após número definido de tentativas de login com falha;

II - mecanismo de autenticação do usuário bloqueado, que deve conter a verificação da senha por meio de mecanismo que impeça fraudes de repetição, interceptação ou quebra de integridade na comunicação entre o cliente e servidor;

III - armazenamento da senha pelo sistema, de forma criptografada e irreversível;

IV - uniformidade do controle de acesso em todo o sistema, utilizando-se uma única rotina de verificação;

V - registro, pelo sistema, dos eventos significativos para a segurança, principalmente, início e fim de sessão e alterações realizadas;

VI - registro, pelo sistema, das falhas de login, indicando origem e o número de tentativas;

VII - registro, pelo sistema, da criação e bloqueio de usuários, bem como da atribuição e da remoção de direitos (permissões) do usuário;

VIII - proteção da trilha de auditoria contra remoção e alteração por parte de todos os usuários, exceto dos administradores de auditoria;

IX - capacidade de tolerância do sistema à falhas e retorno a operação;

X - inexistência, em aplicações web, de dados sensíveis em campos ocultos ou cookies;

XI - realização das verificações e validações de segurança no servidor, em aplicações web;

XII - acesso aos desenvolvedores apenas aos códigos fontes necessários para a alteração, e desde que autorizados pelo chefe imediato;

XIII - maior semelhança possível do ambiente de homologação frente ao ambiente de produção;

XIV - exigência de que os aplicativos só passem do desenvolvimento para a homologação após verificação da existência e adequação de sua documentação;

XV - existência de documentação de operação do sistema, ressaltando os aspectos de segurança.

Art. 114. Os requisitos ou funcionalidades de domínio devem ser especificados e documentados juntamente com um representante do sistema, bem como as manutenções necessárias, considerando os requisitos de segurança definidos no desenvolvimento do sistema.

Art. 115. A SETIC fornecerá mecanismos de controle de versão (GIT), cujos códigos fontes de sistemas desenvolvidos ou em desenvolvimento deverão ser mantidos e disponibilizados exclusivamente em repositório de código mantido pela SETIC, a fim de assegurar a propriedade intelectual, a segurança, a qualidade, a continuidade e consistência dos softwares desenvolvidos no Poder Executivo do Estado.

§ 1º O acesso aos códigos fontes deve ser controlado e restrito aos desenvolvedores envolvidos, em seus respectivos projetos.

§ 2º Os códigos fontes não devem conter identificação e/ou senhas de acesso às bases de dados, sejam elas de teste, de homologação ou de produção.

§ 3º Para outros acessos aos códigos fonte por outros órgãos ou terceiros, será necessária a autorização expressa e por escrito da CPSI e do Superintendente.

Art. 116. Serão documentados todos os incidentes de segurança e vulnerabilidades identificadas durante o processo de desenvolvimento e manutenção do sistema.

Art. 117. Todo sistema que implique manipulação de dados deve ser desenvolvido de acordo com as regras de controle de acesso a informações de natureza restrita ou sigilosa.

Parágrafo único. Em caso de manipulação de dados sensíveis, mecanismos adicionais que possibilitem a rastreabilidade das operações efetuadas devem ser considerados.

Art. 118. Os ambientes de desenvolvimento de testes, de homologação e de produção serão isolados entre si.

Parágrafo único. A passagem de sistemas e dados para o ambiente de produção será controlada de maneira a garantir a integridade e disponibilidade desse ambiente para sua execução.

Art. 119. Devem ser definidos e utilizados procedimentos de testes no sistema para todo desenvolvimento ou manutenção realizados, os quais devem contemplar, dentre outros, controles tais como:

I - validação de dados de entrada;

II - controle de processamento interno;

III - integridade de mensagens;

IV - validação de dados de saída;

V - testes automatizados;

VI - testes de carga;

VII - testes de estresse.

§ 1º Os testes devem validar os mecanismos de segurança especificados no desenvolvimento ou na manutenção do sistema.

§ 2º Os testes de aceitação do sistema serão realizados por uma equipe diferente da equipe desenvolvedora, composta por usuários da área de desenvolvimento e da área do negócio solicitante.

§ 3º Em sendo utilizadas para testes, as informações contidas na base de dados do ambiente de produção devem sofrer alterações de modo a preservar sua confidencialidade.

Art. 120. A implantação de um novo sistema será realizada de acordo com o calendário definido pelo cliente do software, com a participação do setor de desenvolvimento.

Art. 121. O setor de desenvolvimento irá assegurar que os sistemas de processamento em operação e em implantação possuam documentação suficiente para garantir sua manutenção e utilização.

Art. 122. Será estabelecida uma metodologia para todo desenvolvimento ou manutenção, com base nas melhores práticas de mercado, contemplando, entre outros: planejamento; análise de requisitos; projeto; codificação; revisão; compilação e testes.

Art. 123. O setor de desenvolvimento assegurará que todo sistema desenvolvido na SETIC seja submetido a uma ferramenta de inspeção contínua da qualidade do código, que possa verificar as boas práticas de desenvolvimento de software e identificar e eliminar falhas, débitos técnicos e vulnerabilidades de segurança.

§ 1° A ferramenta de inspeção contínua da qualidade de código estará ajustada, no mínimo, aos seguintes critérios:

I - 0% (zero por cento) no quesito vulnerabilidade de segurança;

II - 0 (zero) no quesito bug em software; e

III - 60% (sessenta por cento) de cobertura de testes automatizados.

§ 2° Será desenvolvido um painel gerencial para fornecer métricas, diariamente atualizadas, acerca da qualidade de código de todos os sistemas desenvolvidos, permitindo acesso externo.

Art. 124. Toda aplicação desenvolvida deve ter garantido seu isolamento de outras aplicações, evitando que uma aplicação possa interferir no funcionamento de outra aplicação armazenada no mesmo ambiente.

Art. 125. Em sua fase de desenvolvimento, um sistema web deve prever e adotar medidas de proteção para minimizar ou extinguir formas de ataque, listadas e atualizadas anualmente pela OWASP (https://owasp.org/), o que inclui injection, autenticação quebrada, exposição de dados sensíveis, controle de acesso quebrado, configuração incorreta de segurança, XXE, XSS, *insecure deserialization*.

CAPÍTULO XVII
DA CONFORMIDADE

Art. 126. Será fielmente seguido o Plano de Gestão de Incidentes de Segurança da Informação da rede de dados da SETIC, regulamentado por normativo próprio e executado por um processo contínuo, definido de maneira formal, visando assegurar que fragilidades e eventos de segurança da informação sejam comunicados, registrados, monitorados e avaliados.

Art. 127. Será definido um Plano de Continuidade e Recuperação de Serviços da rede de dados da SETIC, regulamentado por normativo próprio e executado por um processo contínuo, definido de maneira formal, visando assegurar a não interrupção dos serviços críticos da rede de dados, contra falhas ou desastres significativos, bem como a sua retomada em tempo hábil se necessário, através da combinação de ações de prevenção e recuperação.

Art. 128. O usuário que fizer uso de forma ilegal dos recursos da rede de dados da SETIC, bem como agir em desacordo com os termos desta PSI, fica sujeito à aplicação das penalidades previstas em lei, podendo implicar processos cíveis, criminais e/ou administrativos.

§ 1º O desrespeito a esta PSI será considerado como um incidente de segurança e, dependendo das circunstâncias, poderá ser motivo para encerramento de contrato de trabalho, de prestação de serviços, assessoria e/ou qualquer tipo de vínculo com o Governo do Estado de Rondônia.

§ 2º Na ocorrência de transgressão, será notificado o usuário infrator, com comunicação ao seu chefe imediato, à Coordenadoria correspondente, à CPSI e ao Superintendente.

§ 3º Uma vez que o usuário é responsável por qualquer atividade a partir de sua conta, o mesmo responderá por qualquer ação judicial proposta a respeito em desfavor do Estado.

CAPÍTULO XVIII
DISPOSIÇÕES FINAIS

Art. 129. A CPSI decidirá acerca dos casos omissos e das dúvidas surgidas na aplicação desta Política.

Art. 130. A PSI será revisada e atualizada periodicamente, no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Parágrafo único. Considera-se a presente portaria como a versão 1.0 da PSI.

Art. 131. A PSI será divulgada para todos os que de alguma forma interagem com a rede de dados da SETIC, garantindo que a conheçam e a pratiquem no desenvolver de suas atividades.

Art. 132. Esta portaria entra em vigor na data de sua publicação.

Publique-se, dê-se ciência e cumpra-se.

DELNER FREIRE - CEL PM RR

Superintendente - SETIC

ANEXO I

SIGLA DOS ÓRGÃOS E ENTIDADES DO GOVERNO DO ESTADO DE RONDÔNIA NA FERRAMENTA DE GERENCIAMENTO DE USUÁRIOS DE REDE (AD - ACTIVE DIRECTORY)

AGR - AGERO - Agência de Regulação de Serviços Públicos Delegados do Estado de Rondônia

AGV - AGEVISA - Agência Estadual de Vigilância em Saúde de Rondônia

CAE - CAERD - Companhia de Águas e Esgotos do Estado

CBM - Corpo de Bombeiros Militar do Estado de Rondônia

CCI - Casa Civil

CGE - Controladoria Geral do Estado

CMI - Casa Militar

CMN - CERIMONIAL - Departamento de Relações Públicas e Cerimonial

CMR - Companhia de Mineração de Rondônia

DER - Departamento de Estrada de Rodagens, Infraestrutura e Serviços Públicos

DPE - Defensoria Pública do Estado de Rondônia

DTR - DETRAN - Departamento Estadual de Trânsito

EMB - EMBRAPA - Empresa Brasileira de Pesquisa Agropecuária

EMT - EMATER - Empresa Estadual de Assistência Técnica e Extensão Rural do Estado de Rondônia

FAP - FAPERO - Fundação de Amparo ao Desenvolvimento das Ações Científicas e Tecnológicas e à Pesquisa do Estado de Rondônia

FEA - FEASE - Fundação Estadual de Atendimento Socioeducativo

FUN - FUNCER - Fundação Cultural do Estado de Rondônia

GOV - Governadoria

IDA - IDARON - Agência de Defesa Sanitária Agrosilvopastoril

IDP - IDEP - Instituto Estadual de Desenvolvimento da Educação Profissional de Rondônia

IPM - IPEM - Instituto de Pesos e Medidas do Estado de Rondônia

IPR - IPERON - Instituto de Previdência dos Servidores Públicos

JUC - JUCER - Junta Comercial do Estado de Rondônia

OGE - Ouvidoria Geral do Estado de Rondônia

OPE - Núcleo de Operações

PCI - Polícia Civil do Estado de Rondônia

PGE - Procuradoria Geral do Estado de Rondônia

PMR - Polícia Militar do Estado de Rondônia

PRC - PROCON - Programa de Orientação, Proteção e Defesa do Consumidor

RNG - RONGAS - Companhia Rondoniense de Gás

SAS - SEAS - Secretaria de Estado de Assistência e do Desenvolvimento Social

SBR - SIBRA - Superintendência de Integração do Estado de Rondônia em Brasília

SCO - SECOM - Secretaria Estadual de Comunicação

SDE - SESDEC - Secretaria de Estado da Segurança, Defesa e Cidadania

SDI - SEDI - Superintendência Estadual de Desenvolvimento Econômico e Infraestrutura

SDM - SEDAM - Secretaria de Estado do Desenvolvimento Ambiental

SDU - SEDUC - Secretaria de Estado da Educação

SDR - SUDER - Superintendência de Desenvolvimento do Estado de Rondônia

SFN - SEFIN - Secretaria de Estado de Finanças

SGI - SEAGRI - Secretaria de Estado da Agricultura

SGP - SEGEP - Superintendência Estadual de Gestão de Pessoas

SGS - SUGESP - Superintendência de Gestão de Gastos Públicos Administrativos

SJC - SEJUCEL - Superintendência Estadual da Juventude, Cultura, Esporte e Lazer

SJS - SEJUS - Secretaria de Estado da Justiça

SOP - SOPH - Sociedade de Portos e Hidrovias do Estado de Rondônia

SPA - SEPOAD - Superintendência de Estado de Políticas Sobre Drogas

SPG - SEPOG - Secretaria de Estado de Planejamento, Orçamento e Gestão

SPL - SUPEL - Superintendência Estadual de Compras e Licitações do Estado de Rondônia

SPR - SUPER - Superintendência Estadual de Contabilidade

SPT - SEPAT - Superintendência Estadual de Patrimônio e Regularização Fundiária

SSU - SESAU - Secretaria de Estado da Saúde

STC - SETIC - Superintendência Estadual de Tecnologia da Informação e Comunicação

STR - SETUR - Superintendência Estadual de Turismo

ANEXO II

POLÍTICA DE MESA LIMPA E POLÍTICA DE TELA LIMPA

1. Este Anexo institui a política de mesa limpa para papéis e mídias removíveis, bem como

a política de tela limpa para os recursos de processamento da informação, reduzindo assim os riscos de acessos não autorizados, danos e perdas de informações durante e fora do horário normal de trabalho.

1.1. Esta política deverá considerar a classificação das informações, os riscos correspondentes e os aspectos culturais da SETIC.

1.2 Os servidores deverão observar que os documentos, dispositivos e quaisquer informações deixadas sobre as mesas de trabalho são potenciais alvos para furtos, ou mesmo, podem ser extraviadas durante as atividades de limpeza. Da mesma forma, essas forntes de informação, caso deixadas sobre as mesas, estarão expostas ao risco de danos ou destruição em caso de sinistro, como incêndios ou inundações por exemplo.

2. Os pontos de controle recomendados são os listados abaixo:

a. Papéis e mídias de computador, quando não estiverem sendo utilizados, devem ser guardados em locais seguros (cofres, arquivos metálicos ou gavetas), com fechaduras, principalmente fora do horário de expediente normal.

b. Informações restritas ou sigilosas, quando não requeridas, devem ser guardadas em local distante, seguro e fechado, se possível em um cofre ou arquivo resistente a incêndios, principalmente após o expediente ou quando o local de trabalho estiver vazio.

c. Computadores pessoais, estações de trabalho e impressoras não devem ser deixados ligados quando não assistidos, e sempre devem estar protegidos por senhas, chaves ou outros tipos de controle de acesso.

d. Área de Trabalho ou Desktop nas estações de trabalho não devem ser local de armazenamento de informações. As Informações deverão ser mantidas nos servidores de rede e/ou nuvem.

e. Pontos de envio e recepção de correspondências e equipamentos de fax, quando não assistidos, devem ser protegidos.

f. Copiadoras devem ser travadas de forma a estarem protegidas contra uso indevido, fora do horário de expediente normal.

g. Informações classificadas como restritas ou sigilosas, quando impressas, devem ser acompanhadas e retiradas da impressora imediatamente.

3. Uma política de mesa e tela limpa reduz o risco de acesso não autorizado, perda e dano de informações durante e após o horário normal de trabalho. Cofres, servidores de rede e outras formas de instalações de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

Documento assinado eletronicamente por **DELNER FREIRE**, **Superintendente**, em 09/06/2021, às 12:48, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0018466170** e o código CRC **92EFF5EB**.

Referência: Caso responda esta Portaria, indicar expressamente o Processo nº 0024.093152/2021-11 SEI nº 0018466170