GOVERNO DO DISTRITO FEDERAL

SECRETARIA DE ESTADO DA MULHER DO DISTRITO FEDERAL

Subsecretaria de Administração Geral

Diretoria de Tecnologia da Informação e Comunicação

Plano Diretor de Tecnologia da informação e Comunicação - PDTIC da Secretaria de Estado da Mulher do Distrito Federal

Para o Biênio 2021 – 2023

COMITÊ GESTOR DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO - CGTIC

(PORTARIA Nº 40, DE 11 DE MAIO DE 2021)

I - Secretária Executiva – VANDERCY ANTONIA DE CAMARGOS

II - Subsecretária de Administração Geral – REJANE PARENTE LUCAS

III - Subsecretária de Enfrentamento à Violência Contra as Mulheres – IRINA ABIGAIL TEIXEIRA STORNI

IV - Subsecretária de Politicas para Mulheres – FERNANDA FIGUEIREDO FALCOMER MENESES

V - Diretor de Tecnologia da Informação e Comunicação – RODRIGO MARCELINO DA SILVA

1. INTRODUÇÃO

O Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC da Secretaria de Estado da Mulher - SMDF, abrange o período de 2021 à 2023.

Este instrumento tem a finalidade de orientar o direcionamento tecnológico da SMDF, permitindo que o desempenho das atividades exercidas pelos colaboradores desta Secretaria, seja mais eficiente e eficaz, sempre com foco no atendimento aos serviços prestados por esta Secretaria, visando a agilidade no fluxo das informações e conhecimentos, perpassando pela substituição de toda estrutura física de equipamentos, de servidores, de introdução de novas rotinas de produção e armazenamento de documentos, de uma rede social de comunicação, de transferência de experiências, informações e serviços.

Todas as fases de implantação de modernização são necessárias para a melhoria da infraestrutura de equipamentos e serviços atualmente disponibilizados. O ambiente tecnológico defasado torna-se responsável pela inconsistência dos serviços disponibilizados, impossibilitando a implantação de novas tecnologias capazes de melhorar o atendimento ao cidadão.

As inovações apresentadas serão acompanhadas de justificativas capazes de corroborar a necessidade latente da sua implantação, cada uma em sua singularidade, adequando a realidade global de introdução de novas e modernas iniciativas. Inovações estas, com intuito muito peculiar de trazer, novamente, a Secretaria para o eixo das instituições preocupadas em acompanhar os avanços tecnológicos em prol do alcance dos objetivos sociais.

Todos os procedimentos e soluções apontados neste documento foram definidos conforme as necessidades levantadas junto às Unidades Organizacionais da SMDF, previsto nas ações do Plano Plurianual (PPA 2020-2023) e no Planejamento Estratégico Institucional –PEI/SMDF.

O PDTIC abrange a descrição das estratégias e políticas da SMDF no que afeta a Tecnologia da Informação, bem como, os princípios e diretrizes aplicáveis ao planejamento e a estrutura organizacional desta Secretaria. Para isto, utilizou-se a análise SWOT (“Strenghts”, “Weaknesses”, “Opportunities” e “Threats”, na sigla em inglês), um sistema de avaliação dos pontos fortes, dos pontos fracos do ambiente corporativo e das oportunidades e das ameaças externas a este ambiente. Tal análise permite, de forma simples, verificar a situação da área de tecnologia em face às necessidades de informação e comunicação da SMDF.

2. MOTIVAÇÃO

Uma preocupação constante da Gestão das organizações é a busca pelo alinhamento estratégico entre a área de Tecnologia da Informação e Comunicação e a área de negócios da Instituição, com o objetivo de atender à demanda pela alta qualidade de seus serviços, economia, confiabilidade, flexibilidade, agilidade e racionalização de seus fluxos de trabalho.

Devido ao elevado grau de automação dos processos operacionais e administrativos da SMDF e ao desenvolvimento das atividades finalísticas executadas, a instituição passou a confiar e a depender, cada vez mais, de sua infraestrutura tecnológica para viabilizar aplicações de missão crítica e implementar novas soluções que aumentem a agilidade, a capacidade de adaptação, a otimização de custos e a melhoria da qualidade dos serviços prestados aos seus clientes e usuários.

No cenário atual, a complexidade e os riscos inerentes ao ambiente tecnológico da SMDF, tem gerado aumento nos custos, enquanto a satisfação dos usuários de tecnologia com o suporte e o tempo de resposta para a resolução dos problemas vem decrescendo.

Diante destas realidade, é necessário que as áreas de TI das organizações mudem seu enfoque de atendimento aos usuários, de reativo para proativo, alcançando um gerenciamento integrado dos processos envolvidos na entrega e suporte a serviços de tecnologia da informação.

Esta mudança se dá por meio do aumento da aderência das áreas de TI às melhores práticas de mercado, incrementando os processos de gestão dos serviços, aprimorando o controle sobre a infraestrutura tecnológica e implantando um Modelo de Governança Tecnológica que alcance o autogerenciamento e valorize as soluções sob a perspectiva de todas as áreas interessadas.

O Governo do Distrito Federal vem definindo diretrizes para as áreas de TI dos seus órgãos, estabelecidos na Estratégia Geral de Tecnologia da Informação – EGTI, com o objetivo de promover a mudança no modelo de gestão da área de TI.

Diante do exposto, um dos requisitos fundamentais para atingir os objetivos da EGTI, é a elaboração e aprovação do Plano Diretor de Tecnologia da Informação e Comunicação dos órgãos vinculados ao GDF, tendo como base o Planejamento Estratégico Institucional, o Planejamento Diretor de Tecnologia da Informação e Comunicação (IN/SLTI 04/2014, Art. 2º, X E Art. 4º, §ÚNICO, III), o Planejamento da Contratação (IN/SLTI 04/2014, Art. 8º) e outros PDTICs já elaborados.

3. PERÍODOS DE VALIDADE E REVISÕES

O período de vigência do Planejamento de Tecnologia da Informação da SMDF abrange os anos de 2021 - 2023.

As revisões cabem ao Comitê de Tecnologia da Informação e Comunicação da SMDF.

4. HISTÓRICO DA SECRETARIA E CENÁRIO ATUAL

Com a publicação do Decreto nº 39.610, de 1° de janeiro de 2019, a Secretaria de Estado da Mulher desvinculou-se da estrutura da SEDESTMIDH, passando a integrar a estrutura organizacional da Administração Direta do Distrito Federal, como Secretaria de Estado. No entanto, a sua estrutura meio, permaneceu no âmbito da Secretaria de Estado de Desenvolvimento Social - SEDES, tendo, inclusive, sua estrutura de TI abarcada pelo PDTI 2019-2023 daquela Pasta, o que foi alterado após a publicação da nova estrutura administrativa, que se deu por meio do Decreto nº 40.698, de 7 de maio de 2020, tornando a SMDF, autônoma, continuando com a missão de melhorar a estrutura de atendimento às mulheres do Distrito Federal, trabalhando no enfrentamento à violência contra a Mulher e na sua autonomia econômica.

A Área de Tecnologia está presente na SMDF, por meio da Diretoria de Tecnologia da Informação - DITEC, subordinada à Subsecretaria de Unidade de Administração Geral - SUAG, sendo responsável por implementar e buscar soluções e inovações na área de TI.

Atualmente, os serviços corporativos de tecnologia da informação e comunicação, tais como, armazenamento de dados, acesso à internet e hospedagem de servidores, aplicações e sistemas, são hospedados no Data Center da Subsecretaria de Tecnologia - SUTIC, da Secretaria de Estado de Economia do Distrito Federal, e são geridos por equipe técnica especializada, com funcionamento 24h por dia, 7 dias na semana, garantindo um ambiente seguro, aparelhado com sistema de combate a incêndios, ar de precisão, energia e segurança, com soluções integradas de hardware e software com a finalidade de prover serviços de Tecnologia para todo o GDF.

5. REFERÊNCIAS ESTRATÉGICAS

5.1. Planejamento Estratégico Institucional da SMDF

Este PDTIC está alinhado à visão, missão e objetivos estratégicos da SMDF, conforme mapa abaixo:

5.1.1. Missão

Promover Políticas Públicas voltadas para as mulheres do Distrito Federal.

5.1.2. Visão

Ser reconhecida pela excelência na prestação de serviços e na implementação de políticas públicas voltadas para as mulheres do Distrito Federal.

5.1.3. Efetividade

Atuar sempre com vistas à obtenção de resultados positivos, com eficiência e eficácia, controlando os riscos inerentes às atividades de TI.

5.1.4. Economicidade

Viabilizar economicamente as instituições governamentais, por meio de soluções tecnológicas compartilhadas e com melhor custo-benefício.

5.1.5. Inovação

Incentivar a busca contínua de soluções inovadoras para uma melhor utilização das informações, soluções e recursos de TI.

5.1.6. Transparência

Dar ampla publicidade das ações governamentais na área de TI, com o intuito de elevar a qualidade na prestação de informações à sociedade.

5.1.7. Premissas

O PDTIC deve estar alinhado ao Planejamento Estratégico Institucional da SMDF em cumprimento da missão, objetivos e metas, e obedecer às normas que regulamentam o processo de aquisição e/ou implantação de tecnologias no Distrito Federal.

6. OBJETIVOS E INICIATIVAS ESTRATÉGICAS

6.1. Com a implantação do PDTIC, no decorrer do biênio 2021-2023, a SMDF pretende atingir os seguintes objetivos estratégicos:

- aprimorar a Gestão de serviços de TI;
- otimizar os processos de trabalho;
- integrar a gestão da informação e do conhecimento;
- ter segurança da informação de TI balizada nas boas práticas;
- implantar mecanismos básicos de Governança de TI;
- ter os processos de contratação de TI baseados nas melhores práticas;
- reduzir riscos inerentes às atividades de TI;
- promover serviços de qualidade ao cidadão;
- ampliar o atendimento às mulheres do Distrito Federal.

6.2. DOCUMENTOS NORTEADORES

- Modelo PDTIC – Governo Federal – Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG;
- PDTIC da Secretaria de Transparência e Controle;
- PDTI do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq;
- Instrução Normativa nº 04 de 11 de setembro de 2014.
- PDTI SEDESTMIDH 2019-2023.

6.3. PRINCÍPIOS E DIRETRIZES

Na elaboração do PDTIC da SMDF foram adotados os seguintes princípios e diretrizes:

6.3.1. Princípios

- Conformidade: agir sempre de acordo com as leis e normas Distritais e Federais;

- Economicidade: escolher a melhor solução levando em consideração sempre o menor preço;

- Independência Tecnológica: possuir recursos físicos que lhe possibilitem prover e gerenciar serviços, como o armazenamento e a troca de informações;

- Transparência: atuar com transparência, publicando as informações relevantes da SMDF a todos interessados.

6.3.2. **Diretrizes**

As diretrizes são as linhas segundo as quais se traçam um plano para atingir uma finalidade. Portanto, as diretrizes que serão as instruções para alcançar os objetivos do PDTIC são as seguintes:

DIRETRIZES	DESCRIÇÃO
D1	Manter os processos internos de TI mapeados, formalizados, mensurados e otimizados.
D2	Promover o atendimento às normas de acessibilidade (e-Mag) e interoperabilidade do Governo Eletrônico (e-Ping), incluindo padrões de governança.
D3	Garantir a segurança da informação e comunicações.
D4	Buscar a melhoria contínua da infraestrutura de TI.
D5	Estimular a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar padronização, integridade e segurança.
D6	Adotar padrões abertos no desenvolvimento de tecnologia da informação e comunicação.
D7	Dispor de servidores efetivos suficientes e capacitados.
D8	Prestar atendimento de qualidade aos usuários.
D9	Garantir a disponibilidade, confidencialidade e integridade dos serviços de TI.
D10	Aprimorar a integração entre os sistemas de informação da SMDF com os demais sistemas do GDF.
D11	Buscar a melhoria contínua do processo de contratação e execução dos serviços de TI.
D12	Maximizar, sempre que possível, a terceirização de tarefas operacionais, para permitir que os servidores efetivos lotados na TI, trabalhem com gestão e governança da TI.
D13	Padronizar o ambiente de TI, visando à integração de Soluções no GDF.
D14	Estar alinhado com a EGTI do GDF.
D15	Estar alinhado com a Lei Geral de Proteção de Dados - LGPD.

7. ESTRUTURA DA TI

Atualmente a área de TI da SMDF está subordinada à Subsecretaria de Administração Geral - SUAG, possuindo uma Diretoria e uma Gerência.

- **Diretoria de Tecnologia da Informação e Comunicação - DITEC**
  - **Gerência de Suporte técnico - GESUT**

8. ANÁLISE SWOT

A Análise SWOT é uma ferramenta utilizada para fazer análise de cenário (ou análise de ambiente), sendo usada como base para gestão e planejamento estratégico de uma instituição e devido a sua simplicidade, pode ser utilizada para qualquer tipo de análise de cenário.

A ferramenta foi utilizada para se ter um panorama geral da área de TI, considerando o ambiente interno (formas e fraquezas) e o ambiente externo (oportunidades e ameaças), conforme exposto abaixo:

AMBIENTE INTERNO	
Forças	**Fraquezas**
• Planejamento Estratégico Institucional instituído • Apoio dos Dirigentes • Recursos Orçamentários disponibilizados • Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC em fase de finalização	• Quadro de servidores da TIC, insuficiente • Ausência de uma gerência de Sistemas • Serviços operacionais executados por profissionais da área de gestão • Ausência de objetivos e de indicadores de desempenho da gestão e do uso da TIC
AMBIENTE EXTERNO	
Oportunidades	**Ameaças**
• Lei de Acesso à Informação • Maior fiscalização pelos órgãos de Controle • Estratégia Geral de Tecnologia da Informação – EGTI instituída no GDF • Lei Geral de Proteção dos Dados - LGPD • Estabelecimento de parcerias com outros órgãos de outros poderes, visando ações sinérgicas • Inovações tecnológicas disponibilizadas pelo mercado • Fortalecimento Institucional • SMDF com necessidade de informatização	• Alta rotatividade dos gestores e recursos humanos na TIC • Descontinuidade da gestão pública • Baixa sinergia e pouco alinhamento entre programas e políticas de governo • Pouca percepção das áreas de negócio em relação à realidade, à importância e às características das áreas de TIC • Contingenciamento orçamentário • Altos custos dos serviços de TIC • Decisão política prevalecendo sobre critérios técnicos

9. ANALISE DE MATURIDADE

Com base nos quadros e gráficos apresentados, será possível avaliar os recursos e tecnologias da SMDF e os resultados de sua utilização, conforme será apresentado abaixo:

9.1. **Itens de Infraestrutura e atendimento**

ÁREA	INFORMAÇÕES	ADERÊNCIA
Ambiente físico	Possui ambiente protegido fisicamente? (Sala cofre)	Não

e segurança física	Os servidores possuem fontes redundantes?	Sim
	As fontes redundantes dos servidores estão ligadas em réguas diferentes, em quadros e circuitos elétricos distintos?	Sim
	Os servidores possuem garantia ativa?	Não aplicável
	Possui Nobreak funcional e ativo?	Não aplicável
	Possui gerador funcional e ativo?	Não aplicável
	São realizados testes periódicos nos geradores para garantir que estão funcionando?	Não aplicável
	São realizados testes periódicos nos nobreaks para garantir que estão funcionando?	Não
	A rede elétrica é protegida, possui caminhos físicos distintos para diferentes quadros elétricos, e possui Nobreak?	Não
	O acesso as áreas dos equipamentos são protegidas de entrada de pessoas não autorizadas?	Sim
	Existe acompanhamento da equipe em caso de manutenções feitas por empresas terceiras?	Sim
	Os acessos ao datacenter e acompanhamentos de terceiros pela equipe são registrados em alguma ferramenta ou documentação?	Sim
	Possui garantia contratual ativa da sala cofre?	Não
	Possui garantia contratual ativa do (s) nobreak (s) ?	não
	Possui garantia contratual ativa do (s) gerador (es) ?	Não
	É realizada manutenção preventiva da sala cofre?	Não
	É realizada manutenção preventiva do (s) nobreak (s)?	Não aplicável
	É realizada manutenção preventiva do (s) gerador (s) ?	Não
	Existem controles adotados para minimizar o risco de ameaças potenciais, como roubo, fogo, explosão, fumaça, água, poeira, vibração, efeitos químicos, interferência no fornecimento de energia, radiação eletromagnética ou inundação nas áreas dos equipamentos?	Não
	O Nobreak está cadastrado na ferramenta de monitoração, alertando a equipe de monitoração do NOC em caso de falhas?	Não aplicável
	O Gerador está cadastrado na ferramenta de monitoração, alertando a equipe de monitoração do NOC em caso de falhas?	Não aplicável
	A sala-cofre está cadastrada na ferramenta de monitoração, alertando a equipe de monitoração do NOC em caso de falhas?	Não aplicável
Antivírus	Possui licença da solução de antivírus?	Não
	Possui ambiente de proteção para os servidores?	Não
	Possui ambiente de proteção para as estações?	Não
	Possui dados estatísticos de atividades de vírus na rede?	Não
Monitoração e Operação	Possui um NOC monitorando e atuando nos serviços, notificando as partes interessadas em caso de incidentes?	Não
	Possui check-list do ambiente físico e equipamentos do cliente?	Sim
	Possui dados estatísticos sobre incidentes de rede?	Não
	Possui informações de disponibilidade segmentada por área de atuação com monitoração do SLA?	Não
	Notifica incidentes via SMS pra o cliente?	Não
	Possui ferramenta de monitoração?	Sim
	Ferramenta de monitoração permite agendamento de manutenção programada (downtime)?	Sim
	A ferramenta de monitoração permite gerar dashboard de disponibilidade dos ambientes?	Sim
	Ferramenta de monitoração permite excluir da disponibilidade global os tempos de indisponibilidades causadas por manutenções programadas?	Não
	A equipe de monitoração consegue atuar remotamente através de VPN ou outro método seguro?	Sim
	A equipe de monitoração possui acesso à ferramenta de ITSM para abertura de tickets?	Sim
Armazenamento Corporativo	Possui storage para armazenamento dos dados corporativos?	Sim
	Recebe periodicamente informações de utilização do espaço storage? (Ocupado/Disponível/Etc)	Sim
	Possui replicação entre storages?	Sim
	É realizado algum teste de falha com periodicidade definida?	Não
	A área de armazenamento de dados do usuário (File Server) possui cota habilitada?	Não
	A área de armazenamento de dados do usuário (File Server) possui restrição de alguns formatos de arquivos? Ex. MP3, MOV, etc	Sim
	Existe política informando que tipo de informações devem ser armazenadas nos servidores de arquivo com suas respectivas restrições e pressupostos?	Sim
	Os usuários e seus superiores são notificados quanto colocado algum arquivo que não esteja em conformidade com a política estabelecida?	Não
	As partes interessadas recebem informações sobre a utilização dos servidores de arquivos? Ex. Área que mais utiliza o armazenamento, quantidade de arquivos por área, etc.	Não
Virtualização	Ambiente de virtualização está licenciado?	Sim
	Os hosts estão ligados ao storage através de interface apropriada e de alta performance?	Não
	Monitora a utilização de recursos dos hosts?	Sim
	Possui ferramenta de recuperação de desastres?	Não
	Faz backup do ambiente virtualizado através de alguma ferramenta?	Sim
	A tecnologia de virtualização permite adição de recursos sem necessidade de reinicializar o servidor?	Sim

Serviço de diretório e autenticação	Possui serviço de autenticação replicado, com cluster e tolerante a falhas?	Sim
	É realizado teste de falha desse ambiente periodicamente?	Não
	São criadas contas específicas para serviços e são devidamente documentadas?	Sim
	As senhas são documentadas e armazenadas em um sistema e/ou local seguro?	Sim
	Existe processo e documentação para criação e exclusão de novos usuários da rede?	Sim
	O serviço de diretório está cadastrado na ferramenta de monitoração?	Sim
	Possui uma CA interna?	Não
	Os sistemas internos utilizam autenticação integrada com serviço de diretório?	Sim
	Utiliza smartcard ou sistemas biométricos para autenticação?	Não
Correio Eletrônico	Os usuários conhecem a política de envio de correio?	Sim
	Possui instrução normativa de correio eletrônico?	Sim
	Possui dados estatístico de tráfego de mensagens?	Não
	Possui dados estatísticos de utilização das bases de dados de e-mail segmentados por área interna?	Não
	Possui ferramenta de AntiSpam?	Sim
	O usuário pode ter sua própria lista de spam personalizada, informando sua lista de rejeição para ferramenta?	Sim
	Os e-mails são criptografados entre os usuários corporativos?	Não
	Possui antivírus para solução de e-mail?	Sim
	Possui serviço de correio replicado, com cluster e tolerante a falhas?	Sim
Windows Server	Todos os sistemas operacionais são licenciados?	Sim
	Os sistemas operacionais são padronizados quanto a instalação?	Sim
	Possui suporte vigente?	Sim
	As partições de informações sensíveis são separadas do sistema operacional?	Não
	Os logs de segurança são armazenados em local que seja possível recuperação de acessos e violações?	Sim
	Existe templates padrão para o sistema operacional?	Sim
	As solicitações de novos servidores passam por um processo padronizado?	Sim
	O servidor é atualizado em um repositório interno de pacotes? (WSUS)	Sim
	Os login no sistema operacional são feitos utilizando autenticação no serviço de diretório da instituição?	Não
	São monitorados contadores de desempenho de rede, cpu, carga, i/o de disco, interrupções, fila de cpu, swap e outros na ferramenta de monitoração?	Sim
	São feitas atualizações dos pacotes periodicamente?	Sim
	São realizadas verificações de segurança e auditorias utilizando alguma ferramenta? Ex. Microsoft Baseline Security Analyzer	Sim
	O sistema de arquivos do disco é criptografado?	Não
Windows Clients	Existe uma padronização da versão do sistema operacional no ambiente?	Não
	As informações sensíveis dos usuários estão em uma partição separada do sistema operacional?	Não
	Os sistemas operacionais são padronizados quanto ao processo instalação?	Não
	Existe servidor de imagens? Ex. Ghost, WDS.	Não
	As imagens são atualizadas periodicamente?	Não
	As estações são atualizadas em um repositório interno de pacotes? (WSUS)	Não
WSUS	Possui serviço do Windows Server Update Service instalado?	Sim
	Possui informações estatísticas dessas atualizações e informa o cliente?	Não
Ambiente de rede	Os ativos de rede estão cadastrados na ferramenta de monitoração para envio de alertas?	Sim
	Os equipamentos permitem a comunicação com software de monitoração a fim de gerar alertas?	Sim
	Existe backup das configurações dos equipamentos de forma a configurar um novo dispositivo em caso de falhas?	Sim
	A rede lógica está segmentada?	Sim
	Existe documentação da rede?	Sim
	As senhas dos equipamentos são documentadas e armazenadas em um sistema e/ou local seguro?	Sim
	Os logins nos equipamentos são feitos utilizando autenticação no serviço de diretório da instituição?	Não
	Existe redundância na comunicação entre os switches de acesso e o core da rede?	Não
	São feitos testes de failover nos equipamentos periodicamente?	Não
	O acesso à rede pelos usuários e estações de trabalho é controlado por intermédio do 802.1x ou protocolo semelhante com a mesma finalidade?	Sim
	Existe monitoração do tráfego entre os switches de acesso e o core afim de tratar gargalos na rede?	Não
	Existe monitoração de utilização física de portas dos equipamentos a fim de tratar pontos que não possuem usuário ou equipamento na borda?	Não
	Existe monitoração dos erros dos equipamentos como perda pacotes, desabilitação de portas, mudança de topologia de rede, etc.?	Não
	Existe algum mecanismo de proteção que impeça que o usuário adicione por engano um equipamento na rede que não esteja autorizado? (Ex. Hub, switch, access points, etc)	Não
	Existe e está configurado no switch algum mecanismo de proteção de portas que bloqueia computadores ou dispositivos que estejam gerando erros na rede?	Não
	A rede cabeada foi certificada?	Não
	A rede cabeada é identificada permitindo facilmente a ativação dos pontos?	Sim
	Existe equipamentos de teste de continuidade e localização dos pontos de rede? (Testador e localizador de cabos)	Sim

	Existem servidores de distribuição de endereços de IP na rede (DHCP) trabalhando de forma redundante?	Sim
	É realizado teste de falha nos servidores de DHCP periodicamente?	Sim
	Existem servidores de resolução de nomes na rede (DNS) de forma redundante?	Sim
	É realizado teste de falha nos servidores de DNS periodicamente?	Sim
Segurança	São realizados testes de penetração e segurança nas aplicações antes que elas entrem em produção?	Não
	Existe procedimento de segurança aplicado aos sistemas operacionais de acordo com as melhores práticas?	Sim
	Existe um processo para criação de regras no firewall de forma que seja possível rastrear as solicitações?	Sim
	As regras são comentadas e associadas ao número do ticket da ferramenta de ITSM?	Não
	O firewall da rede possui tolerância a falhas?	Sim
	São realizados testes de failover periodicamente no firewall?	Não
	É feita periodicamente revisão das regras do firewall, documentado e encaminhado para o cliente informando possíveis inconformidades?	Não
	Existe ferramenta de auditoria capaz de identificar a integridades dos arquivos corporativos?	Não
	Existe uma política de segurança na instituição de fácil acesso as partes interessadas?	Sim
	Existe uma campanha periódica de divulgação da política de segurança?	Sim
	Os incidentes de segurança são comunicados as partes interessadas seguindo uma matriz de comunicação definida?	Sim
	Existe ferramenta de detecção de intrusão (IDS) no ambiente?	Sim
	Existe ferramenta de prevenção de intrusão (IPS) no ambiente?	Sim
	Os equipamentos e sistemas envolvidos na segurança estão na garantia?	Sim
	Os equipamentos de segurança estão cadastrados na ferramenta de monitoração?	Não
	Existe campanha de conscientização dos usuários na intranet outro meio sobre políticas de segurança, como por exemplo, a importância de não divulgar a senha a terceiros?	Sim
	Os usuários e seus superiores são notificados nos casos de infringirem as normas de segurança?	Sim
	Existe classificação das documentações criadas na instituição?	Sim
	É feita análise de vulnerabilidade do ambiente periodicamente?	Não
	Existe um controle eficiente criação/remoção de funcionários terceirizados na rede?	Sim
	Funcionários terceirizados preenchem termo de confidencialidade da instituição?	Sim
	Os logs dos servidores são registrados e armazenados em mídia ou outro meio de forma que seja possível dar respostas aos incidentes de segurança pelo período de 5 anos?	Não
	Os acessos à Internet de todos usuários são registrados em log, e armazenados em mídia ou outro meio de forma que seja possível dar respostas aos incidentes de segurança pelo período de 5 anos?	Não
	Aplicações WEB que necessitam de transferência de usuário e senha são protegidas por certificado SSL devidamente validado pela cadeia de certificação?	Não
	Existe um processo de formatação de baixo nível de servidores e estações que serão mais utilizados, a fim de prevenir a recuperação dos dados no disco?	Não
Backup	Existe política de backup definida na instituição?	Sim
	As mídias são armazenadas fora do ambiente de produção?	Sim
	São feitos testes de recuperação com periodicidade definida?	Não
	Existe redundundância no sistema de backup possibilitando realização do backup mesmo com falha de algum de seus componentes?	Não
	É feito backup das máquinas virtuais permitindo voltá-las em caso de falhas?	Não
	Além do backup convencional feito em mídia, existe outro mecanismo que permita recuperar o arquivo rapidamente para o usuário diminuindo o tempo de recuperação? Ex. Shadow Copies	Não
	Existe robô de backup na instituição?	Não
	O backup é feito em mais de um tipo de mídia? Ex. disco e fita	Não
	É feita análise periódica do consumo de backup do ambiente, e encaminhado para o cliente?	Não
	A política de backup é revisada periodicamente pela equipe?	Não
	Os equipamentos e sistemas envolvidos no backup estão na garantia?	Não
	São realizados backups das configurações do ambiente? Ex. arquivos de configuração do sistema operacional, switches, regras de firewall, etc.	Sim
	Existe um cálculo definido para janela de backup?	Não
	As políticas de backup estão documentadas?	Não
	A ferramenta de backup está cadastrada no software de monitoração?	Sim
	Existe um plano de recuperação de desastres no ambiente?	Não
	É realizado teste de recuperação de desastres periodicamente?	Não
Banco de dados	Existe segmentação ambiente com desenvolvimento, homologação e produção?	Não
	O acesso à produção é restrito apenas aos administradores do banco?	Sim
	A criação de contas na produção é feita pelo administrador do banco de dados, seguindo um processo definido e divulgado para os interessados?	Sim
	Os usuários e senhas dos bancos são documentados e armazenados em um sistema e/ou local seguro?	Sim
	Os bancos de dados são redundantes e tolerantes a falhas?	Não
	É realizado teste de falhas do SGBD periodicamente?	Não
	São monitorados contadores de desempenho dos SGBD's?	Não

	Os SGBD's estão cadastrados na ferramenta de monitoração, gerando alertas para equipe em caso de falhas?	Sim
	Os bancos de dados pagos possuem suporte ativo?	Não
	São monitoradas as conexões abertas com os bancos a fim de evitar esgotamento de recursos?	Não
	É executado teste das consultas (queries) das aplicações no ambiente de homologação antes de ir para o ambiente de produção a fim de evitar problemas de desempenho?	Não
	As senhas das aplicações são criptografadas no banco?	Não
	Os nomes dos bancos, tabelas e colunas utilizam nomes consistentes seguindo um padrão previamente definido pelo órgão?	Não
	As tabelas são criadas sem utilização de prefixos desnecessários? Ex. TblCadastro	Não
	Todas tabelas são criadas com um campo ID, afim de melhorar indexações, associações, etc?	Não
	As indexações são realizadas sempre em colunas com tipo inteiro e suas variantes?	Não
	Utiliza técnica de ORM para aplicações orientadas a objeto?	Não
	Os SGBD's possuem plano de recuperação de desastres?	Não
	Os SGBD's estão em cluster failover?	Não
	As triggers, stored procedures e scripts estão documentados?	Não
	Utiliza ferramentas de análise de consultas (queries) para definição da criação de índices?	Não
	Os servidores de banco são separados dos servidores de aplicação?	Sim
	Os bancos de dados são desenhados e modelados juntamente com o DBA que cuida da infraestrutura?	Não
Itens de Atendimento (Service Desk):		
Atendimento Service Desk	Possui supervisor de atendimento?	Não
	O supervisor de atendimento ou membro da equipe são integrantes do comitê de gestão de mudanças?	Não
	O supervisor de atendimento participa das reuniões de mudança do ambiente?	Não
	O Atendimento é informado dos impactos das mudanças antes que elas sejam feitas?	Sim
	As equipes de analistas informam de maneira formal, com procedimentos de atendimento quando surge um problema no ambiente?	Não
	O fechamento dos incidentes e requisições são feitos pelo SPOC independente de quem tenha atendido a solicitação, garantindo que a solicitação do usuário tenha sido atendida?	Não
	No processo de gestão de mudança está incluído o impacto que será causado no usuário final e a resposta padrão que será utilizada caso a mudança não seja feita com sucesso?	Sim
	Os colaboradores conhecem os SLA's acordados e suas respectivas metas?	Não
	São divulgadas alterações ou criações dos SLA's para colaboradores e usuários?	Não
	O centro de suporte possui elementos estratégicos como Visão, Missão e Valores?	Não
	O dimensionamento da equipe foi realizado de acordo com as normas de atendimento de mercado? (Demonstre o método utilizado)	Não
	O centro de suporte elabora matriz de SWOT a fim de pesquisar para suas forças, fraquezas e saber identificar suas oportunidades e ameaças?	Não
	Seu centro de suporte identifica na ferramenta de ITSM os custos por serviços e apresenta os resultados aos stakeholders para tomadas de decisões?	Não
	A estratégia do suporte realiza levantamento de custos por setor, afim de identificar GAP's de conhecimento e planejar futuros treinamentos e workshops?	Não
	As áreas que mais contribuem positivamente para o suporte são reconhecidas formalmente? Ex. envio de e-mail marketing, convite para cofee-breaks, etc.	Não
	A estratégia possui relatório de utilização tecnológica a fim de identificar por que canais as solicitações costumam vir e com que frequência?	Não
	A estratégia do suporte possui relatório de soluções que foram realizadas remotamente, como meio de comparação com atendimento presencial?	Não
	É possível extrair relatórios de telefonia do cliente?	Não
	A estratégia do suporte possui acesso a relatórios estatísticos de telefonia?	Não
	A equipe de suporte de campo realiza atendimento proativo periodicamente?	Não
	Os serviços são separados por requisição, incidente, problema e mudança, de modo que possam ser geradas estatísticas coerentes?	Não
	A equipe de suporte de nível 1 possui um processo de escalação definido com a respectiva matriz de responsabilidade?	Não
	A equipe de suporte de nível 2 possui um processo de escalação definido com a respectiva matriz de responsabilidade?	Não
	Os níveis (1 e 2) informam o usuário quando uma requisição está sendo escalada para outro nível de atendimento que não seja o dele?	Não
	A estratégia do atendimento possui matriz de métricas gerenciais e operacionais e as mesmas estão divulgadas para os técnicos?	Não
	Os incidentes/requisições que são fechados possui link correspondente da solução para Base de Conhecimento?	Não
	A estratégia do suporte possui acesso a relatórios de KPI's da gestão de mudança? Ex. quantas falharam, não autorizadas, com sucesso, etc.	Não
	O suporte possui relatório ou acesso aos relatórios de IC's que apresentam maior número de incidentes?	Não
	Realiza gerenciamento de ativos do cliente, incluindo inventário de software?	Não
	Utiliza a técnica S.M.A.R.T (Específico, Mensurável, Atingível, Relevante e	Não

	Atrelado a tempo) para elaborar KPI's de atendimento?	
	Possui um relatório matinal padrão enviado para os stakeholders, contendo um dashboard operacional do dia anterior?	Não
	Realiza pesquisa de satisfação definindo o público alvo e quem se quer atingir?	Não
	Possui histórico e planejamento futuro das pesquisas de satisfação?	Não
	Possui planilha de S.I.P?	Não
	Possui relatório de GAP's da equipe do centro de suporte?	Não
	Realiza comparação dos GAP's com as melhores práticas do mercado	Não
	Possui relatório de GAP's de conhecimento e habilidades da equipe do centro de suporte?	Não
	Realiza uma previsão de treinamento com base nos GAP's de conhecimento?	Não
	Possui plano de substituição do supervisor?	Não
	Possui histórico das notas das avaliações ou provas realizadas durante o processo de contratação dos candidatos?	Não
	Possui plano de contingência dos técnicos do atendimento?	Não
	Os usuários possuem a opção de instalar programas básicos utilizando o método self-service e autoatendimento?	Não

9.2. **Resultados Gráficos:**

Item	ADERÊNCIA AOS ITENS	PERCENTUAL
1	Ambiente físico e segurança física	26%
2	Antivírus	0%
3	Monitoração e Operação	60%
4	Armazenamento Corporativo	60%
5	Virtualização	60%
6	Serviço de diretório e autenticação	60%
7	Correio Eletrônico	55%
8	Windows Server	80%
9	Windows Clients	0%
10	Atualização de sistemas de estações	50%
11	Ambiente de rede	60%
12	Segurança	50%
13	Backup	25%
15	Atendimento	20%
GLOBAL		48%

10. **INVENTÁRIO DE NECESSIDADES**

As necessidades de TI foram identificadas e definidas as prioridades em conformidade com a Portaria nº 40, de 11 de maio de 2021.

Após a identificação das demandas, os projetos foram priorizados aplicando-se a Matriz GUT (Gravidade, Urgência e Tendência) na qual foi atribuída a pontuação 1, 3 e 5 em cada uma das características e multiplicados os valores atribuídos. O maior resultado dessa multiplicação representa o projeto de maior prioridade, em que:

Gravidade: representa o impacto do problema analisado caso ele venha a acontecer. É analisado sobre aspectos, como: tarefas, pessoas, resultados, processos, organizações etc. Analisam seus efeitos a médio e longo prazo, caso o problema em questão não seja resolvido. "Se não resolver o problema agora, qual será o impacto em minha organização?"

Tendência: representa o potencial de crescimento do problema, a probabilidade do problema se tornar maior com o passar do tempo. É a avaliação da tendência de crescimento, redução ou desaparecimento do problema. "Se eu não resolver esse problema agora, ele vai piorar pouco a pouco ou vai piorar bruscamente?"

Urgência: tempo disponível ou necessário para resolver o problema. Quanto maior a urgência, menor será o tempo disponível para resolver o problema. "A resolução deste problema pode esperar ou deve ser realizada imediatamente? "

Pontos	Gravidade	Urgência	Tendência
5	Quando estiver alinhada às ações do Planejamento Estratégico	É necessária uma ação imediata no ano corrente	Se nada for feito, haverá um grande e imediato agravamento
3	Quando impactar no desenvolvimento de pessoas e processos	É necessária uma ação mais cedo possível	Se nada for feito, haverá um agravamento em médio prazo
1	Quando impactar melhorias pontuais	Pode esperar	Não irá mudar

Em função do inventário de necessidades, seguem abaixo as informações mapeadas e priorizadas:

Inventário de Necessidades de TIC DA SMDF						
Item	Atividade	Justificativa	MATRIZ GUT			Pontuação GUT
			Gravidade	Urgência	Tendência	
1	Aquisição de Computadores / mouses / teclados/ monitores	Os Equipamentos de hoje, estão fora da garantia, sem reposição de peças, não confiáveis.	5	5	5	125
2	Aquisição Pacote office	Aplicativo de escritório para uso dos servidores.	5	5	5	125
3	Modernização e ampliação do parque tecnológico e da infraestrutura	Modernização e Ampliação do atual parque de TI.	5	5	5	125
4	Contratação de Outsourcing de impressão (Impressora preto/branco e colorido)	Equipamento essencial para o trabalho dos servidores.	5	5	5	125
5	Contratação de Fábrica de software – Desenvolvimento de sistemas	Manter os processos internos de TI mapeados, formalizados, mensurados e otimizados, bem como o desenvolvimento de sistemas para as áreas fim.	5	5	5	125

6	Contratação de Software para videoconferência	Visa atender as necessidades da Secretaria para reuniões entre equipes e demanda de programas existentes.	5	5	5	125
7	Contratação de Software de apoio à aprendizagem, executado num ambiente virtual	Ferramenta para auxiliar a implementação de Programas da SMDF no armazenamento de cursos online, bem como a possiblidade de grupos de trabalho e comunidades de aprendizagem dentro da própria Secretaria.	5	5	5	125
8	Contratação de Sistema de emissão de folha de frequência dos servidores	O Sistema automatizado de emissão das folhas de frequência dos servidores desta Secretaria que importe informações do SIGRH tais como ABONOS, FÉRIAS, LICENÇAS MÉDICAS, PRÊMIO, MATERNIDADE, entre outras.	5	5	3	75
9	Aquisição de Equipamentos para videoconferência (web cams, headsets, equipamentos similares)	Em tempos de pandemia as reuniões e atendimentos virtuais se acentuaram, equipamentos de videoconferência se tornaram primordiais para o cotidiano.	5	5	3	75
10	Aquisição de Notebook	Atender a reuniões, apresentações, cursos, eventos, palestras.	5	3	5	75
11	Aquisição de Tv corporativa/ Video Wall	Canal de comunicação que utiliza TVs profissionais localizados em pontos estratégicos das unidades da SMDF, trazendo informações úteis sobre a secretaria e sobre o público que a Secretaria atende, pode ser utilizado de diversas maneiras, feed de noticiais, anuncio de senhas, informativos, etc.	5	3	5	75
12	Contratação de Monitoramento por câmeras	Proporcionar segurança para o patrimônio da SMDF e usuários atendidos	5	3	5	75
13	Aquisição de Tablets	Busca ativa, Mobilidade.	5	3	5	75
14	Aquisição de Caixa de Som e microfones	Eventos, apresentações e reuniões.	5	3	5	75
15	Contratação de redes moveis (chips/modens)	Para ser utilizado nos tablets/notebooks nas unidades moveis da SMDF	5	3	5	75
16	Aquisição de Rede sem fio	Notebooks, celulares, impressoras, instalação de rede em locais provisórios.	5	3	5	75
17	Aquisição de Impressora térmica	Emissão de senhas de espera e comprovante de qualidade de atendimento.	5	3	5	75
18	Contratação de Voip com central telefônica em nuvem	Melhoria nos serviços de telefonia.	3	5	5	75
19	Aquisição de Certificado digital	Assinatura de contratos e convênios.	5	3	5	75
20	Aquisição de Antivírus	Segurança da rede e dos dados.	5	3	5	75
21	Aquisição de Softwares de automação de marketing	Ferramenta para auxiliar a implementação de Programas da SMDF na demanda de captação de leads, permitindo a automação no envio de novas oficinas e cursos e a eficiência na entrega da informação (cursos, oficinas, programas, empregos).	3	5	3	45
22	Aquisição de Switches	Atualização e ampliação da rede.	3	3	3	27
23	Contratação de Projetor e tela de multimídia	Atender a reuniões, apresentações, cursos, eventos, palestras, etc.	3	3	3	27
24	Aquisição de Ferramenta de BI	Gestão de informação.	3	3	3	27
25	Consultoria para gestão e mapeamento de processos de trabalho	Otimização dos processos internos de trabalho.	5	1	1	5
26	Aquisição de Equipamento de áudio/vídeo	Instrumentos e equipamentos necessários para desenvolver os serviços de comunicação interna e externa.	3	1	1	3
27	Aquisição de Câmera fotográfica profissional	Serviços da área de comunicação e eventos.	1	3	1	3
28	Aquisição de Software Visio	Fluxogramas, organogramas, projetos.	3	1	1	3
29	Aquisição de Software Adobe in Design	Ferramenta com finalidades editoriais e tipográficas para ASCOM.	3	1	1	3
30	Aquisição de Software Bizagi	Modelagem de processos.	3	1	1	3
31	Aquisição de Software Photoshop	Ferramenta utilizada para edição de imagens Para Ascom.	3	1	1	3
32	Aquisição de Software Autocad	Auxiliar na elaboração de projetos na parte de logística e engenharia.	3	1	1	3
33	Aquisição de Software Volare	Auxiliar na elaboração de projetos na parte de logística e engenharia.	3	1	1	3
34	Aquisição de Software CorelDraw	Auxiliar a logística e Assessoria de Comunicação.	3	1	1	3
35	Contratação de empresa para emissão de crachás	Identificação de servidores.	3	1	1	3
36	Aquisição de Rack para Switches	Organização e segurança dos equipamentos de rede.	1	1	1	1
37	Aquisição de Software Msproject	Serviços internos de elaboração de projetos	1	1	1	1
38	Aquisição de Nobreaks	Estabilidade da rede, dos servidores e dos equipamentos.	1	1	1	1
39	Aquisição de Ônibus itinerante	ÔNIBUS equipado com equipamentos de TI (computadores, rede sem fio, internet, impressora).	1	1	1	1
40	Aquisição de Computador integrado touch screen	Terminais de autoatendimento para suportar os sistemas de emissão de senhas e de registro de qualidade de atendimento	1	1	1	1
41	Aquisição de Equipamentos de gravação de vídeo em estúdio, como câmeras de	Possibilita a profissionalização de criação de vídeos para fins educacionais, vídeo aulas e videoconferências.	1	1	1	1

	vídeo, microfones, iluminação, entre outros					
42	Contratação de ponto eletrônico	Controle das jornadas de trabalho	1	1	1	1

11. PLANO DE GESTÃO DE RISCOS

O Plano de Gestão de Riscos visa identificar os riscos inerentes à inexecução parcial ou total do PDTIC, medidas preventivas, contingências e os responsáveis pela adoção dessas medidas.

O Plano busca apresentar os riscos reais, relevantes e prováveis, além de estabelecer medidas de prevenção e de contingência, que sejam possíveis e eficazes, conforme tabela abaixo:

Riscos	Medidas Preventivas	Medidas de Contingência	Resp
Defasagem tecnológica do ambiente computacional da SMDF	Realizar atualizações periódicas na capacidade dos atuais equipamentos.	Não há	SUAG/
Exposição a furtos de equipamentos e periféricos dentro das instalações da Sede	Otimizar protocolo de entrada e saída de equipamentos.	Não há	SMDF
Queda da qualidade e disponibilidade dos serviços impressão	Realizar gestão no contrato existente, atentando-se para prazo de vigência, qualidade nos serviços prestados e valores praticados. Iniciar um novo processo licitatório em tempo hábil.	Não há	SUAG/
Falta de planejamento para realização dos projetos de TI	Alinhar as iniciativas de TI ao PEI/SMDF, ao PDTIC e orçamento anual.	Não há	SUAG/
Falta de comprometimento da alta gestão com inciativas de TI	Sensibilização dos gestores da SMDF para a estruturação da área de TI.	Não há	Grupo
Falta de pessoal com conhecimento em TI para desenvolvimento dos projetos na SMDF	Contratação de profissional conhecedor da área de TI.	Não há	SUAG
Baixa qualidade dos serviços terceirizados	Edital com exigências de qualidade dos serviços que serão prestados. Níveis de acordo de serviço estabelecidos.	Não Há	DITEC/
Falta de priorização orçamentária para realização dos projetos contemplados no PDTIC.	Previsão orçamentária anual que contemple as demandas de TI; Utilização correta dos recursos alocados; Alocar os recursos para cumprir os projetos prioritários estabelecidos no PDTIC.	Não Há	SUAG/

12. POLÍTICAS, NORMAS E PROCEDIMENTOS

12.1. Este tópico compreende em normatizar o uso de equipamentos e dispositivos de informática dentre as particularidades da Secretaria de Estado da Mulher do Distrito Federal, no nível da Administração Pública. Do Monitoramento e da Auditoria do Ambiente, obedecendo aos seguintes padrões:

PADRÃO	DESCRIÇÃO
ITIL - Information Technology Infrastructure Library.	Conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de tecnologia da informação (TI).
Decreto Nº 33.528/2012	Art. 2º A partir da publicação deste Decreto os órgãos da Administração Direta e Indireta têm prazo de 120 dias para a elaboração e publ Diretor de Tecnologia da Informação – PDTIC. Parágrafo único. Cabe ao Comitê Gestor de Tecnologia da Informação e Comunicação a orientação aos órgãos, em caso de dúvida, e a apr Diretor de Tecnologia da Informação, conforme Decreto nº 33.050, de 19 de julho de 2011.
Instrução normativa IN Nº 04 de 12 de novembro de 2010 – SLTI	Art. 3º em consonância com o art. 4º do Decreto nº 1.048,de 1994, o órgão central do SISP elaborará, em conjunto com os órgãos setoria a Estratégia Geral de Tecnologia da Informação - EGTI para a Administração direta, autárquica e fundacional do Poder Executivo Federal, anualmente, para servir de subsídio à elaboração dos PDTIC pelos órgãos e entidades integrantes do SISP." Art. 4º As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, elaborado em harmonia com o P estratégia do órgão ou entidade.
Estratégia Geral de Tecnologia da Informação 2011-2012	Estabelece metas de curto e médio prazo a serem cumpridas pelos órgãos e entidades do Governo do Distrito Federal, em diferentes per propõe a mensuração objetiva de resultados por meio de indicadores. Incentiva a elaboração do PDTIC e promove a troca de informaçõe conhecimento e desenvolvimento colaborativo entre os órgãos que compõem o GDF.
Comitês Gestores	Status legal: Decreto nº 33.050 de 19 de julho de 2011, publicado no DODF em 20 de julho de 2011. Portaria nº 71 de 12 de agosto de 20 agosto de 2011. EGTI publicada através do decreto nº 33.528 de 10 de fevereiro de 2012, publicado no DODF em 13 de fevereiro de 2012 * Comitê coordenado pela Casa Civil

12.2. POLÍTICAS GERAIS

12.2.1. SEGURANÇA DA INFORMAÇÃO E RISCO OPERACIONAL

O termo "segurança computacional" abstrai a avaliação de risco que os usuários da SMDF possuem sobre a possibilidade de redução ou aumento no valor de alguns de seus bens como decorrência da utilização dos meios eletrônicos de armazenamento, processamento e comunicação para acesso às informações.

Entre os bens a preservar, destacamos a integridade das informações do público atendido por esta Secretaria. As informações são pautadas em:

Confidencialidade: toda informação mantida em equipamentos sob responsabilidade da SMDF só pode ser acessada por pessoas formalmente identificadas e autorizadas.

Integridade: toda informação trocada de/para a SMDF deve manter seu conteúdo inalterado desde o momento que deixa a origem até chegar ao seu destino, independente dos recursos utilizados na comunicação.

Autenticidade: a origem e o destino das mensagens devem pertencer a autores legitimamente identificados nos sistemas de origem e destino.

Disponibilidade: o acesso à informação deve ser possível para o conjunto da comunidade autorizada, a qualquer tempo e sem degradação no desempenho.

Contabilidade: toda informação com origem ou destino em sistemas legados provido pela SMDF, ou que trafega utilizando-se de infraestrutura de comunicação da mesma, estará sujeita a auditoria para identificação de seus autores, tempo e meios utilizados, durante um período definido em lei.

13. ARQUITETURA TECNOLÓGICA/ARQUITETURA DA INFORMAÇÃO

13.1. SISTEMAS CORPORATIVOS

NOME	DESCRIÇÃO	SGBD	INTERNET	LINGUAGEM	SITUAÇÃO
SEI	Sistema Eletrônico de Informações.	Outros	Sim	HTML	Em uso
SIGGO	Sistema Integrado de Gestão Governamental, mantido pelo GDF.	Outros	Não	Outras	Em uso
SISGEPAT	Sistema Geral de Patrimônio – para controle do patrimônio utilizado na SMDF, mantido pelo GDF.	SQL Server	sim	Outras	Em Uso
SIGRH	Sistema Integrado de Gestão de Recursos Humanos, para controle e gestão dos Recursos Humanos da SMDF, mantido pelo GDF.	Outros	Sim	Outras	Em Uso

Site Corporativo	Site que apresente informações para o público interno e externo, agregando várias informações, serviços e notícias.	SQL Server	Sim	WordPress	Em Uso

13.2. **SOFTWARES HOMOLOGADOS**

Tipo	Nome
Sistema Operacional	Windows 10 Professional 64 bits, Windows 8 Professional 64 bits,
Leitura de PDF	Acrobat Reader, PDF Xchanger Editor, Reduce PDF Size, PDF TRT 14
Comunicador Instantâneo	Whatsapp
Pacote de Escritórios	MS Office Professional 2007 e 2013
Navegador de Internet	Mozilla Firefox, Google Chrome
Aplicativo de E-mail	Outlook Microsoft Exchange 2007 e 2013
Compactador de arquivo	7-zip
Acesso remoto à rede	Ultravnc

13.3. **REDES**

Item	Quantidade
Switchs de marcas variadas	5

13.4 **DISPOSITIVOS**

Item	Quantidade
Computadores	226
Notebook marcas variadas	4

14. FATORES CRÍTICOS DE SUCESSO

Para que o PDTIC da SMDF alcance o sucesso pretendido, faz-se necessário que todas as ações de TI estejam alinhadas com o Planejamento Estratégico da SMDF.

Posto isto, é necessário o acompanhamento e controle para evitar que hajam ações paralelas não relacionadas aos objetivos estratégicos.

O reduzido número da equipe de TI da SMDF é fator crítico para o sucesso do PDTIC, além da criação das áreas especializadas.

15. CONSIDERAÇÕES FINAIS

Uma preocupação constante da gestão, é a busca pelo alinhamento estratégico entre a área de Tecnologia da Informação e o plano negócio da instituição, como forma de atender à demanda pelo aumento da qualidade dos serviços, economia, confiabilidade, flexibilidade, agilidade e racionalização dos fluxos de trabalho da Organização.

O processo de automação e informatização das atividades operacionais e administrativas das organizações públicas e privadas vem tornando-as cada vez mais dependentes de sua infraestrutura tecnológica.

As metas definidas para a área de TI devem estar alinhadas ao planejamento estratégico das organizações e refletidas em seu Plano Diretor (PDTIC).

Diante desta necessidade a SMDF criou uma comissão com a atribuição de propor o Plano Diretor de TI, aprovar os programas de ação a serem desenvolvidos e acompanhar a sua execução.

Foi possível identificar e registrar no PDTIC as reais necessidades que representam o pensamento estratégico da Secretaria.

A elaboração dessa primeira versão do PDTIC permitiu que a SMDF, identificasse os problemas e soluções para a melhoria do processo de elaboração das versões posteriores.

16. GLOSSÁRIO

Governança de TI: “Governança de TI é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios.” (Professor da FGV Sr. João R. Peres).

BSC (Balanced Scorecard): metodologia de medição e gestão de desempenho, desenvolvida pelos professores da Harvard Business School, Robert Kaplan e David Norton, em 1992. O BSC foi definido, inicialmente, como um sistema de métrica do desempenho e posteriormente como um instrumento de gestão estratégica.

COBIT (Control Objectives for Information and related Technology): framework que tem por objetivo apresentar boas práticas de processo e apresentar atividades numa estrutura lógica e gerenciável. Essa boa prática tem por objetivo organizar a TI, tornado possível seu alinhamento com os requisitos de negócio.

ITIL (Information Technology Infrastrucure Libray): conjunto de melhores práticas que orientam o gerenciamento de serviços de TI. Consiste de publicações que fornecem recomendações para prover serviços de TI com qualidade.

Melhores Práticas: Atividade ou processo provado usado com sucesso por múltiplas organizações. (fonte: COBIT).

SWOT: A Análise SWOT é uma ferramenta utilizada para fazer análise de cenário (ou análise de ambiente), sendo usada como base para gestão e planejamento estratégico de uma corporação ou empresa, mas podendo, devido a sua simplicidade, ser utilizada para qualquer tipo de análise de cenário.

GUT: Técnica para priorizar projetos/demandas/atividades, na qual “G” significa Gravidade e explicita em diferentes graus os prejuízos ou dificuldades decorrentes do fato de não se atender à necessidade. O “U” significa Urgência e explicita a tempestividade em se atender a demanda. O “T” significa Tendência e explicita a busca pela resposta do que irá acontecer se nada for feito para atender à necessidade.

Data Center: local onde os computadores (servidores) são armazenados.

DLP: “Data Loss Protection”. São soluções completas que baseadas em políticas centralizadas, identificam, monitoram e protegem os dados.

IPS: "Intrusion Prevention System" ou sistema de prevenção de invasão/ataque.

IDS: "Intrusion Detection System" ou sistema de detecção de invasão. O IDS informa sobre um potencial ataque.

Antivírus: Programas de computador concebidos para detectar e principalmente eliminar códigos maliciosos dos computadores.

Backup: é o processo de cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais.

Service Desk: Serviço de apoio a usuários para suporte e resolução de problemas técnicos.

GED: Gerenciamento Eletrônico de Documentos ou Gestão Eletrônica de Documentos. Conjunto de tecnologias que permite a uma empresa gerenciar seus documentos em forma digital.

Firewall: dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra (invasão), protegendo assim os recursos de hardware e software.

De acordo:

Secretária Executiva – VANDERCY ANTONIA DE CAMARGOS

Subsecretária de Administração Geral – REJANE PARENTE LUCAS

Subsecretária de Enfrentamento à Violência Contra as Mulheres – IRINA ABIGAIL TEIXEIRA STORNI

Subsecretária de Politicas para Mulheres – FERNANDA FIGUEIREDO FALCOMER MENESES

Diretor de Tecnologia da Informação e Comunicação – RODRIGO MARCELINO DA SILVA

Documento assinado eletronicamente por **VANDERCY ANTONIA DE CAMARGOS - Matr.0273720-5**, **Secretário(a) Executivo(a)**, em 28/07/2021, às 14:04, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **REJANE PARENTE LUCAS - Matr.0279026-2**, **Subsecretário(a) de Administração Geral**, em 28/07/2021, às 14:09, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **RODRIGO MARCELINO DA SILVA - Matr.0277417-8**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 28/07/2021, às 14:34, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **IRINA ABIGAIL TEIXEIRA STORNI - Matr.0274393-0**, **Subsecretário(a) de Enfrentamento à Violência Contra as Mulheres**, em 28/07/2021, às 14:39, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **FERNANDA FIGUEIREDO FALCOMER MENESES - Mat. 0278092-5**, **Subsecretário(a) de Promoção das Mulheres**, em 28/07/2021, às 14:52, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **66568365** código CRC= **825AB55A**.