ATOS NORMATIVOS DA ADMINISTRAÇÃO DIRETA

Secretaria de Estado de Governo e Gestão Estratégica

DELIBERAÇÃO CETI Nº 02, DE 24 DE FEVEREIRO DE 2022.

Aprova Política de Segurança da Informação - PSI.

O PRESIDENTE DO COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO - CETI, no uso de suas atribuições, com fundamento no inciso I, do art. 2º, do Decreto 15.478, de 20 de julho de 2020 e no art. 16, do Regimento Interno, de 30 de novembro de 2020, e

Considerando votação unânime da Política de Segurança da Informação apresentada em reunião realizada em 09 de fevereiro de 2022. Considerando a necessidade de regulamentação desta,

D E L I B E R A:

Art. 1º Aprova a Política de Segurança da Informação.

Art. 2º Esta deliberação entra em vigor na data de sua publicação.

Campo Grande, 24 de fevereiro de 2022.

GUSTAVO NANTES GUALBERTO
Presidente do Comitê Estratégico
de Tecnologia da Informação - CETI

LORIVALDO ANTONIO DE PAULA
Secretário do Comitê Estratégico
de Tecnologia da Informação - CETI

ANEXO I À DELIBERAÇÃO/CETI Nº 02, DE 24 DE FEVEREIRO DE 2022

GOVERNO DO ESTADO DE MATO GROSSO DO SUL
CONSELHO DE GOVERNANÇA DE MATO GROSSO DO SUL
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. APRESENTAÇÃO

A Política de Segurança da Informação, PSI, é o documento que orienta e estabelece as diretrizes corporativas do Governo do Estado de Mato Grosso do Sul para a proteção dos ativos de informação com eficiência e eficácia, de modo seguro e transparente, garantindo a disponibilidade, integridade, autenticidade, legalidade e sigilo das informações neles contidas, de forma alinhada aos requisitos legais e exigências dos Órgãos Regulatórios de acordo com o negócio. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

Este documento foi elaborado com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis brasileiras vigentes.

2. OBJETIVO

A Política de Segurança da Informação é uma declaração formal do Governo do Estado de Mato Grosso do Sul acerca de seu compromisso com a proteção dos ativos de informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários.

3. ABRAGÊNCIA

Esta política aplica-se a todos os colaboradores, prestadores de serviços, usuários internos e externos e quaisquer pessoas que tenham acesso as informações pertencentes ou custodiadas pelo Governo do Estado de Mato Grosso do Sul.

4. TERMOS E CONCEITOS

- ***Software*:** É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares;
- ***Backup*:** É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou

corrupção de dados;

- **VPN (*Virtual Private Network*):** Modalidade de acesso à Rede Estadual de Informática do Governo, que possibilita a conectividade, via Internet, de um equipamento externo à rede, tanto *on premise* quanto em ambiente na nuvem, provendo funcionalidades e privilégios como se ele estivesse conectado física e diretamente à rede;
- **Dados Pessoais:** Informações que permitem identificar, direta ou indiretamente, um indivíduo. Dados pessoais incluem, sem limitação: nome, documentos de identidade, número de telefone, endereço de e-mail e endereço de IP;
- **Princípios da Segurança da Informação:** Integridade, Confidencialidade, Disponibilidade, Autenticidade e Legalidade;
- **Integridade:** Garantia de que a informação esteja completa, exata e íntegra e que seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Confidencialidade:** Garantia de que o acesso à informação estará disponível ou será divulgada somente a indivíduos, entidades ou aplicativos autorizados;
- **Disponibilidade:** Garantia de que os usuários autorizados tenham acesso à informação quando necessário;
- **Autenticidade:** Garantia da identidade do remetente da informação. Pela autenticidade, garante-se que a informação é proveniente da fonte anunciada, sem sofrer alteração durante o envio;
- **Legalidade:** Garantia de que o uso e manuseio das informações sigam as leis vigentes no país;
- **Não repúdio:** Garantia de que o autor não negue ter criado e assinado determinado arquivo ou documento;
- **Engenharia Social:** É uma expressão utilizada para representar uma técnica empregada por criminosos virtuais para induzir usuários desavisados ou desatentos a enviar dados confidenciais, permitir a infecção de seus computadores com *malwares* ou abrir links para sites suspeitos, visando obter informações sigilosas e dados confidenciais. Essa técnica se baseia principalmente na falta de conscientização do usuário com relação à Segurança da Informação;
- **Incidente de Segurança:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos Recursos de Tecnologia da Informação (RTI's) levando a perda de um dos princípios da Segurança da Informação. Exemplos: Tentativas de ganhar acesso não autorizado a sistemas ou dados lógicos ou físicos e indisponibilidade de informações e dados para a execução de rotinas e processos.
- **REIT (Rede Estadual de Informática e Telecomunicações):** Rede de dados computacional do Governo do Estado de Mato Grosso do Sul;
- **UTIC (Unidade de Tecnologia da Informação e Comunicação):** Departamento responsável pela gestão de Tecnologia da Informação e Comunicação e pelo planejamento, coordenação e acompanhamento das ações relacionadas às soluções de TIC da unidade, do órgão, da autarquia ou da fundação do Poder Executivo Estadual ou, na sua ausência, a Superintendência de Gestão da Informação (SGI), vinculada à Secretaria de Estado de Fazenda (SEFAZ);

5. DIRETRIZES

A. **Divulgação da Política:** Deve ser assegurado pelo Governo do Estado de Mato Grosso do Sul que esta Política e suas normas complementares estejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com o governo e que, direta ou indiretamente, são impactados. Todavia, deve ser esclarecido que é responsabilidade de cada colaborador a consulta esporádica e voluntária para identificar possíveis atualizações dos documentos.

B. **Autorização de uso:** esta Política e suas normas complementares devem ser interpretadas de forma restritiva, dentro do princípio de aplicação do **menor privilégio possível**, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades. Ou seja, tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

C. **Manuseio das informações:** As informações da instituição, dos clientes e do público em geral, geradas, acessadas, manuseadas, armazenadas ou descartadas por um colaborador no exercício de suas atividades, bem como os Recursos de Tecnologia da Informação (RTI) disponibilizados, são de propriedade e direito de uso exclusivo do Governo do Estado de Mato Grosso do Sul e devem ser empregadas unicamente para fins profissionais, limitado às atribuições de cargo e/ou função desempenhadas pelo colaborador, que deve cumpri-las dentro do padrão de conduta ética estabelecida pelo Governo do Estado de Mato Grosso do Sul e em observância a sua obrigação legal de sigilo profissional.

D. **Gestão da Informação:** A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada. A gestão da informação deve ser assegurada por meio de medidas efetivas que proporcionem acesso e divulgação devidamente autorizados e de acordo com a legislação vigente.

E. **Controle de Acesso:** As secretarias do Governo do Estado de Mato Grosso do Sul devem controlar o acesso físico e lógico, às suas dependências e aos seus RTI's. Desse modo, a empresa deve garantir que cada colaborador possua uma credencial de uso individual, intransferível, de conhecimento exclusivo e qualificando-o

como responsável pelas ações realizadas. Todos os órgãos devem orientar seus colaboradores sobre a responsabilidade quanto ao uso e sigilo além de coibir o compartilhamento de credenciais (Crachás, Login e Senha), sob qualquer hipótese.

F. **Monitoramento:** Cada órgão deve comunicar os seus colaboradores sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, seus RTI's, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados, proteção de seu patrimônio e reputação, rastreando eventos críticos e evidenciando possíveis incidentes. O Correio Eletrônico e o acesso à Internet são recursos corporativos, instalados e mantidos para o atendimento dos objetivos de negócios do Governo. Os acessos e históricos são gravados e passíveis de monitoração, portanto, não há expectativas de privacidade em sua utilização.

G. **Incidentes de Segurança:** Os incidentes de Segurança da Informação devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades da instituição. O Governo do Estado de Mato Grosso do Sul deve divulgar aos seus colaboradores para reportar imediatamente os casos de incidentes de segurança da informação, podendo fazer de modo formal ou com uso do recurso de denúncia anônima. A mera tentativa de burlar às diretrizes e controles estabelecidos pelo Governo do Estado de Mato Grosso do Sul, quando constatada, deve ser tratada como uma violação.

H. **Termos/Contratos:** O contrato com os colaboradores, funcionários, estagiários e prestadores de serviços deve prever sua adesão aos termos e condições desta Política de Segurança da Informação, precedido por um Termo de Confidencialidade, Responsabilidade e Sigilo **(NSI 01 – Termo Confidencialidade, Responsabilidade e Sigilo)** que tratem da Segurança da Informação, relacionado com o escopo de sua contratação e também sanções administrativas ou pecuniárias em caso de sua violação. O Governo do Estado de Mato Grosso do Sul deve prover auditorias periódicas que visam certificar o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

I. **Violação:** As ocorrências que podem ser consideradas violações desta Política de Segurança da Informação devem ser avaliadas pela UTIC (Unidade de Tecnologia da Informação e Comunicação e, constatado como um incidente (v. item 4), encaminhadas para a área de Recursos Humanos, responsável para que as medidas cabíveis sejam aplicadas. As medidas disciplinares estão listadas no tópico **VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇOES**.

6. DEFINIÇÕES

6.1 Atribuições e Responsabilidades

Cabe aos listados no tópico **ABRANGÊNCIA** deste documento:

- Cumprir fielmente a Política de Segurança da Informação;
- Buscar orientações com a UTIC (Unidade de Tecnologia da Informação e Comunicação) em caso de dúvidas relacionadas à Segurança da Informação;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Governo do Estado de Mato Grosso do Sul;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à UTIC (Unidade de Tecnologia da Informação e Comunicação) quanto ao descumprimento ou violação desta Política.

Cabe à Unidade de Tecnologia da Informação e Comunicação (UTIC):

- Gerenciar o cumprimento desta Política;
- Assegurar que todos aqueles listados no tópico **ABRANGÊNCIA** deste documento possuam acesso e conhecimento desta Política de Segurança da Informação;
- Se disponibilizar para recebimento de dúvidas e comunicados em eventuais casos de suspeita de violação de Segurança da Informação em quaisquer níveis;
- Propor ajustes, melhorias, aprimoramentos e modificações desta Política;
- Convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política;
- Prover todas as informações de gestão de Segurança da Informação solicitadas por todos os níveis do órgão/fundação/autarquia;
- Proporcionar atividades de conscientização acerca do tema;
- A gestão e atualização desta Política, conforme definido no tópico **VIGÊNCIA E VALIDADE** neste documento. As atualizações devem ser aprovadas pela UGSI (Unidade de Gestão de Segurança da Informação/SEFAZ/SGI) e pelo CETI (Comitê Estratégico de TI).

Para todo caso que houver necessidade de acionar um responsável para aprovações, deve-se considerar o gestor imediato do solicitante. Sempre que o gestor imediato deste solicitante não puder esclarecer as dúvidas ou aprovar a solicitação, deve-se acionar os Diretores do órgão, considerados os responsáveis máximos de aprovação para todos os funcionários da empresa.

6.2 Ativos de Informação

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por meios offline ou por meios eletrônicos, apresentada em vídeo ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é

compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. ”

A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio. A Segurança da Informação é aqui caracterizada pela preservação da Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade.

Para assegurar esses itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda intencional ou não, acidentes e outras ameaças. É fundamental para a proteção e salvaguarda das informações que os usuários adotem comportamento consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações. Campanhas contínuas serão utilizadas por parte do Governo do Estado de Mato Grosso do Sul para conscientização dos funcionários e para evitar riscos e ocorrência de problemas relacionados à Segurança da Informação.

Assim, para efeitos desta Política de Segurança da Informação, são considerados os seguintes **Ativos de Informação**:

A. Recursos de Tecnologia da Informação;
B. Informações pertencentes ou relacionadas aos associados;
C. Informações relacionadas aos colaboradores do Governo do Estado de Mato Grosso do Sul;
D. Estratégias e decisões da alta administração;
E. Informações contábeis do Governo do Estado de Mato Grosso do Sul;
F. Processos internos do Governo do Estado de Mato Grosso do Sul;

Marcas, logotipos e nomes relacionados aos negócios conduzidos pelo Governo do Estado de Mato Grosso do Sul.

6.3 Análise dos Recursos de Tecnologia da Informação (RTI’s)

Cada órgão deve analisar, em intervalos regulares, seus processos e RTI’s, assegurando que estes estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

A. **Ambientes Lógicos:** Deve ser assegurado pelo Governo do Estado de Mato Grosso do Sul que os ambientes de seus sistemas e processos que suportam os RTI’s, tais como data center, salas de TI onde abrigam servidores de dados, sejam confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.

B. **Ambientes Físicos:** Devem possuir controle de acesso nos perímetros de segurança delimitados para garantir a proteção das áreas, bem como controles e registros apropriados para assegurar o acesso somente aos colaboradores autorizados e aos RTI’s homologados. Tais controles são feitos através de biometria, crachás e câmeras de segurança.

6.4 Classificação da Informação

É de responsabilidade do Governo do Estado de Mato Grosso do Sul estabelecer critérios relativos ao nível de confidencialidade de todas as informações geradas na organização, de acordo com as classificações listadas a seguir:

- **Pública:** É uma informação do Governo do Estado de Mato Grosso do Sul ou de seus clientes ou parceiros com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É um tipo de informação que pode ser consumida pelo público externo sem quaisquer tipos de restrições;
- **Interna:** É uma informação do Governo do Estado de Mato Grosso do Sul que a organização não tenha interesse em divulgar, cujo acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem do Governo. Pode ser acessada sem restrições por todos aqueles listados no tópico ABRANGÊNCIA deste documento;
- **Restrita:** É uma informação do Governo do Estado de Mato Grosso do Sul que pode ser acessada somente pelos grupos de usuários previamente cadastrados ao se classificar a informação. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

É de responsabilidade de todos aqueles listados no tópico ABRANGÊNCIA realizar a classificação da informação, de acordo com a análise do material recebido.

Todas as informações devem estar contidas no repositório oficial de arquivos, quando criadas, editadas ou divulgadas. Estas informações devem sempre estar classificadas de acordo com a confidencialidade. Essa classificação deve ser feita sempre que um arquivo é carregado ou criado no ambiente da empresa. Todos os arquivos disponíveis nas ferramentas disponibilizadas pelo Governo deverão ter a classificação de confidencialidade definida.

6.5 Controle de Acessos

O Governo do Estado de Mato Grosso do Sul por meio da UTIC (Unidade de Tecnologia da Informação e Comunicação) deve controlar e registrar os **acessos físicos e lógicos** às suas dependências e aos seus RTI’s. Desse modo, a organização deve garantir que cada colaborador possua uma credencial de uso pessoal, intransferível e de conhecimento exclusivo. Os acessos físicos aos ambientes controlados e lógicos às informações

e recursos computacionais devem ser autorizados pelos gestores ou líder imediato. A formalização do processo de Controle de Acessos é tratada na norma complementar **(NSI 02 – Controle de Acessos).**

Além disso, a política de Controle de Acesos também referência a Política de Uso da VPN **(NSI 03 – Uso da VPN)**.

6.6 Continuidade do Negócio e Contingência dos RTI's

A **Norma de Segurança de Continuidade de Negócio (NSI 04)** contém as diretrizes que devem orientar os processos e planejamento estratégico do Governo do Estado de Mato Grosso do Sul na disponibilidade e continuidade das suas operações críticas.

Visando mitigar os riscos de interrupção causados por incidentes de segurança e manter os níveis de serviços de TI adequados ao negócio do Governo do Estado de Mato Grosso do Sul, através da combinação de ações de prevenção e recuperação, as diretrizes desta Política de Segurança da Informação devem estar alinhadas com o direcionamento da Norma de Segurança de Continuidade de Negócios.

6.7 Proteção e Privacidade dos Dados Pessoais

Os dados pessoais coletados pelo Governo do Estado de Mato Grosso do Sul devem ser tratados somente para fins autorizados, de forma ética e legal, respeitando os direitos do Titulares dos dados e em conformidade com a Lei Geral de Proteção de Dados (LGPD). Todo tratamento de Dados Pessoais deve possuir uma finalidade de tratamento e estar fundamentado em uma das bases legais previstas na LGPD, seguindo um ciclo de vida da coleta, do uso e da exclusão dos Dados Pessoais.

O governo do Estado de Mato Grosso do Sul conta com um comitê para implementação de diretrizes e plano de adequação à LGPD e encarregados em cada um dos órgãos. Foi elaborado pelo comitê uma **Cartilha LGPD** para conscientizar e orientar os colaboradores acerca do tema. Este material e demais informações está disponível no Portal LGPD – www.lgpd.ms.gov.br.

6.8 Descarte de Informações

As informações relativas a dados pessoais somente devem ser retidas pelo tempo necessário para cumprir as finalidades para as quais foram coletadas, sendo possível mantê-las também para atender a quaisquer requisitos legais, contratuais, de prestação de contas, requisição de autoridades competentes, contábeis ou de relatórios. O titular dos dados pessoais pode solicitar a qualquer momento a exclusão de seus dados.

O governo deve estipular um prazo de armazenamento para os dados coletados, levando sempre em consideração a finalidade e o motivo desse armazenamento. É recomendado que as informações em mídias físicas sejam mantidas em um período de até 5 anos ou até que não tenham mais uso. Assim que o período expirar, e desde que não haja uma razão válida ou base legal para que os Dados Pessoais sejam mantidos em cópia física, as mídias físicas serão destruídas como resíduo confidencial.

O governo e seus colaboradores devem regularmente rever todos os dados, sejam eles mantidos de forma física ou digital, para decidir eliminar ou excluir quaisquer dados, uma vez que as finalidades deles já foram atingidas.

O descarte de informações deve ser efetuado quando essas não forem mais necessárias, devendo ser realizado através de procedimentos formais que impossibilitem sua reconstrução, seja a informação física ou digital. A informação deve ser descartada de modo que proteja os direitos e liberdades dos titulares de dados pessoais e considerando prazos mínimos legais ou regulatórios, bem como sua necessidade para o seu projeto ou área, o que for maior. O descarte de informações da empresa deve sempre seguir as orientações das legislações vigentes, considerando prazos mínimos legais ou regulatórios, seguindo as regras descritas no tópico de **ATRIBUÇÕES E RESPONSABILIDADES**.

A UTIC (Unidade de Tecnologia da Informação e Comunicação) se coloca à disposição para orientar todos aqueles listados no tópico **ABRANGÊNCIA** deste documento sobre o armazenamento e descarte de documentos que contenham informações internas, que em teoria não podem ser armazenados ou descartados em locais que comprometam a segurança da organização.

6.9 Ferramentas da Comunicação Social

Os softwares oficiais para comunicação interna por mensagens, chamadas ou vídeo chamadas de assuntos corporativos do Governo do Estado de Mato Grosso do Sul são o MatterMost (chat.sgi.ms.gov.br), para comunicação interna e externa, e o Pandion (ejabberd), para comunicação interna. Quando solicitado por clientes ou parceiros, a utilização de outros programas deve ser consultada e aprovada pelo gestor imediato e solicitada para a UTIC para análise de viabilidade técnica e impacto da mesma no ambiente de trabalho.

6.10 Propriedade Intelectual

Os dados e informações criados nos recursos computacionais dos ativos corporativos do Governo do Estado de Mato Grosso do Sul são de sua propriedade e devem ser utilizados somente por aqueles listados no tópico **ABRANGÊNCIA** neste documento, exclusivamente, no exercício de suas atividades junto ao governo. Caso estes dados e informações sejam criados em favor de um cliente comercial do Governo do Estado de Mato Grosso do Sul, este cliente também tem direito ao acesso e posse destes materiais.

Os *softwares* adquiridos no mercado ou desenvolvidos internamente pertencem exclusivamente ao Governo do Estado de Mato Grosso do Sul, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas, elaboradas e/ou desenvolvidas por aqueles listados no tópico **ABRANGÊNCIA**, durante a vigência da relação de emprego ou contrato.

Quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações

tecnológicas e segredos comerciais pertencentes ao Governo do Estado de Mato Grosso do Sul, é vedada a cópia ou disponibilização através de qualquer meio (eletrônico ou físico) para ambiente externo ao Governo do Estado de Mato Grosso do Sul que não tenham sido previamente autorizados.

6.11 Segurança de Dispositivos Móveis

Cabe aos listados no tópico **ABRANGÊNCIA** deste documento:

- Cuidar dos equipamentos de computação móvel aos quais tenha sido designado;
- Não disponibilizar, emprestar ou ceder seu equipamento para uso de terceiros, nem permitir que pessoas às quais o equipamento não tenha sido designado utilizem-no;
- Não armazenar informações sensíveis, confidenciais, de valor comercial ou que contenham dados pessoais de clientes ou colaboradores (tanto internos, quanto terceiros) do Governo do Estado de Mato Grosso do Sul em locais não definidos previamente pelo Governo. Exceções devem ser autorizadas;
- Nunca anotar, escrever e/ou emitir senhas de forma que elas possam ser encontradas fisicamente. Certificar-se de que não há senhas para o acesso ao seu dispositivo móvel escritos e/ou armazenados em qualquer lugar.

Cabe **à UTIC (Unidade de Tecnologia da Informação e Comunicação):**

- Garantir a proteção dos equipamentos de computação móvel aos quais tenha sido designado, bem como de todas as informações armazenadas neles.

Cada usuário deve estar ciente que o uso de qualquer recurso de TI no ambiente do Governo do Estado de Mato Grosso do Sul, ainda que de propriedade pessoal, está sujeito a vistoria, sempre que a lei local permitir.

Todos os dispositivos devem ser mantidos em segurança pelo membro responsável por sua utilização e manuseio. Quando não assistidos, os dispositivos devem ser mantidos em uma área bloqueada (por exemplo, uma sala ou armário trancado) com acesso controlado e restrito, disponível apenas para pessoas previamente autorizadas pelo gestor.

Dispositivos portáteis, como laptops ou tablets, são itens altamente vulneráveis e sujeitos a roubo. Logo, estes equipamentos não devem ser deixados sem assistência em locais como veículos e espaços abertos.

6.12 Acesso à Internet

Todas as informações, dados e demais materiais cujos conteúdos estão listados nas categorias a seguir estão permanentemente proibidos na REIT (Rede Estadual de Informática e Telecomunicações) do Governo do Estado de Mato Grosso do Sul:

- Sítios de hospedagem gratuita;
- Fóruns e Grupos de discussão;
- Blogs e Fotoblogs;
- Jogos on-line;
- Sítios com salas de bate-papo (chats);
- Grupos virtuais;
- Conteúdos de *streams* em geral (áudio e vídeo);
- Comunicadores instantâneos;
- Sítios de proxies e tunelamento de conexões
- Sítios com conteúdo pornográfico, adulto, hackerismo, pedofilia, discriminação de qualquer gênero, publicidade online, violência, drogas, agressivos.

Todas as informações, dados e demais materiais cujos conteúdos estão listados nas categorias a seguir estão permitidos dentro da REIT do Estado:

- Todos os sítios .gov.br, .jus.br, .edu.br;
- Sítios de bancos;
- Sítios de instituições de ensino;
- Sítios de notícias, esportes, jornais, e demais conteúdos que não apresentem os conteúdos listados como não permitidos.

Todas as informações, dados e demais materiais cujos conteúdos estão listados nas categorias a seguir podem ser solicitas dentro da REIT, mediante solicitação formal do gestor ou chefe imediato, justificando a necessidade do acesso para cumprir as demandas das atividades profissionais.

- Redes sociais;
- Conteúdos de *streams* (YouTube, Vimeo) (áudio e vídeo);
- Sítios para Videoconferência;

Estas regras devem ser seguidas por todos citados no tópico deste documento ABRANGÊNCIA, inclusive fora do horário de expediente.

Para realizar a solicitação de libertação de conteúdo, é necessário realizar o pedido através de Ofício (e-Doc), aos cuidados do Superintende da SGI, informando a necessidade do acesso e a justificativa para liberação do mesmo. Após o envio, o pedido será analisado pela UTIC para avaliar a possibilidade de liberação e o impacto do mesmo na rede do Estado.

6.13 Política de Backup

A **Política de Backup e Restauração (NSI 05)** contém as diretrizes que devem orientar os processos de backup e restauração de informações do Governo do Estado de Mato Grosso do Sul para a proteção e disponibilidade

das informações pertencentes à organização.

7. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta Política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

O infrator poderá ser notificado e a ocorrência da transgressão será imediatamente comunicada ao seu gestor imediato, que deverá repassar ao setor de Recursos Humanos, a fim de tomarem as medidas necessárias e encaminhamento para processo administrativo disciplinar, conforme Estatuto dos Funcionários Públicos Civis do Poder Executivo, das Autarquias e das Fundações Públicas do Estado de Mato Grosso do Sul (Lei nº 1.102).

O Governo do Estado de Mato Grosso do Sul poderá utilizar-se das seguintes medidas disciplinares:

- Advertência verbal, com respectivo aconselhamento ou reeducação/treinamento;
- Advertência por escrito;
- Encaminhamento para abertura de processo administrativo disciplinar para apurar a gravidade e eventuais danos;

As ações/medidas disciplinares relacionadas acima não são necessariamente sequenciais, podendo ser aplicadas gradualmente, isoladamente ou em conjunto, dependendo da gravidade, intenção e reincidência da infração. Devem ser aplicadas com clareza e transparência, assegurando-se ao funcionário a ciência da situação disciplinar e da necessidade de corrigir comportamento e conduta.

As etapas abaixo devem ser seguidas ao tomar decisões que impliquem em aplicação de medidas disciplinares, visando assegurar tratamento justo a todas as pessoas em relação ao seu comportamento e conduta.

- Considerar os fatos conhecidos em relação à infração específica;
- Consultar todas as políticas, procedimentos ou requisitos existentes;
- Verificar se existem informações comparativas disponíveis, protegendo a confidencialidade das pessoas envolvidas;
- Atentar-se somente aos fatos relevantes e não identificar as pessoas envolvidas em qualquer medida disciplinar anterior;
- Levar em conta os fatos existentes e as medidas disciplinares impostas em casos anteriores que envolvam um tipo semelhante de infração;
- Considerar com atenção todos os fatores de agravamento/mitigação;
- Considerar histórico do funcionário.

8. VIGÊNCIA E VALIDADE DO DOCUMENTO

A presente Política passa a vigorar a partir da data de aprovação da versão atual, sendo válida por tempo indeterminado.

O Governo do Estado de Mato Grosso do Sul deve possuir e manter um programa de **revisão/atualização** visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente. A UTIC deve incluir em seu planejamento de trabalho anual as revisões dos controles internos que visam à garantia dos níveis aceitáveis de segurança da informação.

Deve ser realizada uma revisão da Política pela UGSI/SEFAZ/SGI (Unidade de Gestão da Segurança da Informação) com periodicidade máxima de 06 meses, podendo ocorrer em intervalos menores, quando necessário. Toda alteração deve estar prevista no Plano de Ação da Segurança da Informação e ser comunicada a todos aqueles listados no tópico **ABRANGÊNCIA**, após aprovação do CETI.

9. ALINHAMENTO COM NORMAS, ÓRGÃOS REGULADORES E LEGISLAÇÕES

- **ABNT NBR ISO/IEC 27001:2013** – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos;
- **ABNT NBR ISO/IEC 27002:2013** – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação.

ANEXO II À DELIBERAÇÃO/CETI Nº 02, DE 24 DE FEVEREIRO DE 2022

GOVERNO DO ESTADO DE MATO GROSSO DO SUL
CONSELHO DE GOVERNANÇA DE MATO GROSSO DO SUL
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

Termo de Confidencialidade, Responsabilidade e Sigilo.

Nome do colaborador/Prestador de serviço		**RG/CPF**
Unidade Organizacional	**Data**	**Telefone**

COMPROMISSO LEGAL:

Declaro ter conhecimento, estar de pleno acordo e comprometo-me a respeitar as regras consubstanciadas nas políticas e procedimentos do Governo do Estado de Mato Grosso do Sul, descritos na Política de Segurança da Informação e demais Instrumentos Normativos Internos correlatos, dedicando especial cuidado aos seguintes aspectos:

1. Não violar a Política, Normas e Procedimentos de Segurança da Informação;
2. Utilizar de forma adequada e correta os equipamentos de informática, sistemas e telefonia e instalações que forem disponibilizados pelo Governo do Estado de Mato Grosso do Sul, bem como os programas e acessos à rede local, Internet, Correio Eletrônico e aplicativos de negócios;
3. Não divulgar ou facilitar o uso de minha senha pessoal de acesso à rede de computadores do Governo e aos sistemas de aplicativos de negócios;
4. Utilizar o Telefone, Correio Eletrônico e os recursos de informática exclusivamente para fins profissionais em atividades do Governo do Estado de Mato Grosso do Sul;
5. Observar os cuidados a serem adotados conforme a classificação da informação, utilizando as informações disponibilizadas pelo Governo do Estado somente nas atividades a que compete exercer, não podendo transferi-las a terceiros, seja a título oneroso ou gratuito, estando ciente de que suas ações ou consultas poderão ser monitoradas e acompanhadas;
6. Adotar as medidas preventivas disponibilizadas pela UTIC (Unidade de Tecnologia da Informação e Comunicação) contra ameaças digitais, tais como "vírus", "cavalo de troia" e outros acessos indevidos a rede de computadores;
7. Observar os cuidados a serem adotados conforme a classificação da informação, sempre que for necessário transportar documentos, equipamentos ou mídias eletrônicas pertencentes ao Governo do Estado de Mato Grosso do Sul;
8. Comunicar imediatamente ao superior hierárquico e à UTIC (Unidade de Tecnologia da Informação e Comunicação) quaisquer atos relacionados ao uso de bens da informação do qual venho a ter conhecimento, inclusive nos casos de violação não intencional ou culposa, e que possam causar prejuízos ou danos de qualquer natureza;

DECLARAÇÃO DE COMPROMISSO E AUTORIZAÇÃO:

Autorizo o Governo do Estado de Mato Grosso do Sul a monitorar qualquer item da arquitetura tecnológica do Governo e a tomar as devidas providências, caso constate uso indevido.

O presente termo vigorará por tempo indeterminado, ou seja, permanecerá válido mesmo após o meu desligamento do quadro funcional do Governo do Estado de Mato Grosso do Sul, podendo ser utilizado caso qualquer termo de compromisso aqui assumido seja quebrado por algum motivo.

Para tanto, assino o presente Termo de Confidencialidade, Responsabilidade e Sigilo, declarando-me ciente de que a displicência ou descumprimento de qualquer uma das referidas normas poderá acarretar punições disciplinares, além das obrigações de ressarcir o Governo do Estado de Mato Grosso do Sul dos eventuais prejuízos decorrentes das falhas ou omissões por mim cometidas.

Cidade, _____de _____ de _____.

_____
Nome do Colaborador

ANEXO III À DELIBERAÇÃO/CETI Nº 02, DE 24 DE FEVEREIRO DE 2022

GOVERNO DO ESTADO DE MATO GROSSO DO SUL
CONSELHO DE GOVERNANÇA DE MATO GROSSO DO SUL
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

Política de Controle de Acesso

1. OBJETIVO

A Política de Controle de Acesso é uma declaração formal do Governo do Estado de Mato Grosso do Sul acerca de seu compromisso com a proteção dos ativos de informação de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários.

O documento em questão tem como objetivo limitar e assegurar o acesso à informação e aos recursos de processamento da informação, prevenindo o acesso não autorizado a sistemas, serviços e ambientes físicos.

2. ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores, prestadores de serviços, usuários internos e externos e quaisquer pessoas que tenham acesso as informações pertencentes ou custodiadas pelo Governo do Estado de Mato Grosso do Sul.

3. REFERÊNCIA

Este documento foi elaborado com base nas recomendações propostas pela norma **ABNT NBR ISO/IEC 27002:2013**, reconhecida mundialmente como um código de prática para a gestão da segurança da informação,

bem como está de acordo com as leis brasileiras vigentes, e com base na Norma **ISO/IEC 27001**, cláusulas A.9.1, A.9.2, A.9.3 e A.9.4.

4. RISCOS

A divulgação e acesso não autorizado às informações providas pelo Governo do Estado de Mato Grosso do Sul, pode comprometer a segurança do negócio como um todo, ocasionando perdas financeiras e incapacitando a organização de fornecer seus serviços necessários ao cliente final. Esta política destina-se a mitigar esse risco.

O não cumprimento desta política pode ter um efeito significativo no funcionamento eficiente da organização, sendo, portanto, da obrigação de todos os listados no tópico **ABRANGÊNCIA** deste documento, seguir as políticas aqui mencionadas.

5. CONTROLE DE ACESSO

· **Concessão de acesso**

O acesso será concedido utilizando o princípio de privilégios mínimos. Isso significa que cada programa e cada usuário do sistema deve operar usando o menor conjunto de privilégios necessários para concluir o trabalho.

· **Identificação do usuário**

Cada usuário deve estar devidamente identificado por um cadastro único e intrasferível, possibilitando que seja vinculado e responsabilizado por seus atos dentro da organização. A utilização de identidades de grupo só será permitida quando previamente autorizada, por exemplo, contas de treinamento.

Registros de acesso do usuário podem ser utilizados como fornecedores de evidências em caso de incidentes relacionados à segurança da informação.

· **Responsabilidades do usuário**

- Cabe ao usuário assegurar que seu ID e senha não sejam utilizados por terceiros, impedindo que estes sejam utilizados para a obtenção de acesso não autorizado aos sistemas do Governo do Estado de Mato Grosso do Sul;
- Garantir que os dispositivos de sua responsabilidade estejam devidamente bloqueados durante sua ausência;
- Não deixar amostra informações que possibilitem o acesso de terceiros, como login e senha.

· **Acesso físico**

Para que de fato somente pessoas autorizadas tenham acesso físico às áreas seguras, são importantes controles de autenticação que validem esses acessos, sendo que essa autorização só deve ser concedida a quem realmente necessitar dela para o desempenho de suas funções profissionais. Para fins de auditoria, todo acesso a uma área segura deve ser sempre registrado. Para não funcionários o registro deve conter ainda a data, hora de entrada e saída, o motivo do acesso e a pessoa que deu a autorização. E é importante que todos que circulem por áreas seguras possuam alguma forma visível de identificação, incluindo os visitantes, que precisam ser monitorados.

Além disso, cada pessoa deve ter acesso somente a um número limitado de áreas seguras e os direitos de acesso precisam ser revisados regularmente. Pessoas de fora da organização só podem estar presentes nesses locais com algum tipo de autorização e objetivos muito específicos.

· **Acesso a redes**

Qualquer dispositivo não pertencente e previamente autorizado pelo Governo do Estado de Mato Grosso do Sul, quando conectados à rede da organização, pode comprometer e trazer danos à segurança da rede. A fim de mitigar este risco deve-se obter uma autorização específica com a UTIC (Unidade de Tecnologia da Informação e Comunicação) antes de qualquer conexão à rede.

Conexões remotas: em caso de trabalho remoto e conexão à rede do Governo do Estado de Mato Grosso do Sul de forma remota. A UTIC (Unidade de Tecnologia da Informação e Comunicação) deve autorizar previamente o usuário solicitado e a autenticação deve ser de múltiplos fatores (MFA).

· **Trabalho Remoto**

O trabalho remoto inclui toda e qualquer prestação de serviços exercida fora das dependências da organização, podendo suas atividades serem desempenhadas total ou parcialmente externa.

O trabalho remoto deve ser solicitado através do **formulário de solicitação de regime de teletrabalho** e autorizado pelo gestor responsável ou chefe imediato de seu respectivo departamento por meio de uma autorização formal registrada no Service Desk. O trabalho remoto deve ser executado via VPN, seguindo as orientações definidas na **Política de Uso da VPN (NSI 03 – Uso de VPN)**. Deve ser de conhecimento da TI os colaboradores autorizados a exercerem trabalhos de maneira remota, sendo esta informação atualizada periodicamente.

· **Política de Senhas**

As senhas são o primeiro código de acesso exigido para que usuários frequentem, alterem e obtenham informações da organização. Por motivos de segurança, foram definidos os requisitos de senha de todos os domínios da Floresta MS e deve ser usado para todos os sistemas e acessos do governo do Estado de Mato Grosso do Sul:

- Critérios para a elaboração de uma senha segura:
  - Não conter o nome da conta;
  - Não conter mais de dois caracteres consecutivos de partes do nome completo do usuário;
  - Conter pelo menos oito (08) caracteres;
  - Conter caracteres de três das quatro categorias:
    - Caracteres Maiúsculos (A – Z);
    - Caracteres Minúsculos (a – z);
    - Números (0 a 9);
    - Símbolos (!, $, #, %, &).
  - Ser mais complexo que uma única palavra (palavras e frases usadas como senhas são mais

facilmente descobertas por invasores);
- Tempo de vida máximo da senha é de seis (06) meses;
- Histórico máximo de senha é de oito (08) senhas memorizadas (o usuário não conseguirá repetir as 8 últimas senhas).
- Habilitar sempre que a ferramenta disponibilizar, a Autenticação Multifator (MFA) para reforçar a conta contra ataques de phishing.

- Processos de armazenamento e não divulgação de senhas:
  - Não revelar a senha para terceiros;
  - Não utilizar a função "lembrar senha";
  - Não anotar senhas ou guardá-las em locais possíveis de roubo;
  - Não armazenar senhas em computadores e dispositivos móveis sem criptografia;
  - Não utilizar a mesma senha para acesso em diferentes sistemas;
  - Não utilizar a mesma senha para acessos fora da organização.

· **Acesso por terceiros**

Fornecedores terceirizados não devem receber qualquer acesso à rede do Governo do Estado de Mato Grosso do Sul sem prévia permissão da UTIC (Unidade de Tecnologia da Informação e Comunicação). Qualquer alteração indevida ou acesso sem permissão deve ser informado imediatamente à UTIC (Unidade de Tecnologia da Informação e Comunicação) para que possa ser investigado e, se necessário, interrompido.

Todas as permissões e métodos de acesso devem ser previamente analisados e autorizados pela UTIC.

· **Acesso ao sistema operacional**

O acesso aos sistemas operacionais deve ser controlado por processo de login seguro. O controle de acesso e a política de senhas, mencionados anteriormente, devem ser aplicados. O procedimento de login também deve ser protegido por:

- Limitar o número de tentativas malsucedidas e bloquear a conta, se excedido;
- Os caracteres da senha estão escondidos por símbolos;
- Exibir um aviso geral de que somente usuários autorizados são permitidos.

Todo o acesso a sistemas operacionais é feito por meio de um ID de login exclusivo que será auditado e pode ser rastreado de volta para cada usuário individual. O ID de login não deve fornecer qualquer indicação do nível de acesso que ele fornece ao sistema, como, direitos de administração.

Os administradores do sistema devem ter contas de administrador individuais que serão registradas e auditadas. A conta de administrador não deve ser usada por indivíduos para atividades normais do dia a dia. – Ler os itens concessão de acessos e responsabilidades dos usuários, citados anteriormente.

· **Acesso a aplicativos e informações**

O acesso dentro dos aplicativos de software deve ser restrito usando os recursos de segurança incorporados no produto individual. A UTIC (Unidade de Tecnologia da Informação e Comunicação) é responsável por conceder acesso às informações dentro do sistema. O acesso deve seguir as seguintes especificações:

- Estar em conformidade com as seções: concessão de acesso, identificação do usuário, responsabilidades do usuário e políticas de senha (ver itens anteriores);
- Ser dividido por papéis e responsabilidades previamente definidos;
- Fornecer o nível apropriado de acesso necessário para a função do usuário;
- Não permitir a substituição de funções, por exemplo configurações de administrador removidas ou ocultas ao usuário;
- Estar livre de alterações por direitos herdados do sistema operacional que possam permitir níveis mais altos de acesso não autorizados.

6. DIRETRIZES

· **Dispositivos portáteis:**

- Os dispositivos pessoais não devem conter informações sensíveis, pessoais, confidenciais ou de valor comercial sem qualquer prévia autorização. Notebooks podem ser considerados dispositivos portáteis e, em trabalho remoto, terão dados sensíveis;
- Todos os dispositivos usados para negócios do Governo do Estado de Mato Grosso do Sul devem ter criptografia completa de disco e estar em conformidade com as Políticas de Segurança da Informação seguidas pelo Governo do Estado de Mato Grosso do Sul;
- Todos os dispositivos devem ser mantidos em segurança pelo membro responsável por sua utilização e manuseio. Quando não assistidos, os dispositivos devem ser mantidos em uma área bloqueada (por exemplo, uma sala ou armário trancado) com acesso controlado e restrito, disponível apenas para pessoas previamente autorizadas pelo gestor da informação;
- Dispositivos portáteis, como laptops ou tablets, são itens altamente vulneráveis, sujeitos a roubo. Logo estes equipamentos não devem ser deixados sem assistência em locais como veículos e espaços abertas;
- Certifique-se de que não há senhas para acesso ao seu dispositivo móvel escritos e / ou armazenados com ele.

· **Descarte:**

- Dispositivos de mídia removíveis que não são mais necessários ou que foram danificados devem ser descartados com segurança para evitar vazamento de dados. Qualquer conteúdo anterior de qualquer mídia reutilizável, seja dentro do Governo do Estado de Mato Grosso do Sul ou para uso pessoal, deve ser apagado, sendo feita uma remoção completa de todos

os dados da mídia para evitar possíveis vazamentos de informações usando ferramentas e software especializados;
- Todos os dispositivos de mídia removível que não forem mais necessários, ou que foram danificados, devem ser devolvidos ao departamento de TI para descarte seguro.

· **Responsabilidades do Usuário:**
- Qualquer dispositivo de mídia removível usado em conexão com o equipamento do Governo do Estado de Mato Grosso do Sul ou a rede ou que contenha informações usadas para conduzir negócios oficiais do Governo do Estado de Mato Grosso do Sul deve ser adquirido e instalado somente pelo departamento de TI. Qualquer dispositivo de mídia removível que não tenha sido fornecido ou autorizado pela TI não deve ser usado;
- O software de verificação de vírus e malware deve ser usado quando o dispositivo de mídia removível estiver conectado a uma máquina;
- Somente os dados autorizados e necessários para serem transferidos devem ser salvos no dispositivo de mídia removível. Os dados que foram excluídos ainda podem ser recuperados;
- Os dispositivos de mídia removível não devem ser usados para arquivar ou armazenar registros como uma alternativa a outro equipamento de armazenamento;
- Cuidados especiais devem ser tomados para proteger fisicamente o dispositivo de mídia removível e os dados armazenados contra perda, roubo ou danos. Qualquer pessoa que use dispositivos de mídia removível para transferir dados deve considerar a maneira mais adequada de transportar o dispositivo e demonstrar que foi tomado o cuidado necessário para evitar danos ou perdas;
- Para obter conselhos ou assistência sobre como usar com segurança dispositivos de mídia removível, entre em contato com a UTIC.

7. CONFORMIDADE
- Se algum usuário violar esta política, ele poderá estar sujeito à procedimentos disciplinares do Governo do Estado de Mato Grosso do Sul. Se uma infração penal for considerada como tendo sido cometida, podem ser tomadas outras medidas para ajudar na acusação do infrator(s);
- Em caso de dúvidas quanto as implicações desta política ou como ela pode se aplicar a você, procure a UTIC (Unidade de Tecnologia da Informação e Comunicação) do Governo do Estado de Mato Grosso do Sul.

ANEXO IV À DELIBERAÇÃO/CETI Nº 02, DE 24 DE FEVEREIRO DE 2022

GOVERNO DO ESTADO DE MATO GROSSO DO SUL
CONSELHO DE GOVERNANÇA DE MATO GROSSO DO SUL
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

Política de Uso da VPN

1. OBJETIVO

A Política de Uso da VPN tem como objetivo prover as diretrizes gerais para o uso apropriado de conexões VPN, para acesso à rede computacional do Governo do Estado de Mato Grosso do Sul (REIT), visando o bom desempenho do serviço e a segurança da informação no que tange aos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

2. ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores, prestadores de serviços, usuários internos e externos e quaisquer pessoas que estejam devidamente autorizados pela chefia a utilizarem o(s) recurso(s) de acesso remoto.

3. DEFINIÇÕES E FUNÇÕES

· **VPN (Virtual Private Network):** Rede privada virtual que permite ao usuário receber um número IP da Rede Estadual de Informática do Governo em seu equipamento remoto. O acesso via VPN utiliza encriptação de dados para a comunicação entre o equipamento remoto e a rede local do Governo. Por meio da VPN, usuários cadastrados podem acessar sua estação de trabalho e/ou sistema(s) previamente autorizado(s) através dela, acessar todos os locais que já possui autorização para realização do trabalho, da mesma forma que seria feito presencialmente à partir do computador remoto;

· **REIT (Rede Estadual de Informática e Telecomunicações):** Rede de dados computacional do Governo do Estado de Mato Grosso do Sul;

· **UTIC (Unidade de Tecnologia da Informação e Comunicação):** Departamento responsável pela gestão de Tecnologia da Informação e Comunicação e pelo planejamento, coordenação e acompanhamento das ações relacionadas às soluções de TIC da unidade, do órgão, da autarquia ou da fundação do Poder Executivo Estadual ou, na sua ausência, a Superintendência de Gestão da Informação (SGI), vinculada à Secretaria de Estado de Fazenda (SEFAZ);

· **Acessos via VPN:** A conexão via VPN ao ambiente de trabalho no Estado é provido pela Unidade de Tecnologia da Informação e Comunicação (UTIC), por meio de uma conta de usuário e senha utilizados para acesso e trabalho na rede do Governo. Os usuários autorizados a usar a VPN são servidores e colaboradores terceirizados que desempenham suas funções na forma de trabalho remoto, devidamente autorizados pelo chefe imediato;

- **Integridade:** Garantia de que a informação esteja completa, exata e íntegra e que seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Confidencialidade:** Garantia de que o acesso à informação estará disponível ou será divulgada somente a indivíduos, entidades ou aplicativos autorizados;
- **Disponibilidade:** Garantia de que os usuários autorizados tenham acesso à informação quando necessário;
- **Autenticidade:** Garantia da identidade do remetente da informação. Pela autenticidade, garante-se que a informação é proveniente da fonte anunciada, sem sofrer alteração durante o envio;
- **Legalidade:** Garantia de que o uso e manuseio das informações sigam as leis vigentes no país.

4. POLÍTICA

Compete aos usuários com privilégios de acesso à rede local do Governo via VPN:

- Garantir a veracidade e exatidão dos dados pessoais fornecidos para o cadastro;
- Ser responsável pelo seu acesso à Internet, pelo equipamento a ser utilizado e por qualquer instalação de software necessário ou ainda, por qualquer valor associado ao uso da VPN;
- Assegurar que seu login de acesso é de uso único e exclusivo, não podendo em hipótese alguma ser repassado para outras pessoas ou compartilhado;
- Todos os computadores conectados à rede interna do Governo via VPN devem estar com as versões atualizadas do sistema operacional, do software antivírus, e com os últimos "patches" de segurança instalados através do Windows Update ou programa similar em seu sistema operacional;
- Estabelecer somente uma única conexão VPN com a rede do Estado;
- Acessar a infraestrutura do Governo somente por necessidade de serviço, realizando as tarefas e operações, em estrita observância aos procedimentos aqui elencados;
- Ter concordado com as "NORMAS DE USO" desta "Política de Uso da VPN";
- Utilizar equipamentos com sistemas operacionais compatíveis com a infraestrutura;
- Não alterar, sem prévio consentimento, a configuração da VPN fornecida pela Unidade de Tecnologia da Informação e Comunicação;
- Entender e aceitar que os equipamentos pessoais para acesso à VPN passam a ser uma extensão da rede do Estado e como tal, estão sujeitas às mesmas regras, políticas e regulamentações que se aplicam aos equipamentos de propriedade do Governo, ou seja, as máquinas devem ser configuradas para atender às normas da instituição para execução do trabalho;
- Não utilizar o acesso VPN para transferência de grandes volumes de dados, exceto se as informações forem estritamente necessárias ao desenvolvimento do trabalho;
- Não utilizar programas "peer-to-peer" sobre VPN;
- Manter a máxima cautela necessária quando da exibição de dados em tela, impressora ou em gravação em meios eletrônicos, como pen drive, e-mail etc., a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;
- Não é permitido copiar e armazenar arquivos e informações de trabalho da rede do Governo em seu computador pessoal;
- Não se ausentar da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;
- Declaro, ainda, estar plenamente esclarecido e consciente que:
    - É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade dos dados, informações contidas nos sistemas, e da infraestrutura de tecnologia da informação a que tenha acesso, devendo comunicar por escrito à minha Chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas e na infraestrutura de tecnologia da informação, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;
    - Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos dos sistemas de informação e na infraestrutura de tecnologia da informação, aos quais tenha acesso, para outros servidores não envolvidos nos trabalhos executados;
    - Devo alterar minha senha sempre que for solicitado pela equipe da Unidade de Tecnologia da Informação e Comunicação ou que tenha suspeita de descoberta por terceiros, e não usar combinações simples que possam ser facilmente descobertas;
    - Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na rede do Governo (tais como privilégio e direitos de acesso);
    - Observar e Cumprir as Boas Práticas de Segurança da Informação, e suas diretrizes, bem como esta política de acesso.

Compete **à UTIC (Unidade de Tecnologia da Informação e Comunicação)**:

- Liberar o tráfego de dados entre a estação de trabalho remota do usuário e sua estação de trabalho em uma única conexão (túnel VPN). Qualquer outro tráfego fora da VPN será descartado;
- Conceder em casos excepcionais, permissão à rede de bancos de dados por meio da VPN, mediante justificativa formal da necessidade e com a autorização expressa do gestor da área ou chefe imediato;
    - A permissão de acesso à rede de banco de dados não garante o acesso às bases de dados.
- Monitorar o volume de dados das conexões VPN e desconectar qualquer sessão onde se verifique taxas divergentes da média normal das outras sessões que comprometam ao bom desempenho da

rede local;
- Auditar, quando necessário e com autorização, os sistemas utilizados e a comunicação de dados para acesso, por meio de VPN, a fim de verificar a aderência aos requerimentos de segurança aqui mencionados;
- A UTIC poderá por motivos de segurança e/ou outros, suspender o serviço de VPN, sem aviso prévio, quando entender que o acesso está dificultando o trabalho dos demais colegas ou colocando a rede em risco;
- A autorização para utilização do serviço de VPN tem validade enquanto o usuário mantiver o vínculo com o Governo e a necessidade de acesso remoto.

A Unidade de Tecnologia da Informação e Comunicação poderá expedir normas próprias que não conflitam com esta política.

Qualquer atualização desta Política de Uso da VPN estará implicitamente aceita pelos usuários atuais.

5. CONFORMIDADE

A violação desta política por qualquer usuário será reportada ao chefe imediato ou à equipe de suporte da Unidade de Tecnologia da Informação e Comunicação, que poderá tomar medidas para suspender de forma imediata, temporária ou permanente os seus privilégios de acesso a rede de dados computacional do Governo do Estado de Mato Grosso do Sul.

ANEXO V À DELIBERAÇÃO/CETI Nº 02, DE 24 DE FEVEREIRO DE 2022

GOVERNO DO ESTADO DE MATO GROSSO DO SUL
CONSELHO DE GOVERNANÇA DE MATO GROSSO DO SUL
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

Norma de Continuidade de Negócio

1. OBJETIVO

A Norma de Continuidade de Serviços tem por objetivo formalizar o processo de definição do Plano de Continuidade de Negócios, adotado pelo Governo do Estado de Mato Grosso do Sul.

2. ABRANGÊNCIA

Esta norma aplica-se a todos os colaboradores, prestadores de serviços, usuários internos e externos e quaisquer pessoas que tenham acesso as informações pertencentes ou custodiadas pelo Governo do Estado de Mato Grosso do Sul.

3. TERMOS E CONCEITOS

- **Plano de Continuidade de Negócio:** Processo de gestão da capacidade de uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de negócios críticos. O PCN deve ser desenvolvido preventivamente a partir de um conjunto de estratégias e planos táticos capazes de permitir o planejamento e a garantia dos serviços essenciais, devidamente identificados e preservados.
- **Teste:** Atividade na qual os planos de continuidade são exercitados de forma a garantir que os planos contenham as informações apropriadas e produzam o resultado desejado quando colocados em prática;
- **RPO**:(do inglês, Recovery Point Objective) diz respeito à quantidade de informação que é tolerável perder, no caso de indisponibilidade nos serviços;
- **RTO**:(do inglês, Recovery Time Objective) diz respeito à quantidade de tempo que as operações levam para estarem acessíveis, após uma indisponibilidade.

4. REFERÊNCIA

Este documento foi elaborado com base nas normas e padrões **ITIL, COBIT 5, ISO 20001** e **ABNT NBR 15999-1.**

5. RESPONSABILIDADES

- Grupo Executivo
  - Aprovar esta política e demais documentos complementares;
  - Implementar e gerir o Plano de Continuidade;
  - Participar da aprovação na ocorrência de contingências significativas ou cenários em que seja necessária tomada de decisões estratégicas para a organização ou segmento de negócios.
- Grupo de Comunicação / Apoio ao Executivo
  - Tomar decisões relacionadas aos serviços oferecidos na empresa;
  - Garantir a disseminação adequada da informação para áreas internas;
  - Efetuar contatos com as entidades externas, grupos participantes e fornecedores.
- Grupo de Administração de Crises
  - Supervisionar as atividades do Grupo Operacional;
  - Assegurar os recursos necessários para a operação do Plano de Continuidade;
  - Gerir cenários de contingência;
  - Apoiar o processo de decisão do Grupo de Comunicação;
  - Fazer testes para avaliação da continuidade dos serviços.
- Grupo Operacional
  - Apoiar o Grupo de Administração de Crises;

- Acessar e executar operações relacionadas às instalações e retorno do funcionamento dos serviços.

- Todos os colaboradores
  - Observar as práticas de segurança que possam contribuir no processo de gestão eficaz de continuidade de negócios.

6. PROCESSO DE CONTINUIDADE DE SERVIÇOS DE TI

A Gestão da Continuidade deve ser feita a fim de estabelecer e manter um plano que permita a TI e o negócio responderem a incidentes e interrupções para continuar a operação de processos críticos de negócio e serviços de TI necessários, mantendo a disponibilidade de informações em um nível aceitável para a empresa.

6.1 Definição de Escopo de Continuidade

- Todos os processos de negócios internos e terceirizados, atividades de serviço críticas para as operações da empresa ou necessárias para atender às obrigações legais e/ou contratuais devem ser identificados para a definição de um escopo a ser abordado no Plano de Continuidade.
- Todos os cenários possíveis que possam dar origem a eventos que podem causar incidentes perturbadores significativos devem ser identificados para a definição de um escopo do Plano de Continuidade.
- Fazer uma análise de impacto nos negócios a fim de avaliar o impacto de uma interrupção ao longo do tempo em funções críticas de negócios e o efeito que essas interrupções causam sobre elas.
- Estabelecer tempo máximo de recuperação dos serviços e suportes de TI e um número de interrupções máximas toleráveis em um período.
- Avaliar as probabilidades de ameaças que possam causar perda de continuidade dos negócios, a fim de identificar medidas uma melhor prevenção e maior resiliência.
- Definir condições e procedimentos de recuperação que permitam a retomada de processamento de negócios, incluindo atualização e reconciliação de bancos de dados de informações para preservar a integridade das informações.
- Analisar opções técnicas estratégicas, seus requisitos e custos de recursos avaliados.
- As exigências de backup de informações necessárias para suporte em casos de continuidade estão definidas no Procedimento de Backup.

6.2 Educação e Conscientização

- Todos os colaboradores da organização devem conhecer as fases do desenvolvimento do Plano de Continuidade e contribuir para a identificação de ameaças e riscos que possam afetar o negócio.
- O Plano de Continuidade deve considerar possíveis situações de risco e priorizar aquelas com maior impacto.
- O Plano de Continuidade deve ser incorporado na cultura do Governo do Estado de Mato Grosso do Sul.
- Realizar treinamento e conscientização de todos os colaboradores, para que a organização esteja preparada para momentos de contingência e garantia da continuidade dos serviços.
- Os treinamentos deverão ter o conteúdo ajustado de acordo com as funções do público-alvo e deve incluir orientações para desenvolvimento e implantação do Plano de Continuidade e para avaliação de riscos e ameaças.

6.3 Revisão e Auditoria

- Fazer revisões e auditorias do Plano de Continuidade e dos resultados dos testes regularmente, garantindo integridade no atendimento aos riscos de todos os sistemas da empresa (técnicos, logísticos, administrativos, comerciais e operacionais) e considerando o impacto de mudanças na organização empresarial, processos de negócios, acordos de terceirização, tecnologias, infraestrutura, sistemas operacionais e sistemas de aplicativos.
- Após a realização de revisão, fazer recomendações para melhorar o Plano de Continuidade vigente com base nos resultados.
- Comunicar todos os envolvidos após qualquer alteração no Plano de Continuidade.
- Os principais fornecedores e parceiros terceirizados devem ter continuidade efetiva em vigor certificada periodicamente.

6.4 Testes

- Esta regra visa orientar para a elaboração de testes e avaliações periódicas ou extraordinários a fim de garantir que o Plano de Continuidade cumpra seus objetivos.
- Fazer simulações de incidentes e interrupções nos testes a fim de avaliar possíveis problemas que podem ocorrer durante uma execução real.
- Os resultados e relatórios dos testes devem ser integrados e consolidados, a fim de integrar conhecimentos e novos procedimentos para o Plano de Continuidade.

ANEXO VI À DELIBERAÇÃO/CETI Nº 02, DE 24 DE FEVEREIRO DE 2022

GOVERNO DO ESTADO DE MATO GROSSO DO SUL
CONSELHO DE GOVERNANÇA DE MATO GROSSO DO SUL
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

Política de Backup e Restauração

1. OBJETIVO

A Política de Backup e Restauração tem como objetivo formalizar o processo de backup e restauração sistêmico do Governo do Estado de Mato Grosso do Sul. Seu propósito é realizar de forma segura a recuperação

de dados, independente da forma como eles foram perdidos, tais como: corrupção de dados (falha elétrica e de softwares), apagamentos acidentais (exclusão realizada por algum usuário), falha física de equipamento, falha por intempéries (mau tempo ou quaisquer condições climáticas mais intensas, como vento forte ou chuva torrencial) ou falhas na segurança dos dados (invasões ou ataques externos), assegurando a segurança, integridade e disponibilidade da informação.

2. ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores, prestadores de serviços, usuários internos e externos e quaisquer pessoas que tenham acesso as informações pertencentes ou custodiadas pelo Governo do Estado de Mato Grosso do Sul.

3. REFERÊNCIA

Este documento foi elaborado com base nas recomendações propostas pela norma **ABNT NBR ISO/IEC 27002:2013**, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis brasileiras vigentes.

4. DEFINIÇÕES E FUNÇÕES

- **Administrador de Banco de Dados**: Responsável técnico pelo serviço de instalação, configuração e gerenciamento do ambiente de banco de dados;
- **Administrador da Virtualização**: Responsável técnico pelo serviço de instalação, configuração e gerenciamento dos ambientes virtuais baseados em virtualização;
- **Backup Completo**: Modalidade de backup na qual todos os dados são copiados integralmente;
- **Backup Diferencial**: Modalidade de backup na qual somente os arquivos novos e modificados desde o último backup completo são copiados;
- **Backup Incremental**: Modalidade de backup na qual somente os arquivos novos e modificados desde o último backup realizado são copiados;
- **Backup de primeiro nível**: Armazenamento do backup em disco local;
- **Backup de segundo nível**: Armazenamento do backup em mídia externa;
- **Backup off-site**: Estratégia de backup que abrange a replicação de dados do backup em um local geograficamente separado do local dos sistemas de produção;
- **Catálogo de Serviços**: Listagem com todos os serviços ativos, que necessitam de backup;
- **Colaborador**: Integrante do quadro de funções da UTIC.
- **Mídia**: Meio físico no qual efetivamente armazenam-se os dados de um backup (fita magnética);
- **Retenção**: Período em que o conteúdo da mídia de backup deve ser preservado;
- **Recuperação de desastre**: Estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
- **Responsável pelo Serviço**: Colaborador da UTIC responsável pela operação de determinados serviços ou recursos computacionais do Governo do Estado;
- **RPO**:(do inglês, Recovery Point Objective) diz respeito à quantidade de informação que é tolerável perder, no caso de indisponibilidade nos serviços;
- **RTO**:(do inglês, Recovery Time Objective) diz respeito à quantidade de tempo que as operações levam para estarem acessíveis, após uma indisponibilidade;
- **Serviço de *backup***: todo ativo que possui informações ou dados e foi incluído nos serviços de *backup* em conformidade com as regras de inclusão.

5. DOMÍNIOS DE DADOS

Os serviços que serão contemplados nesta política de backup e restauração estarão divididos em dez categorias, para que cada tipo de dado possa ser tratado com maior especificidade, atendendo da melhor forma, cada tipo de serviço. As categorias são:

1. Arquitetura;
2. Banco de Dados;
3. Repositório de Arquivos;
4. E-mail;
5. Hospedagem;
6. Infraestrutura;
7. LDAP;
8. Plataformas WEB;
9. Sistemas;
10. Virtualização.

6. ATRIBUIÇÕES E RESPONSABILIDADES

A UTIC (Unidade de Tecnologia da Informação e Comunicação), é a equipe responsável pelo backup, delegando as atribuições de manter a política e procedimentos relativos aos serviços de backup e restauração, bem como de guardar as mídias e assegurar o cumprimento das normas aplicáveis.

A UTIC deve:

- Definir os modelos de documentos envolvidos em todo o processo de backup;
- Definir a periodicidade de relatórios técnicos, os quais avaliem todo o processo de restauração efetuado;
- Propor modificações visando o aperfeiçoamento da política de Cópia de Segurança e Restauração de Dados;
- Criar e manter os backups;
- Executar os procedimentos de restauração;
- Configurar a ferramenta de backup conforme os serviços;
- Configurar e operar os serviços e os ambientes de Restauração;

- Criar e testar procedimentos a fim de operacionalizar as atividades;
- Gerenciar mídias;
- Criar notificações e relatórios de backup;
- Criar Relatório de Execução de Restauração;
- Criar Modelo de Notificação conforme cenário de restauração;
- Verificar periodicamente os relatórios gerados pela ferramenta de backup;
- Restaurar os backups em caso de necessidade;
- Gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;
- Fazer manutenções periódicas dos dispositivos de backup;
- Fazer o carregamento dos backups programados para as mídias necessárias;
- Comunicar ao Responsável pelo Serviço as falhas e ocorrências de anomalias durante os procedimentos de backup e restauração;
- Fazer o armazenamento das mídias de backup em cofre;
- Definir o documento para Solicitação do Serviço de Backup;
- Definir o documento para Solicitação do Serviço de Restauração;
- Gerar relatórios gerenciais mensais.

Todo e qualquer serviço de responsabilidade da UTIC deverá ser ponderado e estudado antes de sua inclusão no backup. Após incluído, obrigatoriamente deverá seguir os procedimentos de restauração.

Serão abrangidos por esta política de backup e restauração, todos os serviços classificados com criticidade alta, no Catálogo de Serviços e, no mínimo, oitenta por cento dos serviços que possuírem criticidade média.

O responsável por cada serviço deverá definir quais servidores e respectivos diretórios e arquivos serão incluídos no backup, tendo como prioridade:

- Arquivos de configurações de ambientes e aplicativos referentes a serviços deste servidor em questão;
- Arquivos de log dos aplicativos, inclusive log da ferramenta de backup e restauração;
- Dados e configurações de banco de dados;
- Arquivos de usuários (documentos e e-mail).

A UTIC (Unidade de Tecnologia da Informação e Comunicação) deverá definir quais diretórios e arquivos não serão incluídos no backup, tendo como referência:

- Arquivos do sistema operacional ou de aplicações que podem ser obtidos através de uma nova instalação;
- Arquivos temporários;
- Arquivos salvos nas unidades locais das estações de trabalho;
- Arquivos da área de transferência;
- Arquivos particulares dos usuários.

Para os aplicativos e/ou bancos de dados de terceiros devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante, desde que estas não infrinjam nenhum dos artigos e parágrafos aqui descritos.

Os procedimentos de backup deverão ser atualizados quando houver:

- Novas aplicações desenvolvidas;
- Novos locais de armazenamento de dados;
- Novos arquivos com relevância para funcionamento do serviço;
- Novas instalações de bancos de dados;
- Novos aplicativos instalados;
- Outras informações que necessitem de proteção através de backups deverão ser informadas a UTIC, pelo Responsável pelo Serviço.

O backup deverá ser programado na ferramenta de backup e deverá ser testado antes de aplicar a programação solicitada. Estes testes deverão incluir uma restauração para comprovar a eficácia do backup.

A configuração e monitoração das funcionalidades relativas ao backup de banco de dados será de responsabilidade do Administrador de Banco de Dados.

7. PROCEDIMENTO DE BACKUP

Os backups de dados serão efetuados da seguinte forma:

1. O procedimento padrão para as Categorias de Dados que não possuírem especificação própria, seguirá a seguinte estratégia:
   A. O Backup Completo de todas as aplicações, será executado entre os 10 primeiros dias de cada mês e será copiado em dois locais diferentes. O primeiro será em storage, para facilitar o acesso rápido, em pequenas restaurações e terá sua retenção de 30 dias. O segundo será fita magnética e terá sua retenção detalhada no próximo capítulo.
   B. O Backup Incremental será executado durante os demais dias do mês e será copiado diariamente em dois locais diferentes. O primeiro será em storage e terá sua retenção finalizada após a realização do próximo backup Completo. O segundo será fita magnética e terá retenção de 3 meses.
2. O procedimento para a Categoria de Banco de Dados seguirá a seguinte estratégia:
   A. O Backup Completo será executado semanalmente e será copiado em dois locais diferentes. O primeiro será em storage e terá sua retenção de 30 dias. O segundo será fita magnética e terá sua retenção detalhada no próximo capítulo.
   B. O Backup Incremental e diferencial serão executados a cada 12 horas, intercalando as rotinas e será realizado em dois locais diferentes. Serão feitas em storage e sua retenção finalizada após a realização do próximo backup Completo. O segundo será fita magnética e terá retenção de 3

meses.

3. Quando um serviço for descontinuado, a UTIC deverá ser notificada e então providenciará um Backup completo final, envolvendo seu banco de dados e arquitetura quando necessário. Este backup deve ser gravado em fita magnética e guardada na fitoteca ou local de armazenamento aquedado no órgão.

8. GUARDA DOS DADOS

- Os backups do tipo Completo, realizados em fita magnética devem ser guardados mensalmente na fitoteca ou em local adequado designado pela UTIC, no dia 10 (dez) de cada mês, ou no dia útil consecutivo, juntamente com uma identificação física do conjunto de fitas;
- Deverá ser providenciado, juntamente com as fitas, uma planilha ou documentação equivalente para identificação física das mídias com o objetivo de viabilizar a restauração em caso de desastres;
- Visando atender a grande diversidade de naturezas dos serviços, contemplados por legislações, que definem diferentes prazos obrigatórios para guarda de documentos, os dados serão armazenados atendendo os requisitos desta política;
- As fitas armazenadas de cada ano terão tempo de guarda indeterminado, após descartada as informações armazenadas, a fita magnética será encaminhada para sobrescrita ou para descarte, caso apresente sinais de degradação ou esteja chegando ao final de sua vida útil;
- Deve-se acompanhar e providenciar um local seguro, para que o armazenamento das mídias.

9. **TRANSCRIÇÃO DE DADOS E DESCARTE DE MÍDIAS**

A fita magnética só será considerada confiável durante os dois primeiros terços da vida útil estabelecida pelo fabricante. Após expirado este prazo, as informações nela contidas deverão ser transcritas para uma nova mídia, a fim de zelar pela integridade dos dados.

O descarte das mídias de backup não confiáveis deverá ser realizado pela equipe responsável pelo backup, após informar a chefia imediata na UTIC.

- As fitas a serem descartadas deverão ser destruídas fisicamente, seguindo orientações do fabricante quanto a vida útil, de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.

10. **PROCEDIMENTO DE RESTAURAÇÃO**

A recuperação dos backups deverá obedecer às seguintes orientações:

- Todo e qualquer usuário que precisar recuperar arquivos, deve entrar em contato com a UTIC (Unidade de Tecnologia da Informação e Comunicação), que registrará a solicitação na ferramenta de controle de atendimento;
- A equipe responsável pelo cadastramento do chamado técnico solicitará o nome e setor do usuário, o(s) arquivo(s) a ser(em) recuperado(s), subdiretório(s) em que se encontra(m) e a data da versão que deseja recuperar, sendo esta última informação obrigatória para viabilizar a recuperação do arquivo;
- O chamado técnico será encaminhado à UTIC (Unidade de Tecnologia da Informação e Comunicação), que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) arquivo(s) ou informando o motivo pela impossibilidade de realização do mesmo;
- Deverá ser mantido registro de todos os arquivos cuja restauração foi solicitada, juntamente com as informações relativas ao solicitante, nome do arquivo, data da versão restaurada e data e hora da solicitação;
- A restauração dos arquivos somente será possível nos casos em que o arquivo tenha sido atingido pela estratégia de backup que ocorre conforme cronograma ajustado pela UTIC, ou seja, os arquivos criados e eventualmente apagados ou alterados não serão passíveis de recuperação no mesmo dia da criação.

11. **TESTES DE RESTAURAÇÃO**

As cópias de segurança armazenadas deverão ser testadas mensalmente, e a cada mês serão testados domínios de dados distintos, a fim de percorrer anualmente todos os itens descritos no Capítulo 5 (Domínios de Dados).

- A UTIC (Unidade de Tecnologia da Informação e Comunicação) deverá definir quais domínios de dados serão testados a cada mês;
- O teste será realizado com o intuito de validar a suficiência dos dados armazenados e a integridade das mídias de backup;
- O responsável pelo serviço terá total responsabilidade pela validação de todos os dados restaurados pela UTIC (Unidade de Tecnologia da Informação e Comunicação);
- Eventuais dados que não tenham sido incluídos no backup por falta de sinalização do responsável pelo serviço, deverão ser informados a UTIC (Unidade de Tecnologia da Informação e Comunicação) durante o período de testes.

Após a restauração dos dados, a recuperação do serviço deverá ser realizada pelo responsável pelo serviço com auxílio de áreas correlacionadas.

- O responsável pelo serviço deverá informar à UTIC (Unidade de Tecnologia da Informação e Comunicação) se a recuperação do serviço foi bem-sucedida ou se será necessária a inclusão de novos arquivos.

12. **DIRETRIZES DE OPERAÇÃO**

A criação e operação dos backups deverá obedecer às seguintes orientações:

- Criação de backups:

- O backup deverá ser programado para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede.

- Operação de backups:
  - O backup deverá ser monitorado pela UTIC (Unidade de Tecnologia da Informação e Comunicação);
  - Para todos os backups realizados com sucesso, deve ser gerado um extrato automatizado pela própria ferramenta de backup, confirmando a execução dele;
  - Os backups que apresentarem falhas, a UTIC (Unidade de Tecnologia da Informação e Comunicação) deverá verificar a falha e providenciar a correção para que o backup seja realizado novamente com sucesso na próxima janela disponível.

Os backups deverão ser realizados seguindo as regras de acordo com cada nível de serviço, levando em conta a classificação dos dados.

- Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, a UTIC (Unidade de Tecnologia da Informação e Comunicação) deverá adotar as providências no sentido de guarda das informações através de outro mecanismo, como por exemplo: cópia dos dados para outro servidor, execução do backup em outro horário de agendamento etc.

Os backups mensais de todas as categorias deverão ser testados, no prazo máximo de um ano, após a sua execução.

Quaisquer procedimentos programados nos servidores e que impliquem riscos de funcionamento em quaisquer serviços ou equipamento da instituição, somente deverão ser executados somente após a realização de backup com sucesso dos seus dados.

O backup off-site deverá armazenar os dados em fita ou storage, em qualquer unidade do Governo do Estado de Mato Grosso do Sul, atendendo os requisitos deste artigo.

- A armazenagem do backup off-site deve estar obrigatoriamente fora do prédio onde encontra-se o data center de produção;
- Os dados que serão transportados ao backup off-site deverão estar criptografados;
- O armazenamento off-site deve estar em conformidade com padrões estabelecidos nesta política.

13. **CONSIDERAÇÕES FINAIS**

Fica estabelecido o prazo de 90 (noventa) dias, a contar da data de publicação desta política para a adoção das providências necessárias para prover uma infraestrutura à implementação plena desta política de backup pelo Governo do Estado de Mato Grosso do Sul.

Este ato entra em vigor na data de sua publicação.

DELIBERAÇÃO CETI Nº 03, DE 24 DE FEVEREIRO DE 2022.

Aprova a Arquitetura de Referência.

O PRESIDENTE DO COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO - CETI, no uso de suas atribuições, com fundamento no inciso I, do art. 2º, do Decreto 15.478, de 20 de julho de 2020 e no art. 16, do Regimento Interno, de 30 de novembro de 2020, e

Considerando votação unânime da Arquitetura de Referência para Microsserviços apresentada em reunião realizada em 09 de fevereiro de 2022. Considerando a necessidade de regulamentação desta,

D E L I B E R A:

Art. 1º Aprova a Arquitetura de Referência para Microsserviços.

Art. 2º Esta deliberação entra em vigor na data de sua publicação.

Campo Grande, 24 de fevereiro de 2022.

GUSTAVO NANTES GUALBERTO
Presidente do Comitê Estratégico
de Tecnologia da Informação - CETI

LORIVALDO ANTONIO DE PAULA
Secretário do Comitê Estratégico
de Tecnologia da Informação - CETI