Política Corporativa de Segurança da Informação

PCSI

MTPrev

GOVERNO DO ESTADO DE MATO GROSSO

Mauro Mendes – Governador

MATO GROSSO PREVIDÊNCIA - MTPREV

Elliton Oliveira de Souza – Diretor Presidente

DIRETORIA DE ADMINISTRAÇÃO SISTÊMICA

Paola Correia Sanches – Diretora Administrativa

COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO

Flávio Lopes da Silva – Coordenador

Março - 2021

Cuiabá-MT

A Política Corporativa de Segurança da Informação do Mato Grosso Previdência – MTPrev utiliza-se da Resolução nº 003/2010, Anexo I do Governo do Estado de Mato Grosso, definindo Políticas e Diretrizes de Segurança da Informação Estadual como base normativa.

Esta Resolução tem por objetivo estabelecer diretrizes e normas gerais para a gestão da segurança da informação de maneira a preservar a integridade, confidencialidade e disponibilidade das informações. Esse decreto descreve procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

SUMÁRIO

1. INTRODUÇÃO

Política Corporativa de Segurança de Informação é um conjunto de princípios, objetivos e diretrizes que norteiam a gestão de segurança de informações e que deve ser observado por todos os agentes públicos, independentes do cargo ou função que ocupam e por terceiros, que porventura, venham a ter acesso às informações da instituição. Esta Política é aderente aos princípios e diretrizes da segurança da informação instituídas pela Administração Pública Estadual do Poder Executivo e está em conformidade com os requisitos do negócio do MTPrev e com as leis e regulamentações pertinentes.

2. OBJETIVO

O objetivo da Política Corporativa de Segurança da Informação do MTPrev é declarar o direcionamento estratégico acerca da segurança da informação. São objetivos secundários desta Política:

- Preservar a confidencialidade, a integridade e a disponibilidade das informações sob responsabilidade da Instituição;
- Criar, manter e aperfeiçoar conhecimentos de segurança da informação em todos os níveis da entidade;
- Aumentar o nível de conscientização dos agentes públicos e prestadores de serviços da Autarquia em relação a adoção de políticas, regulamentos, normas técnicas e procedimentos de segurança da informação;
- Assegurar aderência às políticas e diretrizes do Estado de Mato Grosso referente às questões relacionadas à segurança da Informação;
- Assegurar a proporcionalidade da adoção de soluções de segurança da informação.

3. PÚBLICO ALVO

Esta Política se destina aos agentes públicos do Mato Grosso Previdência – MTPrev e terceiros com acesso às informações sob a responsabilidade da Autarquia que necessitem acessar e/ou manipular informações de negócio da instituição, seja de modo direto ou através de recursos de informação.

4. PRINCÍPIOS

O Mato Grosso Previdência – MTPrev respeita os princípios constitucionais, organizacionais e do arcabouço legislativo vigente que rege a Administração Pública Estadual e notadamente, os seguintes princípios:

I. Responsabilidade:	Todos os agentes públicos e prestadores de serviço do MTPrev são responsáveis pelo cumprimento das normativas de segurança da informação.
II. Conhecimento:	Todos os agentes públicos e prestadores de serviço do MTPrev tomação ciência de todas as normativas de segurança da informação para o pleno desempenho de suas atribuições regimentais e contratuais.
III. Legalidade:	As ações de segurança da informação levarão em consideração a legislação vigente e as políticas organizacionais formalmente estabelecidas.
IV. Proporcionalidade	O nível, a complexidade e os custos das ações de segurança serão adequados ao entendimento administrativo e ao valor do ativo da informação a proteger.
V. Publicidade	A Política de Segurança da Informação adotada e instituída pelo MTPrev deve ser de conhecimento público por meio da sua publicação.
VI. Transparência	Garantia de informações claras, precisas e facilmente acessíveis, observados os segredos comerciais e industrial.
VII. Proteção de Dados	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
VIII. Moralidade	Os Agentes e a Administração Pública devem agir conforme os preceitos éticos, de boa fé, decoro, lealdade, honestidade e probidade na prática diária da boa administração.
IX. Impessoalidade	Exclusão da promoção pessoal de autoridade ou serviços públicos sobre suas relações administrativas, no exercício de fato. Os atos/informações são da instituição e não dos agentes públicos.

5. DEFINIÇÕES

Agente Público	Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nas entidades da administração pública direta, indiretamente ou fundacional.
Ativo	Qualquer coisa que tenha valor para a organização. Qualquer produto, bem ou informação. (Ex.: equipamentos, relatório impresso, sistema de informação.)
Ativo de Informação	Refere-se ao ativo que armazena, transmite ou processa informações. (Ex.: pedaço de papel, computadores, redes, discos rígidos, banco de dados, fitas, pendrive, dentre outros)
Autenticidade	Conceito referente à garantia de que uma informação é de autoria legítima a quem se atribui.
Confidencialidade	Conceito no qual o acesso à informação deve ser concedido a quem de direito, ou seja, apenas às entidades autorizadas pelo proprietário ou dono da informação.
Custódia	Ato ou efeito de proteger, guardar algo, proteção, guarda.
Disponibilidade	Conceito no qual a informação deve estar disponível para as entidades autorizadas sempre que necessário ou demandado.
Integridade	Conceito no qual somente alterações, supressões e adições autorizadas devem ser realizadas nas informações.
Legalidade	Conceito referente à garantia de que todas as práticas de segurança da informação estão em conformidade com a legislação pertinente.
Política	Intenções e diretrizes globais formalmente expressas pela direção.
Política Estadual de Segurança da Informação	É uma declaração formal do compromisso da Administração Pública do Poder Executivo Estadual com a proteção das informações de sua propriedade e/ou sob sua custódia, devendo ser cumprida por todos os agentes públicos e prestadores de serviços.
Processos	Todos os processos existentes em qualquer instituição, independente de

Organizacionais	porte e segmento de mercado, que viabilizam o funcionamento coordenador dos subsistemas da organização em busca do seu desempenho geral.
Processo Organizacionais Críticos	Processos organizacionais que, se não executados de maneira esperada, podem impedir a MTI de cumprir a sua missão ou causar danos a terceiros.
Proporcionalidade	O nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nas informações considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.
Recurso de informação	Qualquer dispositivo de hardware ou software de apoio à informação.
Credencial de Acesso	Permissão concedida por autoridade competente. Após o processo de credenciamento cujo no qual habilita determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação de usuário e senha.
Terceiro	Pessoa ou entidade que não se enquadra como agente público, mas participa diretamente ou indiretamente de um contrato, em um ato jurídico ou em um negócio, ou que pode ter algum relacionamento com processos da instituição.
Termo de Responsabilidade e Sigilo	Termo assinado pelo usuário comprometendo-se a contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.
Correio Eletrônico Corporativo	Também denominado correio eletrônico institucional, é o sistema de correio cujo domínio identifica a instituição (mtprev.mt.gov.br)
Endereço de Conta de Correio Eletrônico	É o nome individualizado de uma conta de correio eletrônico, formado pela identificação do usuário, caractere “@” acompanhado do domínio. Exemplo: flaviosilva@mtprev.mt.gov.br
Dispositivo Móvel de Armazenamento	É um dispositivo de porte pequeno capaz de armazenar informações (dados) para posterior consulta ou uso. Exemplos: CD, cartão de memória, pendrive.
Homologação	Processo que consiste na aprovação e legitimação de algum ato ou procedimento, por autoridade legal.
Informação Sensível	É aquela informação que deve ser protegida contra exposição, perda e/ou modificação não autorizada. A informação sensível é aquela que, se não protegida adequadamente, pode incorrer em penalidades legais, danos

	aos negócios e/ou à imagem da instituição.
Pastas Públicas	Pasta existente dentro de um sistema de armazenamento de arquivos digitais sem restrição de acesso para leitura.
Recursos de Informação	Qualquer dispositivo de hardware ou software de apoio à informação.
Revogação de Acesso	Ato ou efeito de inibir, em caráter definitivo, o acesso de determinado usuário a algo recurso.
SAC	Serviço de Atendimento ao Cliente
Sistema Aplicativo	Sistema informatizado de apoio a um sistema de informação, tais como: FIPLAN, Sistema de Protocolo, SEAP, E-Turmalina.
Sistema de Comunicação Instantânea	É o Software desenvolvido para troca de mensagens em tempo real. Exemplo: Google Hangout.
Software	São todos os programas existentes em um computador, como sistema operacional, aplicativos, processadores de texto (MS Word), dentre outros.
Software Homologado	Software cuja instalação e uso foram autorizados pela instituição após um processo formal de aprovação.
Usuário	Toda e qualquer pessoa (servidor público, terceirizado, colaborador, consultor, estagiário, menor aprendiz) que obteve acesso aos recursos de informação da instituição.

6. DIRETRIZES

A Política Corporativa de Segurança da Informação do MTPrev tem como princípio norteador proteger adequadamente as informações de sua propriedade e/ou sob sua custódia, independentemente de sua mídia e durante todo o seu ciclo de vida, em conformidade legal.

6.1 Classificação da Informação

Para garantir a proteção adequada, as informações devem ser identificadas e classificadas, considerando os critérios de confidencialidade, integridade, disponibilidade e legalidade além de respeitar o organograma vigente desta Instituição. Todo agente público ou terceiro, ao manter contato com a

informação de responsabilidade desta Autarquia, deve ser capaz de identificar e respeitar a hierarquia e a classificação atribuída e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação atribuídas.

6.2 Proteção da Informação

Toda e qualquer informação interna gerada, adquirida e processada pelo MTPrev é considerado de sua propriedade, devendo ser utilizada exclusivamente, para atender aos seus interesses legítimos. Toda e qualquer informação de propriedade de terceiros, tais como de clientes ou de agentes públicos, gerada, adquirida, armazenada e processada pela Autarquia, é considerada sob sua custódia, devendo ser utilizada exclusivamente para atender aos interesses contratuais e legais do seu proprietário legítimo e a bem do interesse público. As informações de propriedade do MTPrev ou sob sua custódia devem ter mecanismos de proteção adequados, durante todo o ciclo de vida, em conformidade com as classificações atribuídas.

6.3 Recursos da Informação

Todo sistema de informação do MTPrev, bem como seus recursos de informação, é de propriedade da Instituição, devendo ser utilizados exclusivamente para atender aos seus interesses legítimos. A utilização dos recursos de informação pelos agentes públicos ou terceiros deve ocorrer conforme os padrões de segurança adotados pela instituição, de forma a preservar a confidencialidade, integridade e disponibilidade das informações.

6.4 Continuidade dos Negócios

Todos os processos organizacionais críticos deverão estar devidamente documentados, e a documentação deve ser mantida atualizada e disponível para os agentes públicos envolvidos. A execução dos processos organizacionais críticos em sua totalidade, não deverá estar sob a carga de um único agente público. As unidades gerenciais técnicas são responsáveis por elaborar e manter planos de continuidade de negócio, de acordo com a sua criticidade, de forma a reduzir os impactos decorrentes da interrupção de operações causadas por desastres ou falhas de segurança. A implantação do processo de Gestão e Continuidade de Negócios buscará minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades, além de recuperar e reduzir perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação

6.5 Monitoramento e Controle

Todos os agentes públicos e prestadores de serviços da instituição devem ter ciência de que a Instituição pode, a qualquer momento e mediante sua autotutela ou competência como empregadora ou contratante, monitorar as suas atividades no uso de informações e recursos de informação de propriedade ou custódia do MTPrev. Auditorias internas e externas podem ser realizadas pela Instituição periodicamente para averiguar o cumprimento das normas de segurança da informação adotadas.

Sistematizar o processo de monitoramento dos empregados e colaboradores na execução dos seus processos de trabalho, realizando verificações periódicas e identificando possíveis fragilidades quanto aos aspectos de segurança da informação. O MTPrev deve garantir que as atividades em seus processos de trabalho sejam claramente definidas e atribuídas a mais de um empregado ou colaborador de forma a minimizar a probabilidade de alterações indevidas, acessos não autorizados ou controle total das informações.

6.6 Áreas de Segurança

As áreas que armazenas as informações e/ou recursos de informação que são críticos para o MTPrev estão identificadas e protegidas de acordo com a classificação das informações armazenadas. O gestor de Segurança da Informação, em conjunto com a Área de Tecnologia da Informação devem definir os critérios a serem utilizados nos registros de eventos de segurança da informação, considerando os seguintes requisitos mínimos: temporalidade de retenção dos registros, viabilidade e performance, bem como respeitar a classificação atribuída à informação.

6.7 Quanto a gestão de segurança da informação

Manter o controle na elaboração e na execução de Contratos, de maneira que seja exigida a assinatura do Termo de Confidencialidade e de Conhecimento da Política das Normas de Segurança da Informação. As Unidades Administrativas devem monitorara e realizar a análise crítica dos serviços prestados de segurança da informação, seguindo as definições estabelecidas nas normas de regência de licitações e contratos nos termos contratuais. O processo de Gestão de Riscos de Segurança da Informação deve estar alinhado ao planejamento estratégico e, também, com o processo maior de gestão de riscos corporativos.

6.8 Quanto às diretrizes para avaliação da conformidade legal

Realizar a avaliação de conformidade em segurança da informação, considerando no mínimo, as legislações vigentes a respeito da segurança da informação para a Administração Pública Estadual, e as normas internas do MTPrev. Identificar, organizar e armazenar a legislação, regulamentação e contratos relevantes aos processos de trabalho, de forma a facilitar sua localização e uso, bem como preservá-los quanto aos aspectos de autenticidade, confidencialidade, integridade e disponibilidade.

Preservar o direito autoral e propriedade industrial das informações e recursos que são utilizados nos processos de trabalho. Assegurar e garantir que seja divulgada e cumprida a Política de Segurança da Informação e normas correlatas. Planejar e acordar previamente, entre as áreas envolvidas, a realização de auditorias periódicas nos recursos de tecnologia da informação que suportam os processos de trabalho críticos, a fim de diminuir os riscos quanto à segurança da informação.

6.9 Quanto às diretrizes para disponibilização de acessos

Todo agente público dever possuir capacitação mínima nos processos, nos sistemas de informação e na utilização dos recursos necessários à sua rotina de trabalho. Cabe ao gestor imediato providenciar as capacitações.

Todos os agentes públicos e terceiros, ao obter acesso a informações de negócio devem, obrigatoriamente, aplicar as regras de segurança estipuladas pela Instituição. O agente público e/ou terceiro, ao obter acesso a informações de negócio do MTPrev deve:

- Utilizar as informações disponibilizadas pela Instituição somente nas atividades a que compete exercer, não podendo transferi-las a outrem, seja a título oneroso ou gratuito, estando ciente de que suas ações poderão ser monitoradas, acompanhadas e eventualmente auditadas.
- Responsabilizar-se, prestar contas e demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e,

inclusive, da eficácia dessas medidas, quando cabível.

- Guardar o sigilo e a privacidade das senhas de acesso aos recursos de informação de propriedade ou sob a responsabilidade do MTPrev.
- Não coagir outros agentes públicos, inclusive subordinados, a fornecer senhas de acesso a qualquer recurso da informação.
- Observar que o tratamento de dados pessoais, quando necessário, deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.
- Entregar, ao término de seu de contrato de trabalho ou da realização dos trabalhos como agente público e/ou terceiros, todo e qualquer material de propriedade do MTPrev, inclusive notas pessoais envolvendo matéria sigilosa, registro de documentos de qualquer natureza que tenham sidos usados, criados ou estado sob seu controle.
- Ao término de seu contrato de trabalho ou da conclusão dos serviços, não utilizar, sem autorização, qualquer informação de negócio do MTPrev produzida ou adquirida de sua prestação de serviços.

6.10 Termo de Responsabilidade e Sigilo

Todos os agentes públicos do MTPrev devem formalizar o comprometimento com a segurança da informação, através da assinatura do Termo de Responsabilidade e Sigilo adotados por esta Instituição, antes do seu encaminhamento à sua unidade de lotação. Os termos de responsabilidade assinados devem ser mantidos na pasta funcional do agente público, para fins de controle e atendimento a eventuais determinações judiciais, administrativas ou a auditorias formalmente designadas. Terceiros que, pela natureza dos trabalhos a serem desempenhados, necessitarem obter acesso a informações e recursos de informação sob a responsabilidade do MTPrev, devem antecipadamente formalizar o comprometimento com a segurança da informação através da assinatura do Termo de Responsabilidade e Sigilo apropriado, adotado pela Autarquia.

Os termos de responsabilidade assinados devem ser mantidos como parte da documentação dos respectivos contratos, para fins de controle e atendimento a eventuais disputas judiciais ou a auditorias formalmente designadas. Quando não houver contrato formalizado com o terceiro, o Termo de Responsabilidade e Sigilo ficará sob a guarda e controle da Unidade demandante dos acessos. Terceiros investidos de autoridade pública e em diligência não necessitam o compromisso para obtenção dos acessos cedidos, porém ficará sob a responsabilidade da unidade envolvida o registro dos acessos.

6.11 Concessão de Acessos

Os acessos aos recursos de informação deverão ser concedidos em estrita conformidade com as necessidades das atividades desempenhadas pelos agentes públicos e terceiros. A solicitação de acesso aos recursos de informação do MTPrev para o agente público ou terceiro deve ser formalizada pelo gestor imediato ou pelo gestor da unidade demandante, através dos canais de solicitação de serviços instituídos pela Autarquia. Cada solicitação de acesso deve ser criticamente analisada no intuito de verificar se a autoridade do solicitante é devida, se as informações fornecidas estão completas e se a situação funcional do agente público ou a situação contratual do terceiro é compatível com o uso dos recursos solicitados. A identificação do usuário dos recursos de informação deve seguir os padrões estabelecidos na Instituição. As credenciais de acesso aos recursos de informação devem ser comunicadas unicamente ao usuário dos recursos e de modo seguro.

6.12 Gerenciamento dos Acessos

Medidas devem ser implementadas de modo a assegurar que os acessos concedidos são os indispensáveis para o cumprimento de funções, em atendimento aos interesses legítimos do MTPrev. Ações suspeitas de concessão ou revogação indevida de acessos devem ser prontamente informadas à Unidade responsável pela segurança da informação da instituição.

6.13 Afastamentos e Desligamentos

Os acessos a informações e a recursos de informação concedidos:

- Aos agentes públicos e terceiros devem ser bloqueados em eventuais remanejamentos e/ou afastamentos temporários da Autarquia.
- Aos agentes públicos desligados devem ser tempestivamente bloqueados
- A terceiros devem ser tempestivamente bloqueados quando desligados das atividades que demandaram o acesso ou no término do contrato.

Em caso de afastamento temporário ou desligamento, os recursos de informação da instituição sob a guarda do agente público ou de terceiros devem ser formalmente devolvidos ao gestor da Unidade.

6.14 Correio Eletrônico Corporativo

As contas do correio eletrônico corporativo são disponibilizadas aos usuários como ferramenta de trabalho e, portanto, são de propriedade do MTPrev em parceria com a MTI.

- Os usuários não deverão manter qualquer expectativa de privacidade e propriedade sobre as mensagens criadas, armazenadas, enviadas ou recebidas através do sistema de correio eletrônico corporativo.

Todas as mensagens relativas às atividades pertinentes ao trabalho do usuário devem ser enviadas e recebidas pelo correio eletrônico corporativo. Os endereços das contas do correio eletrônico corporativo somente serão fornecidos a terceiros para atender aos interesses do MTPrev. O usuário deve remover das caixas de sua conta de correio eletrônico corporativo as mensagens que não sejam mais necessárias, a fim de não sobrecarregar os recursos do sistema. O usuário deve verificar se a origem da mensagem recebida é de fonte confiável e de interesse da instituição, a fim de evitar algum dano para a instituição e para si mesmo.

- Em caso de suspeita, o usuário não deverá abrir arquivos anexos ou “clicar” em links no conteúdo da mensagem.

O usuário é responsável pelo conteúdo de mensagens enviadas via correio eletrônico corporativo sob sua identificação.

- O conteúdo de qualquer mensagem de correio deve ser apropriado às diretrizes do Mato Grosso Previdência – MTPrev.
- São expressamente proibidas e inaceitáveis mensagens que contenham conteúdo inapropriado e/ou ilícito, tais como, não limitado a: pornografia, discriminação, correntes,

spam ou mensagens de caráter comercial, político-partidário, direcionamento (links) a endereços maliciosos, arquivos executáveis maliciosos, apologia à violência, apologia ao uso de drogas, assédio moral ou sexual, difamação.

É vedado ao usuário o envio de mensagens em massa

- Cabe a Assessoria de Comunicação do MTPrev a responsabilidade pelo envio em massa de mensagens para toda a instituição ou para outras entidades governamentais.

Todas as mensagens originárias de contas do correio eletrônico corporativo deverão conter a assinatura e a foto do remetente em formato padronizado pela instituição.

O usuário não deve compartilhar as credenciais de acesso de sua conta de correio eletrônico corporativo.

- Caso ocorra qualquer irregularidade ou o uso inadequado da conta de correio eletrônico, o titular da conta responderá pelos atos praticados com suas credenciais, se confirmada a negligência ou ação deliberada.

6.15 Sistema de Comunicação Instantânea

A ferramenta de comunicação instantânea institucional, disponibilizada pelo MTPrev, deve ser utilizada para fins institucionais. O conteúdo de qualquer mensagem de comunicação instantânea deve ser apropriado às atividades da instituição.

- São expressamente proibidas mensagens que contenham conteúdo inapropriado e ilícito, tais como, entre outros: pornográficos, discriminatório, correntes, spam, arquivos executáveis maliciosos, apologia à violência, apologia ao uso de drogas, ataques, assédio, difamação.

Não é permitida a criação ou participação do usuário em listas de discussão com assuntos alheios aos interesses da Instituição. O usuário é responsável pelo conteúdo de mensagens enviadas sob sua identificação. O usuário não deverá manter qualquer expectativa de privacidade sobre mensagens trocadas através do sistema de comunicação instantânea corporativo.

6.16 Sistemas, Aplicativos e demais Softwares

É proibido o uso, instalação, cópia, manutenção ou remoção de softwares nos equipamentos do MTPrev, a menos que essas ações façam parte das atribuições legais do agente público ou terceiro. Diante dessas necessidades, uma solicitação deverá ser encaminhada à unidade responsável através do SAC. O acesso, inserção e o uso de dados obtidos pelos sistemas aplicativos devem se restringir ao exercício legal da função do agente público ou do terceiro.

- É expressamente vedado o uso ou divulgação das informações obtidas pelos sistemas aplicativos para qualquer outro propósito distinto do designado.

Todo usuário deve ter privilégio de acesso condizente com as suas funções. Caso o usuário verifique a existência de privilégios além de suas necessidades funcionais, ele deve comunicar ao seu superior para que este providencie a revogação dos privilégios excedentes. Se o usuário não reconhecer as informações do último acesso sob sua identificação que, porventura, sejam fornecidas pelo sistema, ele deve comunicar imediatamente à Unidade responsável pela segurança da informação pelos canais disponibilizados. Em caso de suspeita de uso de sistemas aplicativos e de suas informações por qualquer agente público ou terceiros em desconformidade com os interesses do MTPrev ou com as suas funções, o fato deve ser comunicado a Unidade responsável pela segurança de informação pelos

canais disponibilizados.

6.17 Sistema de Arquivos em Rede e Nuvem

Arquivos relacionados às atividades de trabalho devem ser obrigatoriamente armazenados no sistema de arquivos em rede do MTPrev, em diretórios específicos destinados à unidade gerencial responsável pelo trabalho, a fim de garantir a proteção adequada à continuidade do negócio. É vedado ao agente público ou terceiro armazenar no sistema de arquivos em rede do MTPrev, conteúdos de interesse particular ou alheios aos interesses da instituição. Havendo necessidade de conceder ou restringir acesso a diretórios, o gestor da unidade deve efetuar uma solicitação à unidade responsável pela administração dos sistemas de arquivo através do SAC.

6.18 Internet

É expressamente proibido utilizar a internet, através dos recursos do MTPrev ou dentro de suas instalações de forma que possa prejudicar a imagem, o andamento dos seus trabalhos, ou que coloque em risco os ativos de rede do MTPrev ou do Estado (rede Infovia). Não é permitido o uso das conexões de Internet, através dos recursos de informação do MTPrev, nas seguintes situações, dentre outras:

- Acesso à página de bate-papo, comunidade de discussão, sites de relacionamento e similares sem autorização e fora dos interesses do MTPrev e da Administração Pública.
- Criação de comércio eletrônico fora dos interesses do MTPrev e da Administração Pública.
- Acesso a sites de conteúdo ilegal ou impróprio tais como: pornográfico, preconceituoso, pedófilo, jogos (online, download e/ou jogos de azar) que façam apologia ao uso de drogas ou à violência etc.
- Baixar programas, jogos, protetores de telas, músicas, vídeos, imagens, streaming de vídeo e de áudio etc. sem a devida permissão e autorização.
- As situações descritas no item anterior são consideradas permitidas se, e somente se, estas fizerem parte das atribuições regimentais legítimas, atenderem aos interesses do MTPrev e da Administração Pública.

Os usuários podem baixar conteúdo da internet, desde que estes sejam pertinentes às suas atribuições funcionais e sejam de interesse do MTPrev e da Administração Pública. Somente será permitida a publicação (upload) de conteúdo de propriedade do MTPrev, ou que estejam sob custódia, mediante autorização expressa da Autarquia e em atendimento aos interesses legítimos do MTPrev e da Administração Pública. O MTPrev, através do setor competente, se reserva ao direito, a qualquer momento e mediante a sua autotutela ou competência como empregadora ou contratante, de examinar os registros de acessos à Internet para verificação de atendimento à sua política de segurança. Tais registros podem referir-se a websites visitados, arquivos copiados da internet, tempo gasto nos acessos e outras informações necessárias para o gerenciamento dos recursos e realização de auditorias. As permissões de acesso ao conteúdo da internet serão concedidas em conformidade com as atividades desempenhadas.

6.19 Equipamentos do MTPrev

Ao se ausentar do ambiente de trabalho, o usuário deve bloquear a estação de trabalho de modo a evitar o uso não autorizado dos recursos disponíveis.

- O usuário da estação de trabalho será responsabilizado pelas ações executadas sob sua identificação em caso comprovado de negligência.

Os equipamentos do MTPrev, tais como estações de trabalho, notebooks, impressoras, de responsabilidade do usuário devem ser desligados diariamente ao término do expediente, a menos que expressamente orientado para o contrário.

- O usuário deve encerrar as sessões abertas e desligar o equipamento de forma adequada e segura.
- Os equipamentos portáteis do MTPrev, como notebooks e tablets, quando não estiverem em uso, devem ser mantidos em local seguro.
- Os equipamentos portáveis do MTPrev não podem ser deixados desassistidos, especialmente, em ambientes públicos.

O usuário deve evitar armazenar informações de natureza sensível em equipamentos portáteis cuja exposição não autorizada pode acarretar danos à imagem e aos negócios do MTPrev e da Administração Pública.

- Quando apropriado, o sistema de criptografia adotado pela Autarquia deve ser empregado para proteger as informações sensíveis.

É vedado ao usuário o privilégio de administrador de qualquer equipamento do MTPrev, sem a autorização do diretor da área e anuência da unidade responsável pela manutenção dos equipamentos. O usuário ao observar a falta de qualquer recurso de informação no ambiente de trabalho, deve fazer uma notificação ao superior imediato. O usuário não pode, em hipótese alguma, sem autorização da área responsável, desativar, desinstalar ou alterar as configurações dos sistemas de segurança instalados nos equipamentos do MTPrev, tais como antivírus, firewall e/ou demais softwares instalados. O acesso remoto às estações de trabalho só será permitido pelas unidades responsáveis pela manutenção e suporte dos recursos de informação do MTPrev. É absolutamente vedada ao usuário a abertura de equipamentos para qualquer tipo de reparo, verificação, limpeza ou para quaisquer outras finalidades.

- Ao averiguar qualquer problema de mau funcionamento de recursos de informação do MTPrev, o usuário deve solicitar através do SAC o devido reparo.

É proibida a transferência de equipamentos entre unidades sem a autorização expressa da área responsável pelo controle do sistema de patrimônio do MTPrev. O usuário deve zelar pela conservação dos equipamentos sob a sua responsabilidade. Equipamentos do MTPrev, em hipótese alguma, poderão ser utilizados por pessoas não autorizadas.

6.20 Equipamentos Particulares

Os equipamentos de uso particular poderão se conectar à rede do MTPrev mediante a formalização do processo de autorização. A Autarquia pode revogar a autorização concedida a qualquer tempo. O proprietário é responsável pela guarda e uso do equipamento e será responsabilizado por quaisquer danos causados à instituição e a terceiros decorrentes do uso inadequado ou das vulnerabilidades de segurança existentes no equipamento.

6.21 Dispositivos Móveis de Armazenamento

O usuário deve respeitar o que estabelece a classificação das informações instituídas, armazenando

somente informações autorizadas e, quando requerido, aplicando as tecnologias de proteção adotadas pela instituição. Em caso de perda ou extravio de dispositivos móveis, contendo informações classificadas o usuário deve comunicar o incidente de segurança através dos canais disponibilizados pela instituição. O dispositivo móvel utilizado pelo usuário deverá ser conectado aos recursos tecnológicos da instituição que possuam o sistema de antivírus padrão ativado.

- Caso o sistema de antivírus padrão seja desativado, o usuário deve comunicar à unidade responsável pelo SAC e solicitar providências.

O usuário é responsável pela verificação da existência de códigos maliciosos no dispositivo móvel, utilizando o sistema de antivírus padrão.

6.22 Rede Lógica e Elétrica

Não é permitido realizar varreduras na rede (scan), exceto pelos agentes públicos ou terceiros designados para tal e em conformidade com suas funções regimentais e/ou contratuais. Não é permitido utilizar a rede elétrica estabilizadas para uso de equipamentos que não sejam de Tecnologia da Informação. Não será permitida a alteração da rede lógico-elétrica (layout) dos ambientes de trabalho, exceto pelos agentes públicos ou terceiros designados para tal e em conformidade com suas funções regimentais e/ou contratuais.

7. Disposições Finais

Havendo indícios de quebra de segurança ou violação de quaisquer das vedações constantes neste regulamento, o MTPrev adotará imediatamente, medidas para a sua apuração, utilizando-se para tanto dos meios e procedimentos legalmente previstos. Diante de suspeita ou de evidência de descumprimento de qualquer dos itens deste regulamento, caberá ao agente público comunicar o ocorrido à unidade responsável pela segurança da informação a fim de que sejam encaminhadas as providências de apuração de responsabilidade.

Casos omissos a este documento devem ser tratados pela Diretoria Administrativa Sistêmica do Mato Grosso Previdência – MTPrev. Não é dado ao agente público o direito de alegar desconhecimento do Regulamento de Política Corporativa de Segurança da Informação desta Instituição. O não cumprimento do presente regulamento acarretará penalidades cabíveis, previstas no âmbito administrativo, cível e criminal.

8. ATUALIZAÇÃO

Esta Política deve ser revisada e atualizada, periodicamente, a cada 4 (quatro) anos, desde que não ocorram eventos ou fatos relevantes que exijam uma revisão antecipada.

9. REFERÊNCIAS

- ABNT NBR ISSO/IEC 27002:2013;
- Decreto Estadual Nº 1973 de 25 de outubro de 2013;
- Lei Nº 12.527 de 18 de novembro de 2011;
- Lei Nº 13.709 de 14 de agosto de 2018;
- NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação;
- NBR ISO/IEC 27002:2005 – Código de Práticas para Gestão da Segurança da Informação;
- Norma de Segurança Estadual para Acesso à Informação (Resolução COSINT Nº 0008/2010);
- Norma de Segurança Estadual para Uso da Internet (Resolução COSINT Nº 0010/2011);
- Norma de Segurança Estadual para Uso do Correio Eletrônico Corporativo (Resolução COSINT Nº 0009/2011);
- Política de Segurança da Informação MTI (Portaria Nº 104/2016);
- Políticas e Diretrizes de Segurança da Informação Estadual – Resolução COSINT nº 003/2010;
- Regulamento de Acesso à Informação e Recurso de Informação da MTI (Portaria Nº 115/2016);