SERVIÇO PÚBLICO ESTADUAL

PROCESSO: E-26/011/1095/2015

DATA:29/05/2015 FLS.:

RUBRICA: ID 5023389-0

Governo do Estado do Rio de Janeiro
Secretaria de Estado de Fazenda e Planejamento
Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – PRODERJ

DIRETORIA DE INFRAESTRUTURA TECNOLÓGICA

RIO DIGITAL

TERMO DE REFERÊNCIA

1. APRESENTAÇÃO DO RIO DIGITAL

Este documento apresenta as funcionalidades do projeto Rio Digital.

1.1. Este documento apresenta o projeto Rio Digital que consiste numa arquitetura de serviços de Tecnologia da Informação e Comunicação, Segurança da Informação e Monitoramento de disponibilidade de ativos e ameaças cibernéticas suportados e geridos por uma Gestão Integrada e Inteligente, permitindo uma governança dos serviços oferecidos aos órgãos do Governo do Estado do RJ. Os serviços citados serão contratados via certame licitatório. A seguir, será detalhado cada um destes serviços, os quais podem ser vistos de forma macro na figura1 abaixo.

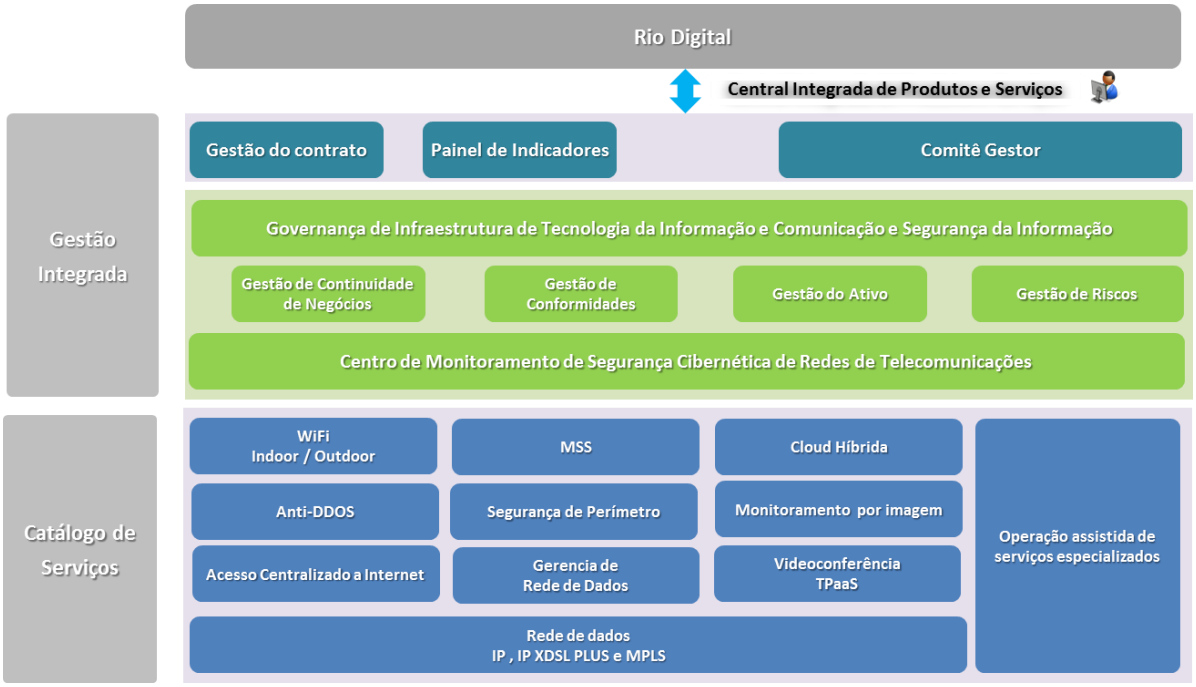


Figura 1 – Arquitetura de Gestão Integrada e Catálogo de Serviços

1.2. O RIO DIGITAL se justifica pela necessidade da utilização de novos serviços pelas Instituições do Governo do estado, acompanhando a crescente evolução tecnológica mundial e do uso da Internet, possibilitando a utilização de novas soluções tecnológicas, como as disponibilizadas em Nuvem, facilitando o desempenho de suas atribuições bem como a melhora contínua dos serviços prestados à população.

1.3. O RIO DIGITAL não se limita a aquisição somente de uma Rede de Dados, mais de uma Rede que engloba Serviços de Telecomunicações, Informação e Gestão Integrada.

2. ARQUITETURA DOS SERVIÇOS

2.1. A arquitetura de serviço é composta de um módulo gestor, denominado de Gestão Integrada que atuará no provisionamento gestão e suporte de todo e qualquer serviço contratado.

2.2. O módulo integrante, denominado Catálogo de Serviços, contém todos os serviços, processos e suas respectivas infraestruturas disponíveis para os serviços de Tecnologia da Informação e Comunicação e Segurança Informação contratados.

2.3. O módulo de Catálogo de Serviços obtém todos os mecanismos de gestão operacional a partir da utilização dos serviços de Gestão Integrada, por isso faz-se necessária à implementação dos módulos de Gestão Integrada para o perfeito funcionamento do catálogo de serviços.

2.4. Os serviços integrantes do Catálogo serão obrigatoriamente suportados pela estrutura de Gestão de Integrada, composta pelos seguintes módulos:

- Gestão de Contrato
- Painel de Indicadores
- Comitê Gestor
- Governança de Infraestrutura de Tecnologia da Informação e Comunicação e Segurança Informação
- Gestão de Continuidade de Negócios
- Gestão de Conformidades
- Gestão de Ativos
- Gestão de Riscos
- Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações

2.5. Os serviços serão contratados conforme disponibilidade na tabela de formação de preços de serviços do edital da licitação.

2.6. Os módulos de Gestão Integrada e de Catálogo de Serviços serão detalhados neste documento.

3. GESTÃO INTEGRADA

3.1. O que é a Gestão Integrada?

- A Gestão Integrada é composta por uma estrutura de Governança estruturada nas melhores práticas de gestão, COBIT, ITIL, ABNT, PMBOK, BPM, ISO/IEC. A gestão Integrada tem como papel fundamental entregar e gerir todos os serviços integrantes do catálogo de forma unificada e com qualidade assegurada durante todo o período do contrato.

- Direcionada por processos é a gestão que permite integrar, nas operações do dia-a-dia os aspectos e os objetivos da Gestão de Continuidade de Negócios, Conformidade, Ativos, Riscos, a Governança de Infraestrutura de TIC e Segurança da Informação e o Centro de Monitoramento de Segurança Cibernética.

- Essa estrutura será a interface principal entre a Contratada e o Contratante provendo indicadores de gestão, e suporte ao Comitê Gestor que garantirá a fluidez da comunicação entre todos os usuários dos serviços contratados.

3.2. Dentre diversos benefícios da Gestão Integrada, podemos citar:

- Melhoria de qualidade em produtos e serviços;
- Realização de objetivos e metas da Contratante;
- Economia de tempo e custos;
- Transparência dos processos e procedimentos internos;
- Maior controle dos riscos;
- Assegurar às partes interessadas o comprometimento com uma gestão operacional demonstrável;
- Redução e controle de custos operacionais
- Oportunidades para conservação de recursos e energia;
- Melhoria do relacionamento com todas as partes interessadas (fornecedores, governo municipal, estadual e federal e os funcionários da Contratante);
- Prevenção de falhas ao invés de suas correções

3.3. CONTEXTUALIZAÇÃO DOS PROCESSOS DE GESTÃO E SERVIÇOS DA GESTÃO INTEGRADA

3.3.1. Segue abaixo a contextualização da Governança de Infraestrutura de Tecnologia da Informação e Comunicação e Segurança da Informação

- A velocidade da comunicação é fator crítico de sucesso nas organizações. Um número cada vez maior de pessoas divulgam instantaneamente comunicados, fotos e vídeos sobre situações que vivenciam sobre sua empresa (a favor ou contra). O uso de uma boa infraestrutura de Tecnologia da Informação e Comunicação (TIC) está deixando de ser diferencial competitivo, para se tornar um serviço básico.

- A infraestrutura de TIC está relacionada às plataformas de telecomunicações, hardware, às instalações físicas, de redes de telecomunicações e às pessoas que serão responsáveis por executar diferentes tarefas e papeis correspondentes aos processos de TIC. Tão importante como estabelecer a arquitetura, é desenvolver os serviços necessários que atendam às necessidades do negócio, o modelo corporativo de dados, além de atingir os objetivos definidos para cada processo. E é aí que entra a definição dos recursos de TIC, do hardware e das capacidades e habilidades requisitadas para que os processos de infraestrutura possam ter uma gestão operacional eficiente e produzir bons resultados.

- A governança da infraestrutura de TIC e a garantia da segurança da informação é condição obrigatória para subsidiar a velocidade com que a Contratante percebe mudanças de cenário, toma decisões que permitam gerar maior interação com seu público-alvo, atendendo às suas necessidades, e garantindo transparência das informações.

- Para o cumprimento dos requisitos de implantação dos serviços de Governança de Infraestrutura de TIC e Segurança da Informação em redes de telecomunicações, deve-se adotar métodos e boas práticas de gestão de projetos, como um Escritório de Projetos (PMO) e de gestão de processos de negócio (BPM).

- O Escritório de Projetos (PMO) é uma entidade organizacional à qual são atribuídas várias responsabilidades relacionadas ao gerenciamento centralizado e coordenado dos projetos sob seu domínio.

- Dentre diversos benefícios de um Escritório de Projetos, podemos citar:
  - Promover um ambiente em que a tomada de decisão colaborativa é mais fácil e mais frutífera;]

  - Minimizar os riscos para projetos individuais em termos de impactos nos negócios;

- Certificar que os recursos humanos são focados no controle e na eficiência;
- Comprovar que o sucesso não acontece somente hoje, mas é mais provável com iniciativas futuras do projeto;
- Gerir a implantação de serviços coincidentes dentro do projeto Rio Digital.

- Aliado ao gerenciamento de projetos, a gestão adequada dos processos de trabalho é fundamental para o alcance dos objetivos de uma organização e atendimento de seu público-alvo.

- Dentre diversos benefícios da Gestão de Processos de Negócio, podemos citar:
  - Permite que os colaboradores da Contratante executarem suas atividades com segurança operacional;
  - Permite uma visão sistêmica dos processos – já que todos estarão disponíveis para consulta;
  - Maior qualidade e agilidade nas informações para tomada de decisão da gestão operacional;
  - É possível automatizar tarefas, através do mapeamento de processos;
  - Simplificar processos gerenciais;
  - Buscar grandes melhorias, não apenas incrementais, através da melhoria continua de mapeamento de processos;
  - Aproximar o funcionamento da organização à forma natural, e por isso mais eficiente e eficaz;
  - Identificar e solucionar problemas e implementar melhorias;
  - Facilitar a consistência e comunicação da arquitetura organizacional;
  - Auxiliar na identificação de inconsistências, duplicidades e omissões;
  - Possibilitar a visualização de interação com entidades externas.

- Com a presente contratação, pretende-se que a execução dos projetos seja controlada adequadamente e que os processos de negócios afetados pela implementação de serviços de Governança de Infraestrutura de TIC e Segurança da Informação em redes de telecomunicações sejam devidamente mapeados e ajustados.

- Desta forma garantiremos o fornecimento de serviços de forma unificada e integrada e com gestão operacional por todas as camadas integrantes do objeto dessa contratação mencionada no edital.

- Dentre diversos benefícios da Governança de Infraestrutura de TIC, podemos citar:
  - Garante segurança, disponibilidade e confiabilidade, fazendo com que a empresa tenha credibilidade perante funcionários, clientes e sociedade;
  - Garante controle efetivo das informações, pois irá minimizar riscos de TIC e

consequentemente do Negócio;

- Automatiza tarefas específicas que passam a ser realizadas em menos tempo, resultando na diminuição do custo, da monotonia de executar tarefas repetitivas, na melhora do processo produtivo (por focar as tarefas mais importantes), obtendo maior produtividade e aumento da competitividade;
- Auxilia a equipe técnica do Contratante a testar algumas decisões antes de colocá-las em prática, propiciando decisões de qualidade, podendo antecipar os problemas e formular soluções;
- Redução de custos e agregação de valor ao negócio do Contratante, pois com processos e atividades mapeados de forma adequada, o Contratante terá economia de tempo e dinheiro.

3.3.2. Segue abaixo a contextualização da Gestão de Continuidade de Negócios

- O escopo do projeto desta proposta se constituiu na implantação de uma infraestrutura de Telecomunicações de rede de longa distância de dados de alta performance, abrangendo todas as localidades das Secretarias e demais órgãos públicos do Governo do Estado do Rio de Janeiro.

- O projeto teve como uma das suas premissas básicas, a de propiciar condições para o aumento de integração e produtividade dos órgãos públicos ao desempenhar suas atribuições, permitindo aos cidadãos a obtenção de informações e o uso dos serviços de governo com maior agilidade, bem como facilitando a interação entre órgãos de governo e destes com a sociedade.

- Em virtude de se tratar de infraestrutura crítica de redes de telecomunicações do Governo do Estado do RJ, que atende as Secretarias que fazem o atendimento aos cidadãos, faz-se necessário a implantação de um serviço de Gestão de Continuidade de Negócios, para garantir que este serviço continue a operar em caso de um incidente grave.

- Um incidente significativo que cause interrupção não programada nos processos da infraestrutura de telecomunicações do Governo do RJ pode trazer impactos devastadores para a sociedade. A resposta a este incidente requer a mobilização de toda a equipe técnica da Contratada, de forma estruturada, rápida e concisa para diminuir ou evitar os impactos negativos. A Gestão de Continuidade de Negócios, cria e mantém atualizado e disponível planos e procedimentos necessários para uma recuperação efetiva, minimizando os impactos para o Governo do RJ.

- A Gestão de Continuidade de Negócios é um processo abrangente que irá identificar as ameaças potenciais para a infraestrutura de Telecomunicações do Governo do RJ e os possíveis impactos nas operações de negócio caso estas

ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a imagem do Governo do RJ e suas atividades de valor agregado.

- Os principais benefícios que a Gestão de Continuidade de Negócios pode propiciar para o Governo do RJ estão descritos a seguir:
    - Identificação proativamente dos impactos e responder eficientemente às interrupções nos processos de negócio.
    - A equipe técnica estará preparada para tratar incidentes na interrupção de processos de negócios críticos.
    - Tendo uma estrutura comum com outros sistemas de gestão, qualidade ou segurança da informação, por exemplo, haverá confiança de que no evento de uma interrupção a organização saberá contornar essa situação sem sofrer prejuízos.
    - Ter planos de continuidades em vigor na organização irá permitir que se atue no tratamento de desastres ou crises que possam abalar a imagem corporativa.
    - Redução de custos através de impacto atenuante de desastres. Diminuindo o impacto desses eventos, consequentemente o prejuízo da organização é menor.
    - Fornece um método exercitado da sua habilidade em prover produtos e serviços em um nível e nos limiares de tempos acordados, para permitir que a organização continue a manter seus negócios após uma disrupção organizacional, ou seja, um desastre.
    - Vantagem competitiva com entrega de produtos e serviços garantida. Além disso, a cadeia de suprimentos de fornecedores fica assegurada.
- A estruturação do serviço de Gestão de Continuidade de Negócios pode ter um grande esforço, relativo ao tempo em que todas as atividades devem estar prontas para entrar em operação, durante um incidente grave. Por esse motivo é necessário que a Contratada implemente uma solução automatizada para minimizar esse esforço.
- A Contratada deve implementar uma solução automatiza que faça a integração de informações e sistemas de diversos setores e centralizar em uma única plataforma o planejamento de políticas de gestão de riscos; a análise dos impactos dos riscos nos negócios; a avaliação de riscos, estratégias e planos de continuidade; o monitoramento e rastreamento de incidentes; e, mais

importante, integrar os alertas de incidentes às decisões que definem sua Continuidade de Negócios.

- As diretrizes para serem implementadas na solução automatizada estão descritas a seguir:
    - Integração da visão de Riscos à Continuidade de negócios;
    - Inventário de ativos da infraestrutura do escopo da continuidade de negócios;
    - Cadastro dos planos da estratégia de continuidade;
    - Atualização dinâmica dos planos e procedimentos;
    - Apoio a realização de testes e simulações;
    - Conformidade com as normas internacionais e as melhores práticas de mercado;
    - Identificação e remediação de vulnerabilidades e riscos;
    - Automatização da coleta de dados e ganho de produtividade;
    - Gerenciamento e redução dos riscos existentes em ativos tecnológicos;
    - Criação de consultas e relatórios de vulnerabilidades;
    - Importação das vulnerabilidades e ativos tecnológicos;
    - Workflow para tratamento dos riscos e vulnerabilidades.

3.3.3. Segue abaixo a contextualização da Gestão de Conformidades

- Conformidade é o ato de cumprir regras, diretrizes ou controles pré-estabelecidos. A Gestão de Conformidade envolve o controle do cumprimento de boas práticas, leis, padrões, ou normas sejam de mercado ou de governo.
- A necessidade de atender novas regulamentações vem exigindo das organizações esforços frequentes e onerosos na geração de controles e evidências.
- Os gestores do Governo do Estado do RJ possuem o grande desafio de adequar-se a diversos modelos (“frameworks”), tarefa que exige conhecimento e ações específicas para cada padrão ou regulamentação a que o Contratante precisa estar em conformidade.

- A contratada deve implementar uma solução automatizada com uma base de conhecimento com diversos padrões e regulamentações simultaneamente. A partir de uma única solução automatizada deve ser possível avaliar o nível de conformidade com diversas leis e regulamentos da administração estadual, órgãos de controle e com as melhores práticas do mercado de Tecnologia da Informação e Comunicação e Segurança da Informação, entre eles, por exemplo: ISO 27001, ISO 27002, ISO 22301, ISO 55000, Resoluções, Leis, Políticas e Procedimentos Internos do Contratante.

- Os processos implementados no Rio Digital devem ser incluídos na solução automatizada para usufruírem dos benefícios da Gestão de Conformidade.

- A Gestão de Contratos também deve estar integrada a Gestão de Conformidade, para avaliar se as cláusulas dos contratos estão sendo cumpridas pelas empresas contratadas.

- A Gestão de Conformidade deve ser integrada com a Gestão de Riscos e a área de Governança de Ativo, viabilizando a implantação de controles internos para o monitoramento e gerenciamento desses riscos. A integração das áreas de conhecimento de Governança, Riscos e Compliance (GRC) cria um modelo abrangente para a proteção do negócio do Governo do Estado do RJ.

- As diretrizes a serem implementadas na solução automatizada estão descritas a seguir:

    - Deve ter uma console de gerenciamento única para Gestão de Riscos e Conformidade;

    - Possibilidade de avaliação de conformidade com diversos padrões simultaneamente;

    - Gerenciamento dos requisitos de segurança em múltiplas auditorias, eliminando custos redundantes e controles desnecessários;

    - Visão georreferenciada dos Riscos;

    - Repositório central de evidências;

    - Geração automatizada de relatórios técnicos e executivos;

    - Automatização do processo de conformidade.

- Os benefícios na implementação uma solução automatizada de Gestão de Conformidade está descrita abaixo:

    - Automatização de atividades de gestão de conformidade e auditorias, com a geração automática de indicadores de riscos, catálogo de não

conformidades, relatórios, gráficos, métricas, entre outro, obtendo maior velocidade em todo o processo;

- Ambiente Integrado para toda a organização da Contratante com interface web (simplicidade na edição, manutenção e atualização dos dados e informações;
- Suporte total à implementação dos requisitos para Compliance como, por exemplo, a ISO 31000, ISO 27002, ISO 22301 entre outros;
- Redução de custo e tempo na implementação de frameworks e no atendimento às múltiplas auditorias. Auditorias mais eficientes e com menores custos;
- Repositório único de documentos normativos do Contratante;
- Redução do risco regulatório;
- Facilidade para prestação de contas para a sociedade e para os órgãos de controle;
- Facilidade de colaboração e integração com outras Secretarias;
- Possibilidade de resultados rápidos;
- Visão georreferenciada de não conformidades de forma lógica e centralizada por meio do Workflow e visualização dos resultados de forma gráfica e em uma única plataforma;
- Conscientização dos colaboradores da Contratante quanto à cultura de gestão e tratamento de riscos e conformidade.

3.3.4. Segue abaixo a contextualização da Gestão de Ativos

- O Governo do Estado do RJ atualmente enfrenta uma revolução no que se refere ao assunto governança. Isso afeta diretamente as práticas de gestão de todas as suas secretarias e instituições diretamente conectadas. A governança foi colocada em evidência e, como consequência, uma grande quantidade de leis e regulamentações estão sendo criadas para forçar a implementação de um ambiente de governança, segurança e controles mais efetivo, garantindo maior transparência e credibilidade dos seus serviços para a sociedade.
- Por meio da implementação de uma solução automatizada a Rio Digital deve ter um Painel de Governança voltado às melhores práticas de mercado, tornando a gestão do ambiente mais organizada, eficiente, produtiva e dinâmica.
- As diretrizes para serem implementadas na solução automatizada estão descritas a

seguir:

- Criar Painel de Governança, interativo e dinâmico;
- Criar indicadores de forma a priorização das ações;
- Fornecer apoio à tomada de decisão por intermédio o envio dos indicadores para o Comitê Gestor do Rio Digital;
- Facilitar a monitoração das atividades por meio de gráficos e painéis automatizados;
- Reduzir custos através da automatização dos processos.

- A Gestão do Ativo deverá descrever as regras de controle de todos os ativos do Rio Digital. Segue abaixo algumas regras, mas não limitado a:
  - Quem está autorizado a solicitar mudanças nos ativos
  - Quem está autorizado a solicitar licenças para os ativos
  - As funções e responsabilidades dos proprietários dos ativos
  - Quem deve implementar controles nos ativos
  - O que deve ser monitorado nos ativos
- O serviço deve ser implementado por meio de uma gestão eficaz, e a gestão de ativos é um ponto crítico dessa implementação, por isso deve-se contemplar a gestão de todo ciclo de vida de um ativo, desde a sua contratação, manutenção e suporte. O gerenciamento leva em consideração o controle e cadastro de informações através de uma solução automatizada para registro de entrada, saída ou modificação.
- O que são ativos?
  - Ativos representam todos os itens da organização onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas, podendo ser um ambiente físico, um processo, uma pessoa e um equipamento de tecnologia. O gerenciamento de ativos é fundamental para priorizar investimentos e concentrar esforços nos ativos mais críticos, que sustentam os processos da organização.
- Uma gestão eficiente de ativos privilegia a rastreabilidade, segurança e qualidade os serviços através de algum tipo de controle. Com o crescimento das organizações isto se torna uma tarefa muito complexa sem um software para este gerenciamento. Uma solução automatizada pode contribuir para uma gestão

eficiente através da tecnologia da informação.

- A Contratada deve implementar o serviço de Gestão de Riscos em conformidade com as diretrizes presente na Norma ABNT NBR ISO 55000:2014 - Gestão de ativos — Visão geral, princípios e terminologia.

- Neste tipo de gestão devem ser considerados todos os controles necessários para garantir o registro de detalhes e valores de um ativo, que devem estar condizentes com os dados registrados na solução automatizada utilizada, e deve garantir o controle de entrada e saída, reposições e reconciliação do balanço do estoque. O Governo do Estado do RJ pode considerar o Ciclo PDCA para criar seu processo de gestão de ativos.

- Para o cumprimento dos requisitos de implantação da Gestão do Ativo deve-se implementar uma solução automatizada que contemple todas as funcionalidades que estão sendo descritas neste documento.

- Uma solução automatizada irá ajudar o Governo do Estado do Rio de Janeiro em automatizar e controlar o processo de gestão de ativos fornecendo inventário para ativos tecnológicos e não tecnológicos, gerenciando os riscos e conformidade com padrões e regulamentações. O sistema deve fornecer de forma gráfica, mapa de relacionamento entre os processos de negócios, sistemas e ativos, fornecendo aos gestores base para priorizar ações e investimentos.

- Os requisitos que uma solução automatizada deve ter estão descritos a seguir:

    - Inventariar os ativos tecnológicos (software e hardware) e não tecnológicos (pessoas, ambiente e processos);

    - Identificar a criticidade do ativo em relação aos processos de negócio que ele suporta;

    - Gerar relatórios automatizados e customizados;

    - Mapear ativos por meio de perímetros;

    - Manter a gestão dos controles e requisitos de conformidade;

    - Manter repositório de evidências;

    - Gerar relatório de ativos, com o Risco, Conformidade e Índice de Segurança permitindo identificar os ativos com maior risco.

- A gestão de ativos é fundamental para priorizar investimentos e concentrar esforços nos ativos mais críticos, que sustentam os processos do Governo do Estado do RJ.

- Desta forma, o Governo do Estado do RJ poderá focar nos maiores benefícios:
    - Rastreabilidade dos ativos;
    - Criação e preservação de um catálogo de ativos preciso;
    - Otimização do uso dos ativos em todo seu ciclo de vida;
    - Aumento da disponibilidade dos ativos;
    - Redução dos custos em reparos e aumento de produtividade;
    - Melhoria do planejamento das ações sob os ativos;
    - Qualidade dos serviços prestados aos clientes;
    - Maximização dos resultados da Contratante;
    - Segurança e conformidade com as regulamentações

3.3.5. Segue abaixo a contextualização da Gestão de Riscos

3.3.5.1. Gestão de Riscos Corporativos e Operacionais

- Em função das exigências da administração estadual, órgãos de controle, conhecer e tratar os riscos deixou de ser uma necessidade técnica e transformou-se em uma questão estratégica para o Governo do Estado do RJ através de suas Secretarias de estado.
- Uma solução automatizada deve prover metodologia sólida e estruturada, alinhada às principais normas e padrões internacionais. Através do ciclo de Gestão de Riscos, que inclui as atividades de inventariar, analisar, avaliar e tratar os riscos, a solução automatizada facilita e automatiza o processo, fornecendo suporte à tomada de decisões.
- Com a solução automatizada deve ser possível obter gráficos e relatórios que permitem ao Contratante comparar a evolução de seus indicadores e estabelecer prioridades para implementação de controles e investimentos.
- Toda e qualquer organização é única, pois possui cultura, valores, diretrizes de conduta, profissionais, processos, sistemas e modelo de gestão específicos. Portanto, é necessário que este ambiente seja entendido e mapeado, e suas vulnerabilidades, fragilidades e controles analisados.
- As diretrizes para serem implementadas na solução automatizada estão descritas a seguir:

o Fornecer um framework comum para gestão de risco e avaliação da conformidade com padrões e regulamentações;

o Gerar indicadores de desempenho e relatórios customizáveis;

o Gerenciar os controles de segurança da informação, fornecendo suporte para múltiplas auditorias, reduzindo custos e eliminando silos;

o Obter visão integrada dos ativos ligados aos processos de negócio do Contratante;

o Apoiar a tomada de decisões, viabilizando a priorização de ações e investimentos;

o Manter inventário de ativos;

o Consolidar informações sobre Análise de Riscos, Conformidade e Continuidade de Negócios;

o Gerar automaticamente relatórios, gráficos e estatísticas;

o Gerar de indicadores de riscos, incluindo índices e métricas;

o Obter visão georreferenciada dos riscos;

o Mapear a evolução dos riscos;

o Apoiar a Gestão da Segurança da Informação e Vulnerabilidades em TIC, Gestão de Riscos Operacionais e Corporativos, e de Centros de Integrados de Operações;

o Gerar de indicadores de riscos para governança.

3.3.5.2. Gestão de Riscos e Vulnerabilidades de Tecnologia da Informação e Comunicação.

- Um dos maiores desafios dos gestores é o fato das organizações conviverem com uma grande quantidade de vulnerabilidades e riscos que comprometem a segurança da informação e só disporem de recursos limitados para gerenciá-los.

- Alcançar o equilíbrio entre investimento, priorização de recursos e segurança é um dos grandes objetivos da implantação de uma Solução Automatizada que irá ajudar ao Contratante a vencer os desafios.

- As diretrizes para serem implementadas na solução automatizada estão descritas a seguir:

o Conhecer os impactos das vulnerabilidades e ameaças sobre a infraestrutura de Tecnologia da Informação e Comunicação;

o Identificar os riscos

o Identificar os controles implementados e não implementados

o Tomar decisões com base em métricas e indicadores;

o Monitorar continuamente os riscos, e agir proativamente para tratar as vulnerabilidades nos ativos de TIC;

o Conhecer as fontes de riscos;

o Implementar workflow e acompanhar o tratamento das vulnerabilidades e riscos.

o Promover uma infraestrutura segura de TIC, em conformidade com as normas internacionais e as melhores práticas de mercado;

o Automatizar a coleta de dados, promovendo um ganho de produtividade;

o Gerenciar e reduzir os riscos existentes em ativos tecnológicos;

o Criar consultas e relatórios para visualizar de forma rápida e objetiva as vulnerabilidades identificadas e suas características, facilitando a tomada de decisões e a priorização de melhorias;

o Importar as vulnerabilidades identificadas;

o Importar automaticamente os ativos tecnológicos do inventário;

o Gerar relatórios customizados de riscos identificados

3.3.6. Segue abaixo a contextualização do Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações.

- Atualmente as ameaças cibernéticas estão presentes em todas as atividades que envolvem sistemas de computador. Cada vez mais aumenta os riscos de intrusão e comprometimento de ativos de informação que utilizam os sistemas conectados em IP. Estas ameaças cibernéticas aos sistemas estão em constante evolução, como por exemplo ataques volumétricos que vem ocorrendo nas conexões via internet. Quando as redes de telecomunicações de missão crítica, como é o caso da Rede de Longa Distância e acesso à internet do Governo do Estado do Rio de Janeiro, se interconectam com outros sistemas baseados em IP, ambos ficam muito expostos a ameaças de segurança cibernética e requerem um gerenciamento de risco proativo.

- Contar apenas com equipamentos de segurança da informação como anti-malware, antivírus, firewalls ou sistemas de detecção de intrusão que examinem o tráfego que atravessa a rede não é mais suficiente. Os sistemas críticos devem estar constantemente monitorizados por técnicos especializados em segurança e devidamente capacitados para detectar, avaliar e responder a eventos de segurança. O monitoramento de segurança cibernético proativo irá contribuir para a Contratante a estar sempre um passo à frente na detecção e redução de ameaças

para manter um ótimo desempenho da rede.

- Visando prover segurança cibernética ao novo backbone MPLS contratado com milhares de pontos de presença (POP) na infraestrutura do Governo do Estado do Rio de Janeiro, algumas medidas e serviços de segurança devem ser observados, a fim de atender aos requisitos Disponibilidade, Integridade, Confidencialidade e Autenticidade das comunicações de dados.

- A Contratada deve adotar boas práticas de configurações de equipamentos, uso de protocolos seguros, gestão de patches e monitoramento contínuo, são alguns dos exemplos. Acompanhamento de gaps de segurança e criação de um planejamento (roadmap) estratégico de segurança são fundamentais para a redução das superfícies de ataques quando tratamos de redes complexas e com múltiplas interligações, como é o caso da rede de telecomunicações do Contratante.

- Uma boa governança de TI com implementação de Política de Segurança da Informação única e padronizada é vital para o sucesso do projeto, pois isso irá permear as decisões desde o estabelecimento da arquitetura, equipamentos, pessoal, capacitações, configurações, restrições e padrões de criptografia.

- Para atingir os objetivos citados nos itens acima, a Contratada deve implementar o serviço de Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações oferecendo uma metodologia integrada para a identificação, a proteção, a detecção, a resposta e a recuperação de redes de Telecomunicações de missão crítica, como é a da Contratante, perante um incidente de segurança cibernética.

- O Centro de Monitoramento acompanha e monitora todas as verticais de serviços monitorados, a fim de detectar perdas de disponibilidades, qualidades de serviços, ataques cibernéticos, contribuindo assim para uma rápida priorização e tratamentos de incidentes em rede.

- Outrossim, o Centro de Monitoramento permite subsidiar as camadas superiores no tocante a Gestão de Riscos, como um todo permitindo ao Comitê Gestor uma visão consolidada, segura e em tempo oportuno para tomadas de decisões.

- O centro deverá ser instalado no ambiente físico do Governo do Estado do RJ com livre acesso de profissionais credenciados pela Contratante e Contratada. Sendo a utilidade de energia elétrica, climatização, controle de acesso físico de responsabilidade do Contratante. É de responsabilidade da Contratada o hardware, software, equipe técnica e mobiliário.

- A Contratada deverá descrever em relatório técnico as necessidades físicas e de infraestrutura para a instalação do Centro de Monitoramento para avaliação pelo Comitê Gestor.

- Para um funcionamento adequado, a Contratante deve implementar as premissas ou requisitos abaixo de Segurança Física:
    - Local físico com área dedicada com uma Sala 40m2 e Ante Sala 20m2;
    - Apoio de Datacenter ou uma sala de servidores para alocação de equipamentos e servidores de aplicações. Com no mínimo de 2 racks prontos para a utilização da equipe técnica da Contratada;
    - Instalações elétricas com capacidade para suportar equipamentos e permitir escalabilidade do projeto. Deve-se implementar nobreaks e geradores para a proteção dos equipamentos e manter a disponibilidade do ambiente em caso de falha de energia;
    - Capacidade de refrigeração para manter temperaturas e umidades adequados ao hardware instalado, com possibilidade de reserva de refrigeração para possíveis expansões;
    - Controle de acesso físico com 02 fatores de autenticação;
    - Proteção de Segurança física;
    - Sistema de alarmes e câmeras de segurança; e
    - Sistema de combate à Incêndios;
    - Deve-se ter 03(três) bancadas com estações de trabalho para até 09 usuários
- O Centro será mobiliado com Hardware e Softwares necessários a operação 24/7/365, sendo composto por soluções livres (Open Source) e soluções proprietárias.
- O Centro será guarnecido com pessoal qualificado e treinado para a operação dos sistemas instalados.
- O estabelecimento de um centro de monitoramento abrangendo as capacidades mencionadas traria como benefícios:
    - Garantia de continuidade do serviço de comunicação de dados;
    - Garantia do nível de serviço / performance;
    - Extensão do controle sobre a infraestrutura cibernética além rede comunicação de dados das redes de Telecomunicações
    - Conhecimento da arquitetura de hardware e software permitindo análise e

avaliação de riscos;

- Melhoria da capacidade de reação em caso de problemas;
- Acompanhamento constante da performance e o nível de serviço acordado com as partes interessadas;
- Conhecer e manter atualizada a catalogação de todos os ativos de TIC;
- Conhecer os pontos de risco e não conformidades permitindo planejamento de ações preventivas;
- Entender o inter-relacionamento e dependências entre os ativos. Permite uma avaliação de riscos em caso de incidente em cada um dos ativos e seu efeito dominó nos demais.

4. GESTÃO DO CONTRATO

4.1. A Gestão de Contratos é a atividade exercida pela Contratante e Contratada visando o controle, o acompanhamento e à fiscalização do fiel cumprimento das obrigações assumidas pelas partes. Deve pautar-se por princípios de eficiência e eficácia, além dos demais princípios regedores da atuação administrativa, de forma a se observar que a execução do contrato ocorra com qualidade e em respeito à legislação vigente.

4.2. A Contratada deve gerenciar as faturas emitidas e a comprovação do acordo de nível serviços contratados, para pagamento ou para o desconto progressivo, caso não seja atendido o SLA contratado.

4.3. O Gestor de Contratos a ser fornecido pela contratada terá no mínimo as seguintes atribuições:

- Responsável pelo relacionamento com o cliente. Receber demandas e direcioná-as internamente;
- Acompanhamento da OS, Data Promessa e interfaces com as áreas internas da contratada;
- Posicionamento ao Cliente sobre todos os aspectos do contrato.

5. PAINEL DE INDICADORES

5.1. A Contratada deve implementar um Painel de Indicadores como a finalidade de estruturar um sistema de indicadores de desempenho e gestão operacional, de forma que a Contratante tenha uma visão geral dos indicadores de desempenho e de um sistema de gestão operacional baseado em análises periódicas, ações de melhorias e foco no resultado operacional.

5.2. Os processos de Gestão Integrada e o Catálogo de Serviços devem prover os seus indicadores para serem monitorados no Painel de Indicadores. A Governança de Infraestrutura de TIC e Segurança da Função tem a função de mapear e documentar os processos de Gestão Integrada e os serviços do Catálogo, nessa atividade serão documentados os indicadores de cada processo e serviço que devem ser implementados no Painel de Indicadores.

5.3. A Contratada deve utilizar indicadores de desempenho, para disponibilizar a informação que o gestor necessita sobre cada etapa do processo, para proporcionar maior exatidão na tomada de decisão, para trazer mais eficiência e eficácia aos processos, proporcionar mais rapidez, melhor compreensão e transparência ao se divulgar resultados e irá permitir a criação de um painel de indicadores com todas as informações disponíveis de forma panorâmica e dinâmica.

5.4. Os dados e informações deste book de indicadores a ser apresentado mensalmente

no período de medição do contrato serão ajustados entre a Contratada e a Contratante após o processo licitatório.

5.5. A Contratada deve implementar uma solução automatizada para a criação e monitoramento dos indicadores.

6. COMITÊ GESTOR

6.1. O Rio Digital deve ser constituído um Comitê de Gestor para a tomada de decisões estratégicas e resoluções de problemas que não foram solucionados pelos gestores da Contratada e do Contratante.

6.2. Este Comitê é um grupo formado com o propósito de tomar as decisões estratégicas, elaborar diretrizes para serem seguidas por todos, mostrar suporte e força para as decisões, e deliberar sobre os aspectos que demandam o envolvimento do Governo do Estado do RJ.

6.3. O comitê deve ser composto por integrantes, com ou sem prazo fixo de mandato, nomeados pelo Governo do Estado do RJ. As deliberações do Comitê devem ser tomadas pela maioria dos membros que o compõe e a função de integrante do Comitê ser indelegável.

6.4. O comitê será composto por integrantes indicados pelo Governo do Estado do RJ, através da Secretaria de Estado de Ciência, Tecnologia, Inovação e Cultura, e representantes da Contratada.

6.5. O número de participantes do Comitê deverá ser definido na reunião de abertura do projeto de implantação do Rio Digital.

6.6. Nos passos iniciais da estruturação do Rio Digital, este Comitê estará envolvido de maneira mais direta. Porém, ao longo do tempo, deve se reunir em reuniões normalmente bimestrais, ou a qualquer momento, conforme requerido pelas circunstâncias, para discutir assuntos relevantes e traçar os objetivos de negócio do Rio Digital.

6.7. Devem ser preparadas atas, documentando o conteúdo das reuniões, que devem ser revisadas e aprovadas pelos integrantes do Comitê e distribuídas aos demais participantes.

6.8. Este Comitê deverá elaborar semestralmente ou em outro momento determinado pelo Governo do Estado do RJ, o documento denominado Relatório do Comitê Gestor, a ser enviado para o Governo do Estado do RJ, contendo, entre outros aspectos, as seguintes informações:

- Descrição das atividades exercidas durante o período;

- Avaliação da efetividade dos serviços contratados, através da análise dos indicadores, com ênfase nos regulamentos, regulamentos internos e cumprimento das leis em vigor;
- Análise dos resultados parciais e finais das ações e atividades do Rio Digital de forma a medir efeitos, comparando-os às metas definidas e realizando os devidos ajustes; e
- Descrição das deficiências detectadas, bem como das recomendações apresentadas ao Governo do Estado do RJ, com a indicação daquelas não acatadas e respectivas justificativas.

7. VISÃO INTEGRADA DE PRODUTOS E SERVIÇOS

7.1. Está função atuará como gestor da entrega dos serviços garantindo a correta internalização e atendimento dos itens a serem providos. Irá funcionar como uma Central de Serviços de TIC.

7.2. Deverá ser constituída uma equipe de no mínimo duas pessoas com as seguintes atribuições:

- Atualização do catálogo de serviços.
- Atendimento das solicitações e demandas.
- Envio das demandas para os responsáveis técnicos.
- Administração da solução automatizada de demandas.
- Propor melhorias na solução automatizada de administração de demandas e no processo de demandas.

7.3. A Contratada deve prover uma solução automatizada para gestão de eventos para as demandas.

8. GOVERNANÇA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO E SEGURANÇA DA INFORMAÇÃO

8.1. Objetivo do Serviço:

8.1.1 Disponibilização de serviços de Governança de Infraestrutura de TIC e Segurança da Informação em Redes de Telecomunicações.

8.1.2 Este capítulo descreve o módulo de Governança de Infraestrutura de TIC e Segurança da Informação da Rede de Telecomunicações referente a arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

8.1.3 A contratação contempla a disponibilização de serviços especializados para a condução de projetos e mapeamento e desenho dos processos de negócios e operacionais relacionados.

8.2. Metodologia de Governança de Infraestrutura de Tecnologia da Informação e Comunicação e Segurança da Informação.

8.2.1.A CONTRATADA deverá disponibilizar os serviços de Governança de Infraestrutura de TIC e Segurança da Informação em redes de telecomunicações em conformidade com as boas práticas abaixo:

8.2.1.1. ABNT NBR ISO/IEC 38.500:2009 – Governança corporativa de tecnologia da informação.

- Incluindo os seguintes requisitos:
  - Cumprimento de obrigações (regulamentares, legislativas, legais, contratuais) relativas ao uso aceitável de TI
  - Riscos no uso da TIC, citando, inclusive, vários aspectos de segurança da informação
  - Correta implementação e operação dos ativos de TIC
  - Clareza quanto a responsabilidade (prestação de contas)
  - Continuidade de Negócios e sustentabilidade do negócio
  - Alinhamento da TIC às necessidades do negócio da Contratante
  - Alocação eficiente dos recursos de TIC
  - Comunicação com as partes interessadas
  - Redução de custos

8.2.1.2. Segue abaixo de forma gráfica de implementação da Governança de Infraestrutura de TIC.

Figura 02 – Modelo do ciclo de Governança de TIC.

8.2.1.3. A Contratada deverá utilizar os conceitos COBIT 5 para implementar a Governança de TIC e Segurança da Informação.

8.2.1.4. A Contratada deve emitir o Relatório de Governança de Infraestrutura de Tecnologia da Informação e Comunicação e Segurança da Informação com as lacunas identificadas e as recomendações de melhoria.

8.2.2.ABNT NBR ISO/IEC 27.014:2013 – Governança de segurança da informação.

8.2.2.1. O escopo da Governança de Segurança da Informação abrange a confidencialidade, integridade e disponibilidade da informação. Entretanto, requer também o processo interno de divulgação, de comunicar os resultados para todas as partes interessadas.

8.2.2.2. Os objetivos da Governança de Segurança da Informação, são: Alinhar os objetivos e a estratégia da Segurança da Informação com os objetivos e estratégia do negócio da organização; agregar valor para a alta direção e para as partes interessadas (entrega de valor) e garantir que os riscos da informação estão sendo adequadamente endereçados para as pessoas responsáveis.

8.2.2.3. O modelo adiante de implantação de Governança de SI é o preconizado pela ABNT NBR ISO/IEC 27014:2013:

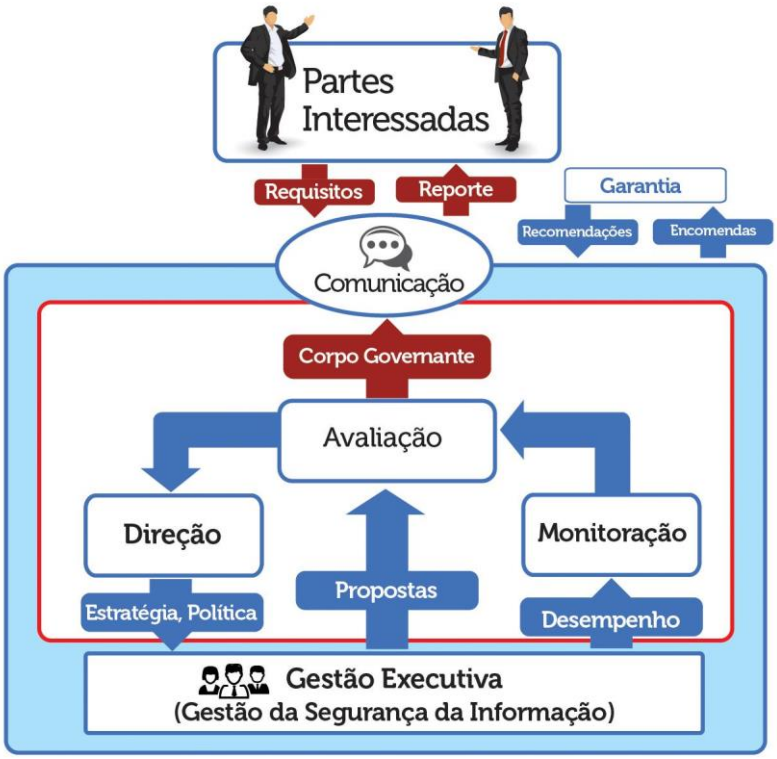


Figura 03 – Modelo de Governança de SI

8.2.2.4. A seguir, a metodologia de implantação da Governança de SI:

- Avaliação
  - Avalia se os objetivos de Segurança da Informação foram atingidos, com base nos indicadores que devem ser propostos durante a implantação do modelo de Governança de Segurança da Informação.
- Direção
  - Etapa em que se deve fornecer o direcionamento sobre os objetivos de Segurança da Informação.
- Monitoração
  - Fase em que se realiza a validação da eficiência, eficácia e evolução dos objetivos de SI, em termos de desempenho, e quanto esses objetivos estão agregando valor ao negócio da organização.
- Comunicação

- Aqui é realizada a troca de informações com as partes interessadas sobre os objetivos de SI e as ações de Segurança da Informação implantadas.

- Garantia
  - Planejado pelo comitê de SI e executado por uma auditoria independente de Segurança da Informação, ou seja, uma auditoria externa à organização.

8.2.2.5. Por fim, os benefícios da implantação da Governança de Segurança da Informação são:

- Apoiar a implantação dos requisitos de Segurança da Informação;
- Alinhar os objetivos de Segurança da Informação com os objetivos estratégicos da organização;
- Certificar que a organização estabelece, implementa, opera e monitora um modelo de gestão de risco em conformidade com o Sistema de Gestão da Segurança da Informação presente na ABNT NBR ISO/IEC 27001:2013;
- Implementar controles eficientes e eficazes para a gestão da Segurança da Informação, conforme a ABNT NBR ISO/IEC 27001:2013 e a ABNT NBR ISO/IEC 27002:2013;
- Assegurar que a informação circulante na organização receba um nível adequado de proteção;
- Assegurar que funcionários, fornecedores e terceiros tenham uma boa conduta no uso das informações.

8.2.2.6. A Contratada deve emitir o Relatório de Governança de SI com as lacunas identificadas e as recomendações de melhoria.

8.2.3. ABNT NBR ISO/IEC 27.002:2013 – Código de prática para controles de segurança da informação.

- Executar uma atividade de análise de lacunas para identificar as lacunas de Segurança da Informação para os ativos contratados do Contratante, utilizando os controles da ISO/IEC 27.002:2013.
- Essa atividade deverá contemplar no mínimo as seguintes seções da ISO/IEC 27.002:2013:
  - A5 – Políticas de segurança da informação
  - A6 – Organização da segurança da informação
  - A7 – Segurança em recursos humanos
  - A8 – Gestão de ativos

- A9 – Controle de acesso
- A10 – Criptografia
- A11 – Segurança física e do ambiente
- A12 – Segurança nas operações
- A13 – Segurança nas comunicações
- A14 – Aquisição, desenvolvimento e manutenção de sistemas
- A15 – Relacionamento na cadeia de suprimento
- A16 – Gestão de incidentes de segurança da informação
- A17 – Aspectos de segurança de informação na gestão de continuidade do negócio
- A18 – Conformidade

8.2.3.1. Emitir um relatório para a Contratante do resultado da Análise de Lacunas sobre o serviço contratado.

8.2.3.2. Emitir recomendações de implementações dos controles aplicáveis da Norma ISO/IEC 27.002:2013.

8.2.4.ABNT NBR ISO 21.500:2012 - Orientações sobre gerenciamento de projeto.

- Executar os projetos de acordo com boas práticas reconhecidas internacionalmente.
- A utilização de um modelo baseado em padrões e metodologias formalizados, reconhecidos internacionalmente, é capaz de se adequar às estratégias, iniciativas e estrutura organizacional do Estado do RJ, além de atender às exigências dos órgãos reguladores e fiscalizadores da administração pública estadual.
- Os benefícios da execução de projetos por meio de um modelo incluem:
  - **Um roteiro único para execução** – Todos sabem o que deve ser feito e como. Além de garantir o alinhamento da equipe, isso reduz a quantidade de discussões (achismos) e aumenta a probabilidade do projeto ser entregue com sucesso.
  - **Cumprimento de prazos** – Não há como garantir que um projeto terminará no prazo, pois ao longo de sua execução acontecem mudanças, situações inesperadas e incontroláveis. No entanto, o gerenciamento de projetos oferece ferramentas para antever, minimizar e evitar atrasos ou, no pior dos casos, avisar com bastante antecedência que um prazo não será cumprido ou que o custo será “estourado”.
  - **Flexibilidade** – O projeto pode ser alterado a qualquer momento, essa

é uma das maiores certezas que um gerente de projetos carrega consigo, mas, ao alterar um projeto, deve-se avaliar e discutir sobre seus efeitos colaterais (impactos) e se a alteração é condizente com o objetivo do projeto. O gerenciamento de projetos oferece ferramentas para controlar mudanças de forma segura, evitando que um simples "pedido do cliente" acabe gerando um caos irreversível.

- **Controle sobre retorno dos investimentos (ROI)** – Sabendo quanto custa cada etapa do projeto é possível controlar sua lucratividade e, com isso, evitar despesas desnecessárias, negociar preços com fornecedores, antecipar receitas e postergar despesas. A empresa passa a ter mais segurança sobre a lucratividade de cada projeto e, por consequência, do retorno sobre seus investimentos.
- **Melhora a percepção de valor do cliente** – Quando se gerencia as expectativas dos clientes, analisando seus desejos (implícitos e explícitos) sua "percepção de valor" aumenta, pois se sente mais prestigiado. É como comparar o atendimento de uma lanchonete "de esquina" com o McDonalds, neste segundo você sabe como vai ser atendido, o que vai receber e em quanto tempo, além de ter certeza de que, se algo der errado, haverá alguém para resolver o problema. Antecipa problemas – Como você já levantou o que pode dar errado no projeto (riscos), fica fácil tomar ações para evitar que problemas aconteçam. Isso aumenta a eficiência da empresa, permitindo que faça mais e mais projetos ou, pelo menos, projetos com maior qualidade.
- **Comunicação fluida** – Um cliente que tem informações sobre o andamento do projeto e que tem suas ideias e necessidades ouvidas e analisadas, sente-se mais satisfeito, mesmo que o projeto dê errado no final.

8.2.4.1. Abaixo é apresentado o modelo de gestão de projetos especificado pela ABNT NBR ISO 21.500:2012

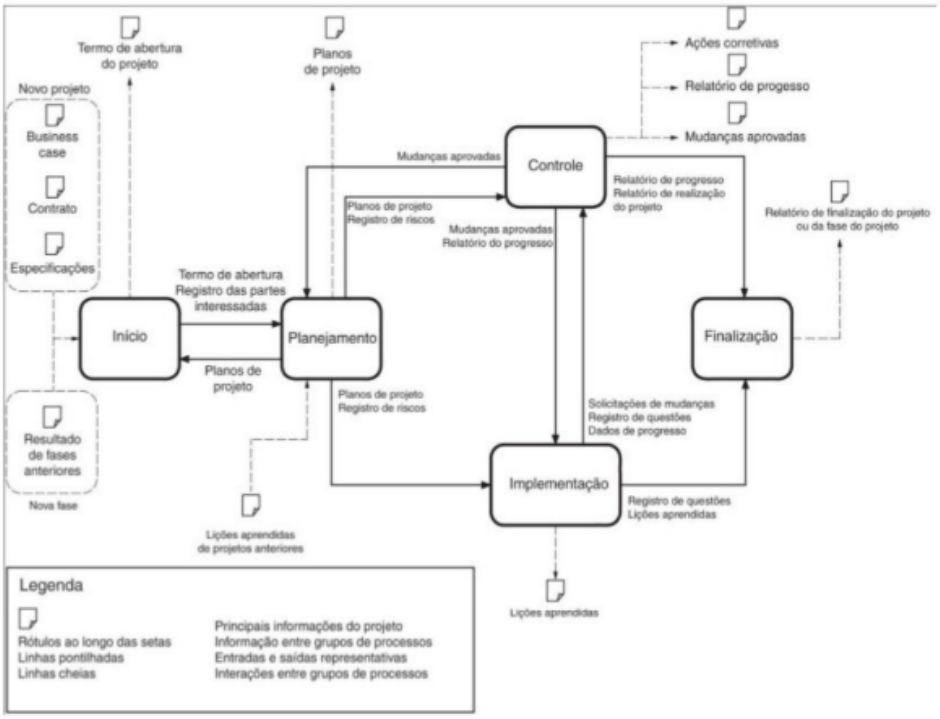


Figura 04 – Processo de Gestão de Projetos

8.2.4.2. A Contratada deve emitir um relatório com as diretrizes para a implantação do Sistema de Gerenciamento de Projetos.

8.2.5.Information Technology Infrastructure Library (ITIL v3)

- ITIL é o modelo para gerenciamento de serviços de TIC mais adotado mundialmente. A utilização das melhores práticas contidas na ITIL V3 (versão atual) ajuda as organizações a atingirem seus objetivos de negócio utilizando apropriadamente os serviços TIC.
- Para se ter uma definição de o que é ITIL é importante entender que ela é organizada em torno do ciclo de vida de um serviço dentro de uma organização e contém os seguintes volumes:
    - Estratégia do Serviço (“Service Strategy”): Definição dos requisitos e necessidades do negócio;
    - Projeto de Serviço (“Service Design”): Definição da solução a ser adotada;
    - Transição de Serviço (“Service Transition”): Relacionado ao gerenciamento de mudanças;
    - Operação do Serviço (“Service Operation”): Assegura que os

serviços estão sendo atendidos baseado nos SLAs;

- Melhoria Contínua do Serviço ("Continual Service Improvement"): Manter a constante melhoria dos serviços baseando-se no cliclo PDCA.

Figura 05 – Modelo do ITIL

8.2.5.1. Dentre os principais benefícios do uso do modelo ITIL v3 podemos mencionar:

- Alinhamento de TIC, seus serviços e riscos com as necessidades do negócio;
- Níveis de Serviço (SLA) negociáveis;
- Processos consistentes e previsíveis;
- Eficiência na entrega de serviço;
- Serviços e Processos mensuráveis e passíveis de melhorias;
- Otimização da experiência do cliente;
- Uma linguagem comum.

8.2.5.2. A Contratada deve emitir um relatório com a definição do Catálogo de Serviços para implantação dos serviços do projeto.

8.2.6. Guia para o Gerenciamento de Processos de Negócio – Corpo comum de conhecimento (Guia ABPMP BPM CBOK V3.0).

- Mapear os processos de negócio de forma a entender os impactos e melhorias necessárias.

- O objetivo da gestão de processos inclui realizar processo planejado de acordo com a especificação pré-determinada, no tempo planejado, no custo planejado e atendendo as expectativas das partes interessadas.
- O gerenciamento de processos é necessário para atender:
    - Mudanças constantes nas empresas;
    - Adequações legais;
    - Aumento dos padrões de qualidade;
    - Adaptação tecnológica;
    - Necessidade de sobrevivência.

8.2.6.1. Abaixo é apresentado um modelo de gestão de processos:

Figura 06 – Modelo de Gestão de Processos

8.2.6.2. Para cada serviço identificado no Catálogo de Serviços será feio o mapeamento deste serviço e elaborado a documentação detalhada do serviço de acordo com as boas práticas de Gerenciamento de Processos de Negócio.

9. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

9.1. Objetivo do Serviço:

9.1.1. Este capítulo descreve o módulo de Gestão de Continuidade de Negócios referente à arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

9.1.2. O objeto desta contratação visa garantir a continuidade dos processos críticos caso aconteça um incidente grave na infraestrutura do Rio Digital contida neste edital.

9.1.3. O processo de Gestão de Continuidade de Negócios irá subsidiar o processo de gestão do Painel de Indicadores do Rio Digital.

9.2. Metodologia de Gestão de Continuidade de Negócios.

9.2.1. A Contratada deve implementar uma solução automatizada para Gestão de Continuidade de Negócios em conformidade com todas as diretrizes deste item sobre “Metodologia do Serviço de Gestão de Riscos”.

9.2.2. As diretrizes da metodologia de implementação do processo de Gestão de Continuidade de Negócios estão em conformidade com a ABNT NBR ISO 22301:2013 - Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos. A utilização de um modelo baseado em padrões e metodologias formalizados, reconhecidos internacionalmente, é capaz de se adequar às estratégias, iniciativas e estrutura organizacional do Estado do RJ, além de atender às exigências dos órgãos reguladores e fiscalizadores da administração pública estadual.

9.2.3. FASE 1 - Planejar o Projeto/Serviço – Esta fase está descrita a seguir.

9.2.3.1. O objetivo desta fase inicial é planejar todas as fases do projeto, organizar as atividades, alocar os recursos necessários e definir os produtos gerados no decorrer dos trabalhos nesse projeto. Nesta fase se estabelece o contexto: fase inicial do projeto, onde se realizam reuniões entre a equipe da Contratada e da Contratante, definindo todos os itens de relevância para a organização do projeto (contexto e escopo).

9.2.3.2. As Atividades da fase estão descritas a seguir:

- Reunião de planejamento: com a finalidade de integrar as equipes envolvidas, da Contratada e da Contratante e alinhar o entendimento sobre o planejamento e a execução do projeto, a reunião de planejamento permitirá que os seguintes pontos sejam discutidos e definidos:
  - As premissas e riscos considerados na pré-venda.
  - As equipes envolvidas.
  - As expectativas do cliente.
  - Fatores críticos de sucesso.
  - Plano de trabalho e os produtos esperados.
  - Cronograma e prazos.
  - Principais milestones.
  - Autorização formal da Contratante para execução das fases do projeto.
- Relatório de Organização e Planejamento: com a visão geral do projeto, dos recursos envolvidos e suas respectivas responsabilidades, este documento também contempla a distribuição das atividades e a previsão de cronograma para a realização das mesmas. A fase 2 do projeto somente será iniciada com a aprovação deste relatório pela equipe responsável e com a aprovação formal da Contratante para a execução do serviço.

9.2.3.3. Os produtos da fase estão descritos a seguir:

- Relatório de Organização e Planejamento
- Apresentação Inicial

9.2.4.FASE 2 - Definir a Política de Gestão de Continuidade de Negócios

9.2.4.1. Nesta fase se estabelece os primeiros conceitos de Gestão de Continuidade de Negócios, efetiva e formalmente; através da definição da Política de Continuidade de Negócios. A Política de Continuidade de Negócios consiste em conjunto formal de regras, padrões e responsabilidades que devem ser seguidas em relação à implantação e

gestão do processo GCN.

9.2.4.2. As atividades da fase estão descritas a seguir:

- Diagnosticar as necessidades de Gestão de Continuidade de Negócios

  - Estudo da legislação aplicável a Contratante: Atendimento as regulamentações brasileiras que são aplicáveis a Contratante.

  - Conhecer a Contratante, necessidades dos Objetivos de Gestão de Continuidade de Negócios e elaborar relatório de diagnóstico justificando os temas que serão abordados.

- Definir grupo de trabalho responsável pela revisão e validação da Política

- Elaborar a Política de GCN

  - Elaboração do Rascunho da Política de GCN

- Revisa e Validar

  - Reunir para revisar e validar a Política de GCN
  - Emitir Ata de Validação/Aprovação da Política de GCN
  - Coletar assinatura na Ata de Validação

9.2.4.3. O produto desta fase está descrito a seguir:

- Política de Gestão de Continuidade de Negócios da Contratante

9.2.5.FASE 3 – Entender a Organização

9.2.5.1. Nesta fase são desenvolvidas as entrevistas para o levantamento das criticidades da empresa, através da execução do BIA (Business Impact Analysis) e da AR (Análise de Riscos). Os resultados desta fase (Relatório de BIA e AR) embasarão as decisões estratégias na fase seguinte (Determinar estratégias).

9.2.5.2. BIA – Business Impact Analysis (Análise de Impacto nos Negócios) -

9.2.5.3. Identificar os impactos decorrentes das situações de interrupções e

desastres que podem afetar a organização, e as técnicas que podem ser usadas para quantificar e qualificar esses impactos. Definir as funções críticas, suas prioridades de recuperação e suas interdependências, de modo que possa ser estabelecida a meta para o tempo de recuperação.

9.2.5.4. As atividades da fase estão descritas a seguir:

- Análise da documentação existente:

o Coleta dos principais documentos a serem cedidos pelo cliente na busca de informações relevantes para o BIA.

- Entrevistas com gestores dos processos:

o Levantamento de informações com os principais gestores do cliente.

- Consolidação dos resultados:

o Análise e consolidação dos resultados gerados através das entrevistas e análise de documentos.

- Elaboração dos relatórios:

o Esta atividade visa elaborar o Relatório do Business Impact Analysis.

9.2.5.5. Execução da Análise de Riscos nos processos críticos da Contratante no escopo da infraestrutura de telecomunicações. A AR tem como objetivo identificar riscos macros nas instalações e infraestrutura dos ambientes físicos, infraestrutura (facilities) e nos ativos de tecnologia da informação.

9.2.5.6. As atividades da fase estão descritas a seguir:

- Levantamento dos Ativos, Sistemas e Processos críticos de acordo com o BIA:

o Inventário na solução automatizada de Gestão de Continuidade de Negócios dos ativos, sistemas e processos e dependências.

- Execução da Análise de Riscos:

o Nesta atividade serão realizadas entrevistas, análises de documentos, de processos e de recursos de Tecnologia da Informação.

- Os principais ativos tecnológicos, que suportam os principais sistemas/processos críticos serão analisados utilizando a solução automatizada de Gestão de Continuidade de Negócios.

- Elaboração dos relatórios de Análise de Riscos:

- Esta atividade visa elaborar todos os mapas, relatórios de análise de riscos e recomendações para reduzir o nível de risco existente nos processos de negócio críticos identificados pela Análise de Impacto no Negócio.

9.2.5.7. Os produtos da fase estão descritos a seguir:

- Relatório do BIA – Business Impact Analysis (Análise de Impacto nos Negócios)

- Relatório de Análise de Riscos (RAR): documento que demonstra os ativos analisados, ameaças consideradas e riscos identificados, além de uma visão gerencial para apoiar a fase de Avaliação.

- Relatório Operacional de Riscos (ROR): documento que identifica os controles não implementados, com índices de riscos por controle e recomendações de priorização no tratamento.

9.2.6.FASE 4 – Determinar e Implementar as Estratégias de Continuidade de Negócios

9.2.6.1. Nesta fase são analisadas as estratégias de recuperação e continuidade que serão adotadas pela Gestão de Continuidade de Negócios. Determinar e orientar a seleção das estratégias operacionais alternativas, para a recuperação dos negócios e das tecnologias de informação dentro da meta estabelecida para o tempo de recuperação, mantendo, ao mesmo tempo, as funções críticas da Contratante e definindo a necessidade de existência ou não de um ambiente alternativo.

9.2.6.2. As estratégias devem ser aprovadas pela Contratante, para prosseguimento das atividades. A responsabilidade da Contratada é de apoiar na escolha da melhor estratégica de acordo com o seu custo benefício, a Contratante deve adquirir a infraestrutura necessária para a implantação da estratégia.

9.2.6.3. As atividades da fase estão descritas a seguir:

- Análise das Estratégias de Continuidade;

  - Consolidação junto aos responsáveis pelo projeto da existência ou não de um site alternativo.

- Análise das Estratégias de Recuperação / Restauração;

  - Consolidação junto aos responsáveis pelo projeto da existência ou não de um site alternativo (operacional/ dados/ storage).

- Levantamento de Dados;

  - Levantamento com as alternativas de soluções.

- Elaboração do Relatório de Estratégia de Continuidade.

  - Relatório onde se encontram resumidas as definições das estratégias estabelecidas.

  - Documento apresentando a especificação técnica, e a cotação de preços.

9.2.6.4. Os produtos da fase estão descritos a seguir:

- Relatório de Estratégias e Continuidade: Documento o processo de análise e seleção da estratégia de continuidade a ser adotada pela Contratante em resposta a interrupção do processo de negócio.

- Apresentação executiva dos resultados.

9.2.6.5. A aquisição de recursos tecnológicos para a implementação da Estratégia de Continuidade é de responsabilidade da Contratante.

9.2.7. FASE 5 - Estabelecer e Implementar os Planos

9.2.7.1. O Objetivo desta fase é desenvolver e implementar os Planos de Continuidade de Negócios, através do desenvolvimento dos planos necessários para a efetiva recuperação dos processos dentro da meta estabelecida para o tempo de recuperação. Nesta fase são executadas

novas entrevistas com os gestores para a elaboração dos planos (PAC, PCO, PRD, PGI e PTV), que são elaborados na solução automatizada de Gestão de Continuidade de Negócios– repositório inteligente de informações que irá apoiar a Contratante na gestão dos planos junto às áreas de negócios e de gestão de ativos. São apresentadas as estruturas dos 5 (cinco) documentos que integram o Plano de Continuidade do Negócio:

- **Plano de Gerenciamento de Incidentes**: Responde ao incidente, focando a contenção dos danos e a priorização das ações para contingência. Sua atribuição é definir os parâmetros de divulgação visando à defesa da imagem.

- **Plano de Administração de Crise:** Representa a garantia mais eficaz da administração em situações adversas. O PAC relaciona o funcionamento das equipes (Recursos Humanos) durante e depois da ocorrência de um evento (em tempo de "guerra").

- **Plano de Continuidade Operacional:** Composto por um conjunto de procedimentos, destinados a manter a continuidade dos processos de negócios e serviços críticos, considerando-se a ausência de componentes que os suportem, devido à ocorrência de eventos previamente identificados e definidos.

- **Plano de Recuperação de Desastres:** Descreve os procedimentos que garantem a recuperação/restauração dos componentes que suportam os processos de negócios críticos, através da avaliação das vulnerabilidades destes componentes.

- **Plano de Teste e Validação:** Determina, pós-desenvolvimento dos planos e, nos contextos de desenvolvimento da Gestão da Continuidade de Negócios, os testes e seus planejamentos para determinar as coletas de evidências (auditoria) e para a correção de problemas que possam invalidar a eficiência dos planos.

9.2.7.2. As atividades da fase estão descritas a seguir:

- Customização da Entrevista de Planos;

- Customização das entrevistas de acordo com as opções de abordagem definidas.

- Aplicação da Entrevista de Plano de Gerenciamento de Incidente;

- Coleta de informações para a resposta a incidentes.

- Aplicação da Entrevista de Plano de Continuidade Operacional;

- Coleta de informações para continuidade operacional dos processos/componentes.

- Aplicação da Entrevista de Plano de Recuperação de Desastres;

- Coleta de informações para recuperação/restauração dos processos/componentes definidos.

- Elaborar Plano de Gerenciamento de Incidentes – PGI;

- Cadastramento dos procedimentos com foco em resposta a incidentes na solução automatizada de Gestão de Continuidade de Negócios.

- Elaborar Plano de Continuidade Operacional – PCO;

- Cadastramento, na solução automatizada de Gestão de Continuidade de Negócios, dos procedimentos com foco em continuidade dos processos/componentes.

- Elaborar Plano de Recuperação de Desastres – PRD;

- Cadastramento, na solução automatizada de Gestão de Continuidade de Negócios, procedimentos com foco na recuperação/restauração dos processos/componentes Definidos.

- Criar todos planos na solução automatizada de Gestão de Continuidade de Negócios;

- Imprimir os planos na solução automatizada de Gestão de Continuidade de Negócios;

- Validar os Planos com Gestores /Responsáveis;

- Obter a aprovação dos Planos junto aos gestores/patrocinador do projeto.

- Ajustes dos Planos com Gestores /Responsáveis;

- Prováveis ajustes ocorridos na Validação dos Planos com os gestores/responsáveis

- Elaborar Plano de Administração de Crise – PAC;

- Cadastramento, na solução automatizada de Gestão de Continuidade de Negócios, procedimentos de cada plano conforme o incidente.

- Validar os Planos (Plano de Administração de Crise) com Gestor da Contratante;

- Obter a aprovação dos Planos junto aos gestores/patrocinador do projeto.

- Ajustes dos Planos (Plano de Administração de Crise) com Gestor da Contratante;

- Prováveis ajustes ocorridos na Validação dos Planos com Gestores /Responsáveis de Continuidade do Negócio.

- Elaborar Plano de Teste e Validação – PTV;

- Cadastramento, na solução automatizada de Gestão de Continuidade de Negócios, procedimentos de cada plano conforme o incidente.

- Executar o Teste de Mesa;

- Planejar o Teste de Mesa;

- Executar o Teste de Mesa;

- Avaliar o Teste de Mesa.

- Ajustes dos Planos (Plano de Teste e Validação) com Gestores /Responsáveis da Gestão de Continuidade do Negócio;

- Prováveis ajustes ocorridos na Validação dos Planos com o gestor do Plano de Continuidade do Negócio.

9.2.7.3. Os produtos da fase estão descritos a seguir:

- Plano de Administração de Crise
- Plano de Gerenciamento de Incidente
- Plano de Continuidade Operacional
- Plano de Recuperação de Desastres
- Plano de Teste e Validação

9.2.8.FASE 6 – Exercitar e Testar

9.2.8.1. A Contratada deverá desenvolver e executar testes para 20% dos planos desenvolvidos na fase anterior. O objetivo é a transferência do conhecimento da Contratada para o Contratante. São também obrigações da Contratada:

- Fazer o pré-planejamento e coordenar os testes dos planos, avaliar e documentar os resultados dos ensaios.
- Desenvolver os processos para manter atualizadas as habilidades de continuidade e a documentação da Gestão de Continuidade de Negócios, em conformidade com a diretriz estratégica da Contratante.
- Certificar-se de que o plano será eficaz, por meio de avaliação dos resultados dos testes.

9.2.8.2. As atividades da fase estão descritas a seguir:

- Definição do tipo de exercícios para a Gestão de Continuidade de Negócios e planos.
- Definição/planejamento dos exercícios da Gestão de Continuidade de Negócios e planos.

- Elaborar exemplo de planejamento, acompanhamento e avaliação de exercícios dos planos.

- Elaborar recomendações para auditoria.

9.2.8.3. Os produtos da fase estão descritos a seguir:

- Relatório de Recomendações para o exercício, manutenção e revisão dos planos

9.2.9.FASE 7 – Divulgar e Capacitar

9.2.9.1. A ABNT NBR ISO 22301:2013 exige que a GCN seja inserida na cultura da Contratante. Isto só é possível com o envolvimento efetivo de toda a organização em torno do tema; o que é conseguido com a implantação de um programa para criar a "conscientização corporativa" e aprimorar as competências necessárias para desenvolver, implementar, manter e executar o Plano de Continuidade de Negócios. Nesta fase, também deve ser escolhido um grupo de colaboradores replicadores para atuar diretamente com o assunto.

9.2.9.2. As atividades da fase estão descritas a seguir:

- Definição de objetivos e métricas da campanha de divulgação de Gestão de Continuidade de Negócios

- Definição de Temas para palestras e treinamento no Gestão de Continuidade de Negócios

9.2.9.3. Os produtos da fase estão descritos a seguir:

- Relatório de Divulgação de Gestão de Continuidade de Negócios.

9.3. A Contratada deverá prover a solução automatizada para a Gestão de Continuidade de Negócio com as seguintes características:

- Possibilidade de gerenciar perímetros (por localidade, por organograma, por função etc.), ativos (tecnologia, pessoa, processo, ambiente ou customizado) e Checklists.

- Possibilidade de gerenciar as pessoas e os grupos de pessoas do Contratante.

- Possibilidade de associar propriedades aos ativos, como: texto, data, número, arquivo, lista de opções etc.

- Possibilidade de gerenciar os riscos nos níveis tático e estratégico do Contratante, inclusive suas associações e atributos, além de visualizar os detalhes dos resultados das últimas análises de riscos e de conformidade de forma integrada.

- Possibilidade de exportar, editar e importar informações da estrutura organizacional e das pessoas usando uma planilha modelo.

- Possibilidade de integrar o inventário de ativos com os equipamentos existente no Contratante. (ex: Microsoft Active Directory, XML ou planilhas Excel).

- Possibilidade de criar relatório de análise de impacto de negócio

- Possibilidade de cadastrar procedimentos de continuidade de negócios

- Possibilidade de cadastrar estratégias de continuidade de negócios

- Possibilidade de cadastrar planos de continuidade de negócios

- Possibilidade emitir planos de continuidade de negócios

10. GESTÃO DE CONFORMIDADES

10.1. Objetivo do Serviço:

10.1.1. Este documento descreve o módulo de Gestão de Conformidades referente a arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

10.1.2. O objeto desta contratação visa verificar a conformidade de leis, regulamentos da administração estadual e órgãos de controle e procedimentos internos da infraestrutura da Rio Digital.

10.1.3. A Gestão de conformidade também visa garantir que todos os serviços contratados estão aderentes aos especificados no edital. Servindo também de insumo para a Gestão de Contrato e a Gestão de Indicadores.

10.2. Metodologia de Gestão de Conformidades

10.2.1. As funções da Gestão de Conformidade na Rio Digital estão descritas abaixo:

- Certificar-se da aderência e do cumprimento das leis pertinentes, organizando as evidências e padronizando os processos;
- Implantar, disseminar e monitorar a cultura de controles internos no Contratante, de acordo com os preceitos de legalidade, transparência, prestação de contas e governança corporativa;
- Promover testes periódicos dos controles internos de cada área do Contratante, avaliando-os e recomendando melhorias;
- Avaliar e acompanhar a criação de novos serviços do Contratante, focando no comprometimento da operação no tocante às normas internas, segregação de funções e risco de imagem do contratante;
- Atuar em parceria com a Área de Controle de Riscos e a Auditoria na realização de seus trabalhos;
- Disseminação de princípios e padrões de ética e integridade;
- Interiorização da cultura de Gestão de Conformidade no Contratante e geração de indicadores de Riscos;
- Identificação das não conformidades e gestão da prestação de contas as áreas responsáveis, com a geração de métricas e relatórios executivos.

10.2.2. A metodologia de gestão de Conformidade deve considerar as normativas e regulamentações internas/externas do segmento de mercado em questão, e avaliar se os controles estabelecidos por esses documentos estão implementados de forma eficaz e eficiente.

10.2.3. A Contratada deve implementar uma solução automatizada para estabelecer, manter e melhorar continuamente a Gestão de Conformidade, focando no ciclo de gestão de qualidade chamado de PDCA.

10.2.4. Na etapa de Inventariar a Contratada deve implementar no mínimo as atividades abaixo:

- Definição do escopo da Gestão de Conformidade;
- Integração com a Gestão de Riscos;
- Levantamento dos ativos, procedimentos, políticas, leis, regulamentos, controles e bases de conhecimento;
- Inventário na solução automatizada dos riscos e controles de conformidade, processos, controles e suas dependências.

10.2.5. Na etapa de Analisar a Contratada deve implementar no mínimo as atividades abaixo:

- Verificar se os requisitos de conformidade que fazem parte do escopo estão implementados;
- Elaborar a base de conhecimento/questionários de conformidade;
- Enviar para os proprietários dos ativos a base de conhecimento de conformidade que devem ser respondidos de acordo com os controles internos da Contratante;
- Criar o Painel de Indicadores de conformidade e de não conformidades;
- Emitir produtos de Relatório de Conformidade.

10.2.6. Na etapa de Avaliar a Contratada deve implementar no mínimo as atividades abaixo:

- Avaliar os controles que não estão implementados e os impactos relacionados;
- Criar workflow para tratamento das não conformidades;
- Elaborar o produto de plano de ação para tratamento das não conformidades.

10.2.7. Na etapa de Tratar a Contratada deve implementar no mínimo as atividades abaixo:

- Monitorar o tratamento das não conformidades;
- Gerar novas métricas de indicadores de conformidade, após o tratamento.

10.2.8. A Contratante é responsável pelo tratamento das não conformidades.

10.2.9. A CONTRATADA deverá prover a solução automatizada com as seguintes características:

- Para medir o nível de conformidade de um ativo, a solução automatizada deve usar métricas diferentes de acordo com o tipo de informação que se queira analisar. São elas: Índice de Não Conformidade e Índice de Conformidade.
- Deve ser possível criar diferentes escalas de respostas para a análise de conformidade dos ativos, como por exemplo: “Alto, Médio, Baixo”; “1, 2, 3, 4, 5”; “Não Atendido, Parcialmente Atendido, Totalmente Atendido” etc.
- Os projetos de conformidade devem poder ser criados para verificar conformidades por meio de um conjunto de atividades que envolvem a seleção de um escopo de análise e o envio de entrevistas para examinar o grau de atendimento a requisitos preestabelecidos por um ou mais documentos de referência.
- Possibilitar a criação de entrevistas - com a geração de formulário web customizado - em diferentes formatos, para a coleta de informações da análise, com a possibilidade de monitorar o recebimento, o preenchimento e o envio das respostas das entrevistas e incluir um revisor para aprovar as respostas.
- A entrevista deve ser formada por uma série de perguntas que permitem examinar o grau de conformidade da Contratante com as regras preestabelecidas em um ou mais documentos de referência. Os entrevistados (usuários cadastrados na solução automatizada) devem ser alocadas para responder a uma entrevista, com um endereço de e-mail válido para que possam receber notificações com os links para responder as entrevistas on-line.
- A solução automatizada deve possibilitar a geração de relatório de análise de conformidade, com o objetivo de apresentar o resultado final de uma análise de conformidade em termos gerenciais, consolidando as informações encontradas durante o projeto. Ele deve auxiliar no processo de gestão fazendo recomendações para a avaliação e tratamento das não

conformidades identificadas.

- A solução automatizada deve possibilitar a total customização de relatórios incluindo: formatação, inclusão e exclusão de campos, inserção de gráficos etc.

- A solução automatizada deve possibilitar o agendamento da geração de relatórios por período, com o envio de alerta por correio eletrônico.

11. GESTÃO DO ATIVO

11.1. Objetivo do Serviço:

11.1.1. Este capítulo descreve o módulo de Gestão Ativos referente à arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

11.1.2. O objeto desta contratação visa avaliar, direcionar e monitorar de forma correta os Ativos de informação, especificamente, sendo eles: ambiente físico, pessoas, processos e tecnologia.

11.1.3. A Gestão de Ativos também visa servir de insumo para a Gestão de Indicadores.

11.2. Metodologia para a Gestão de Ativos

11.2.1. A Contratada deve implementar o serviço de Gestão de Riscos em conformidade com as diretrizes presente na Norma ABNT NBR ISO 55000:2014 - Gestão de ativos — Visão geral, princípios e terminologia e na ABNT NBR ISO 55002:2014 - Gestão de ativos — Sistemas de gestão — Diretrizes para a aplicação da ABNT NBR ISO 55001. Os requisitos do sistema de gestão de ativos na ISO 55001 foram organizados em sete elementos específicos:

11.2.2. Contexto da organização - Os requisitos compreendem:

- Alinhamento com os objetivos organizacionais;
- Necessidades e expectativas das partes interessadas;
- Critérios para tomada de decisão;
- Definição do Escopo (quais ativos farão parte do sistema de gestão de ativos);
- Desenvolvimento de um plano estratégico de gestão de ativos.

11.2.3. Liderança - Os requisitos compreendem:

- Comprometimento com respeito ao sistema de gestão de ativos;
- Promoção da colaboração interfuncional e a melhoria contínua do sistema de gestão de ativos;
- Estabelecimento de uma Política de Gestão de Ativos coerente com o plano organizacional e adequadamente comunicada;
- Atribuição de responsabilidades e autoridades relativas à elaboração de estratégias e planos, sua adequação, eficácia e atualização.

11.2.4. Planejamento - Os requisitos compreendem

- Avaliação de riscos e oportunidades ao longo do tempo;
- Estabelecimento de objetivos de gestão de ativos, consistentes com os objetivos organizacionais e usando os critérios de tomada de decisão em gestão de ativos;
- Integração do planejamento de gestão de ativos com outras atividades de planejamento organizacional;
- Documentar critérios, métodos e processos de gestão de ativos;
- Riscos relacionados a ativos devem constar do gerenciamento de riscos da organização.

11.2.5. Suporte - Os requisitos compreendem:

- Fornecimento de recursos necessários para o sistema de gestão de ativos;
- Garantia de competência apropriada do pessoal;
- Comunicação e conscientização;
- Determinação das necessidades de informação e sua documentação para suportar o sistema de gestão de ativos; considerando o impacto da qualidade, disponibilidade e gerenciamento das mesmas sobre a tomada de decisão, incluindo sua proteção.

11.2.6. Operação - Os requisitos compreendem:

- Implementação e controle de processos para atender aos requisitos e ações definidos no planejamento;
- Tratamento e monitoramento de riscos;
- Gestão da mudança e as possíveis consequências sobre a realização dos objetivos da gestão de ativos;

11.2.7. Avaliação de desempenho - Os requisitos compreendem:

- Definição do que precisa ser medido e monitorado e os métodos de análise/avaliação
- Foco consiste no desempenho financeiro e não financeiro de Ativos, da Gestão de Ativos e do Sistema de Gestão de Ativos;
- Exigência de auditoria interna e análise crítica Comitê Gestor.

11.2.8. Melhoria - Os requisitos compreendem:

- Tratamento de não-conformidades;
- Estabelecimento de processos para identificação de potenciais Não - Conformidades e tomada de ações preventivas;
- Melhoria contínua dos ativos, da gestão de ativos e do sistema de gestão de ativos.

11.2.9. A Contratada deve implementar uma solução automatizada para a Gestão de Ativos.

11.3. A Contratada deverá prover a solução automatizada com as seguintes características:

- Necessário uma ferramenta para exploração de rede e auditoria de segurança para os ativos do tipo de tecnologia.
- Que seja desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais.
- Que utilize pacotes IP de maneira a determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso.
- Onde possa ser utilizado para auditorias de segurança, inventário de rede, gerenciamento de serviços de atualização agendados, e monitoramento de host ou disponibilidade de serviço.
- Possibilidade de gerenciar perímetros (por localidade, por organograma, por função etc.), ativos (tecnologia, pessoa, processo, ambiente ou customizado) e lista de verificação
- Possibilidade de gerenciar as pessoas e os grupos de pessoas do Contratante.
- Possibilidade de associar propriedades aos ativos, como: texto, data, número, arquivo, lista de opções etc.
- Exportação e Importação dos Ativos
    - Possibilidade de exportar, editar e importar informações da estrutura

organizacional e das pessoas usando uma planilha modelo.

- Possibilidade de integrar o inventário de ativos com lista a lista existente no Contratante (ex: Microsoft Active Directory, XML ou planilhas Excel).

11.3.1. Os dados coletados devem ser refinados e expostos em uma estrutura organizacional dos ativos, de acordo com as diretrizes da Governança do Ativo.

12. GESTÃO DE RISCOS

12.1. Objetivo do Serviço:

12.1.1. Este documento descreve o módulo de Gestão de Riscos referente a arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

12.1.2. O objeto desta contratação do serviço visa identificar, analisar, avaliar e criar workflow para tratamento dos riscos dos ativos de informação do objeto contido neste edital.

12.1.3. O processo de Gestão de Riscos irá subsidiar o processo de gestão de indicadores do Rio Digital.

12.2. Metodologia de Gestão de Riscos

12.2.1. A Contratada deve implementar uma solução automatizada para Gestão de Riscos em conformidade com as diretrizes sobre este item “Metodologia do Serviço de Gestão de Riscos”.

12.2.2. As diretrizes da metodologia de implementação do processo de Gestão de Riscos estão em conformidade com a ABNT NBR ISO 31000:2009. A utilização de um modelo baseado em padrões e metodologias formalizados, reconhecidos internacionalmente, é capaz de se adequar às estratégias, iniciativas e estrutura organizacional do Estado do RJ, além de atender às exigências dos órgãos reguladores e fiscalizadores da administração pública estadual.

12.2.3. O que são riscos?

- Riscos: O efeito das incertezas nos objetivos
- Riscos de Segurança da Informação: A possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo de informação ou de um conjunto de ativos, desta maneira causando prejuízo para o Estado do RJ.

12.2.4. A Metodologia de Gestão de Riscos permite identificar os riscos que podem causar impacto negativo nas atividades operacionais e administrativas ao Governo do Estado do RJ.

12.2.5. Consiste na aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

12.2.6. Segue abaixo o fluxograma da Gestão de Riscos de acordo com a ABNT NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes:

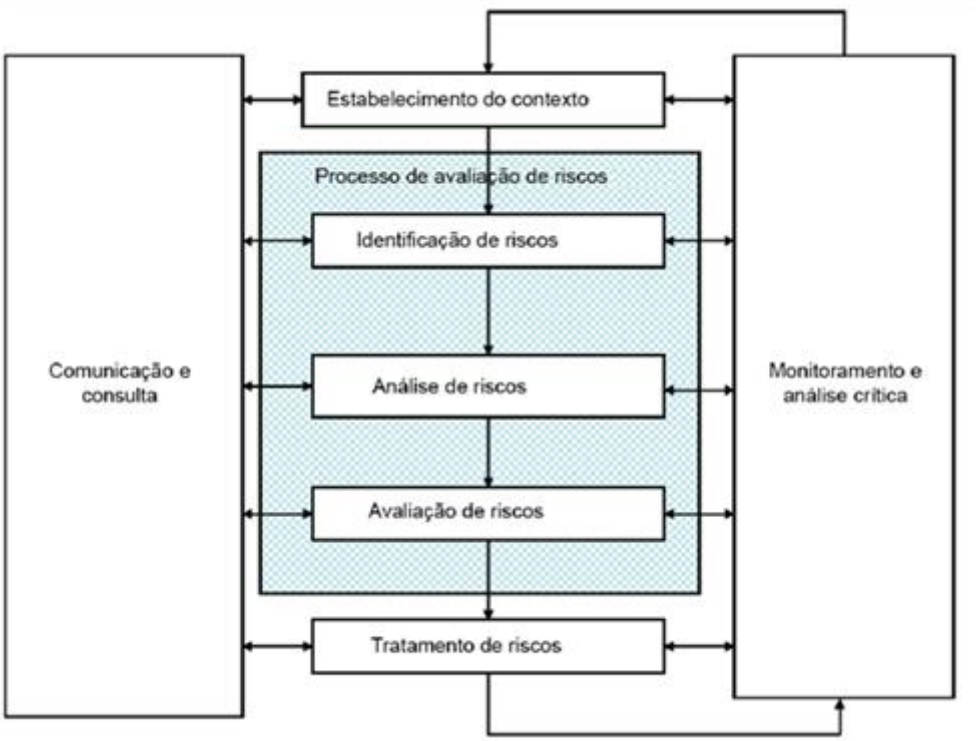


Figura 09 – Fluxograma de Gestão de Riscos

12.2.7. De modo geral, a Metodologia é um conjunto sequencial de ações ou atividades particulares com a finalidade de alcançar um determinado objetivo. Pode ser composto de uma ou mais entradas, que são processadas, retornando uma ou mais saídas. Para a presente contratação do serviço, o processo será dividido em subprocessos, que por sua vez poderão também ser subdivididos em outros subprocessos denominados etapas ou fases.

12.2.8. No caso da Metodologia de Gestão de Risco, ele é composto por 6 (seis) subprocessos a seguir descritos: definição de contexto, análise e avaliação de risco, tratamento de risco, aceitação de riscos, comunicação de risco e monitoração e análise crítica, conforme ilustrado abaixo na figura 10:

Figura 10 – Metodologia de Gestão de Riscos

12.2.9. Subprocesso "ESTABELECER CONTEXTO" - Contexto é um conjunto de circunstâncias que se relacionam de alguma forma com um determinado acontecimento. É a situação geral ou o ambiente a que está sendo referido um determinado assunto, neste caso a análise e avaliação de riscos. Denomina-se contextualização a atividade de mapear todo o ambiente que envolve o evento sob análise. Este subprocesso é composto de 3 (três) etapas, a saber: identificar as informações sobre o contexto interno e externo, definir os critérios da Gestão de Risco e, por último, mapear os ativos de informação, conforme ilustrado na figura 11.

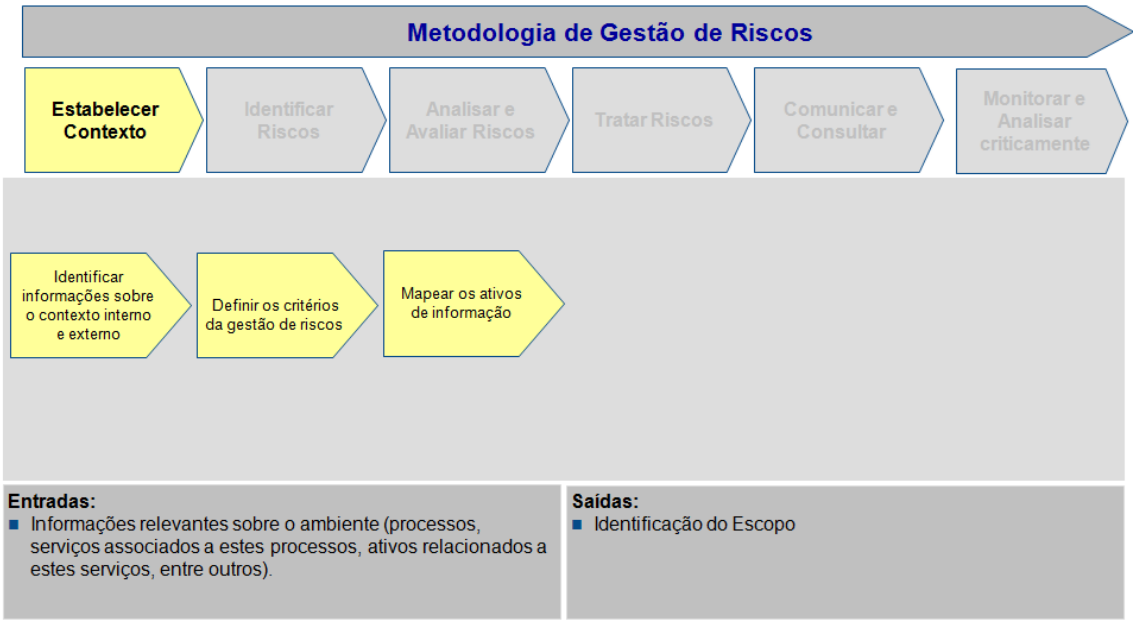


Figura 11 - Estabelecer o Contexto

12.2.9.1. Nas atividades que envolvem a Gestão de Riscos, o estabelecimento do contexto é a parte inicial e tem como objetivo permitir o conhecimento do ambiente da organização. Contextualização é a atividade de mapeamento de todo o ambiente que envolve o evento em análise. Além de identificar o contexto interno e externo do Contratante, os critérios da gestão de riscos deverão ser identificados e os ativos de informação mapeados.

12.2.9.2. Para identificar as informações sobre o contexto interno e externo, deverá ser realizada uma análise no ambiente interno pela equipe da contratada, identificando os elementos que caracterizam o Contratante e que contribuem para o seu desenvolvimento.

12.2.9.3. No que tange à etapa de definição de critérios da Gestão de Riscos, é importante ressaltar que os critérios fazem parte da Metodologia de Gestão de Riscos e são a forma e o valor (pesos) com que os riscos e impactos serão valorados.

12.2.9.4. Quanto à etapa de identificação dos ativos, deve ser feita em um nível de detalhamento que permita o fornecimento de informações adequadas e suficientes para a análise e avaliação de riscos. Devem ser listados os ativos de informação considerados críticos pelo contratante e, também, uma lista de componentes organizacionais que este ativo suporta.

12.2.9.5. A solução automatizada de gestão de riscos deve identificar os ativos de informação que farão parte do escopo da análise e avaliação de riscos. Também deverá ser organizada toda a análise e avaliação dos ativos de informação do escopo.

12.2.10. Subprocesso “IDENTIFICAR RISCOS” - A Contratada deve identificar as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. A Contratada irá aplicar ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados. Informações pertinente e atualizadas são importantes na identificação de riscos. Convém que incluam informações adequadas sobre os fatos por trás dos acontecimentos, sempre que possível. Convém que pessoas com um conhecimento adequado sejam envolvidas. Este subprocesso é composto de 3

(três) etapas, a saber: identificar as ameaças envolvidas; as vulnerabilidades existentes nos ativos de informação; e os controles de Segurança da Informação já implantados, conforme ilustrado na figura 12.

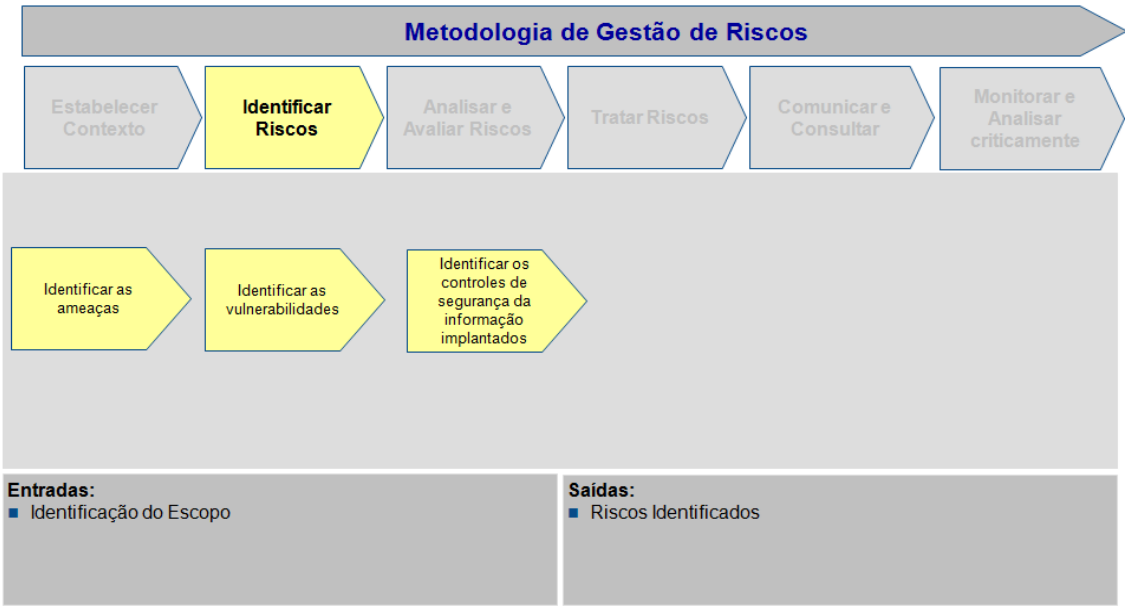


Figura 12 – Identificação de Riscos

12.2.10.1. A contratada deve identificar todas as ameaças que podem causar impacto no escopo da análise e avaliação de Riscos, pois são essas ameaças identificas que podem explorar as vulnerabilidades causando prejuízo para os processos de negócio do contratante. Uma ameaça tem o potencial de comprometer os ativos de informação e, por isso também os processos de negócio do contratante. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais.

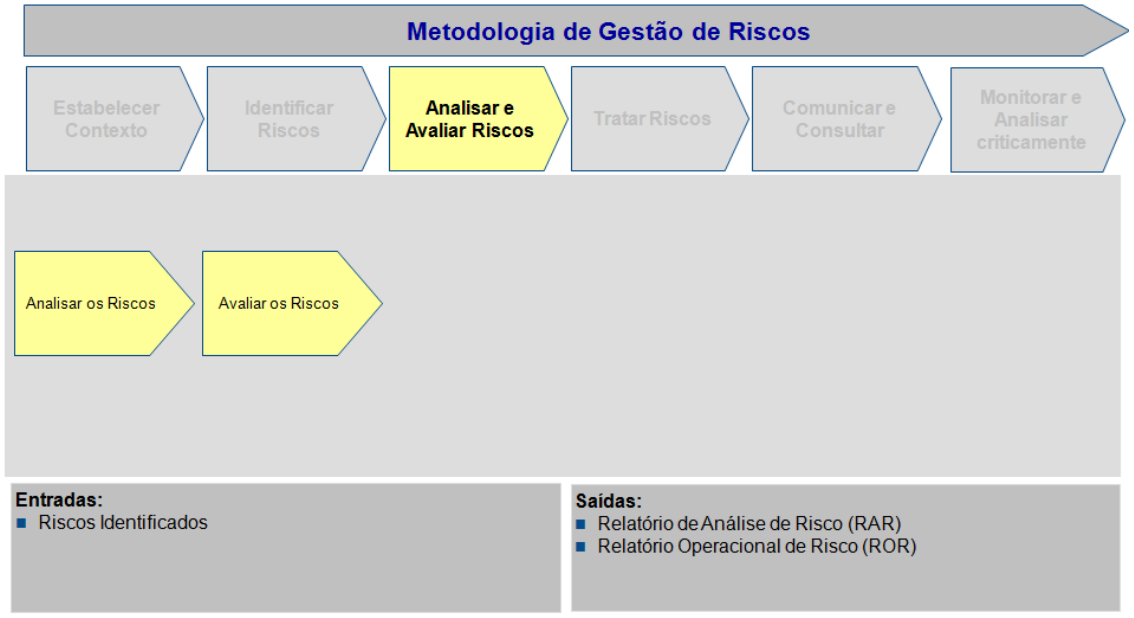
12.2.10.2. A contratada deve identificar todas as fontes das ameaças acidentais, quanto as intencionais. Uma ameaça pode surgir de dentro ou fora da Contratante. Algumas ameaças podem afetar mais de um ativo de informação. Nesses casos, elas podem provocar impactos diferentes, dependendo de quais ativos são afetados.

12.2.10.3. A contratada deve identificar as vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos de informação e os processos de negócio do contratante. Vulnerabilidades podem ser identificadas nas seguintes áreas: Organização (Contratante), em pessoas, processos e procedimentos, rotinas de gestão, recursos humanos, ambiente físico, configuração do sistema de informação, hardware,

software ou equipamentos de comunicação e dependência de entidades externas.

12.2.10.4. A contratada deve verificar os controles existentes seja realizada para evitar custos e trabalho desnecessários, por exemplo: na duplicação de controles. Além disso, enquanto os controles existentes estão sendo identificados, convém que seja feita uma verificação para assegurar que eles estão funcionando corretamente. Um controle que não funcione como esperado pode provocar o surgimento de vulnerabilidades.

12.2.11. Subprocesso ANALISAR E AVALIAR RISCOS - Este subprocesso visa produzir os dados que auxiliarão na decisão sobre quais riscos serão tratados e quais formas de tratamento serão empregadas. Também se subdivide em duas etapas, a saber: análise e avaliação dos riscos, conforme ilustrado na figura 13.



F

Figura 13 – Análise e Avaliação de Riscos

12.2.11.1. A solução automatiza de gestão de riscos da Contratada deve calcular o nível de riscos exponencial de cada risco identificado, de forma que seja aderente às normas ABNT NBR ISO/IEC 27005:2011, ABNT NBR ISO 31000:2009 e ISO Guide 73:2009. O cálculo do nível do risco deve ser aplicável aos ativos de informação tecnológicos, de ambiente físico, processo e pessoas da Contratante.

12.2.11.2. A solução automatiza de gestão de riscos da Contratada deve utilizar um método de Análise de Riscos qualitativa que calcula um índice ("rating") denominado PSR® (Probabilidade, Severidade e Relevância). Este índice define o Risco para cada Controle ausente encontrado na Análise. Da fórmula do Risco:

- RISCO = PROBABILIDADE X IMPACTO

12.2.11.3. A solução automatiza de gestão de riscos da Contratada deve determinar o valor do impacto no negócio é atendido pelas duas variáveis S e R, Severidade e Relevância respectivamente, e esta fórmula do Risco é calculada então pela seguinte equação:

- RISCO = PROBABILIDADE X SEVERIDADE X RELEVÂNCIA

12.2.11.4. A solução automatiza de gestão de riscos da Contratada deve considerar que a ausência de Controle de Segurança da Informação representa uma ou mais vulnerabilidades associadas ao Controle. Caso não exista a vulnerabilidade associada à falta de um Controle específico em algum ambiente, então o Controle deve ser considerado como Não Aplicável - N/A.

12.2.11.5. Após a conclusão da etapa anterior a Contratada deve emitir dois relatórios/produtos:

- Relatório de Análise de Risco (RAR) onde é apresentado, de forma consolidada, o resultado da análise do nível atual do risco dos ativos do Contratante e os riscos encontrados nos componentes de negócio, bem como, a consolidação por tipo de ativo de informação.

- Relatório Operacional de Risco (ROR), onde é apresentado o detalhamento das ações e controles que devem ser implementados para eliminar ou mitigar os riscos.

12.2.11.6. A etapa de avaliação de riscos tem por objetivo comparar os níveis de riscos identificados na fase anterior com os critérios de avaliação e aceitação de riscos e obter uma lista de riscos ordenados por prioridade.

12.2.11.7. Após a emissão dos relatórios, o Contratante avalia e verifica se o nível de risco está dentro dos padrões definidos no contexto interno e externo para a análise e avaliação de riscos para cada um dos ativos de informação que estão no escopo determinado.

12.2.12. Subprocesso TRATAR RISCOS - Este subprocesso visa relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na definição de escopo, detalhados na figura 5. É composto de 2 (duas) etapas, a saber: determinar a forma de tratamento dos riscos, obter parecer do proprietário do ativo de informação, conforme ilustrado na figura 6.

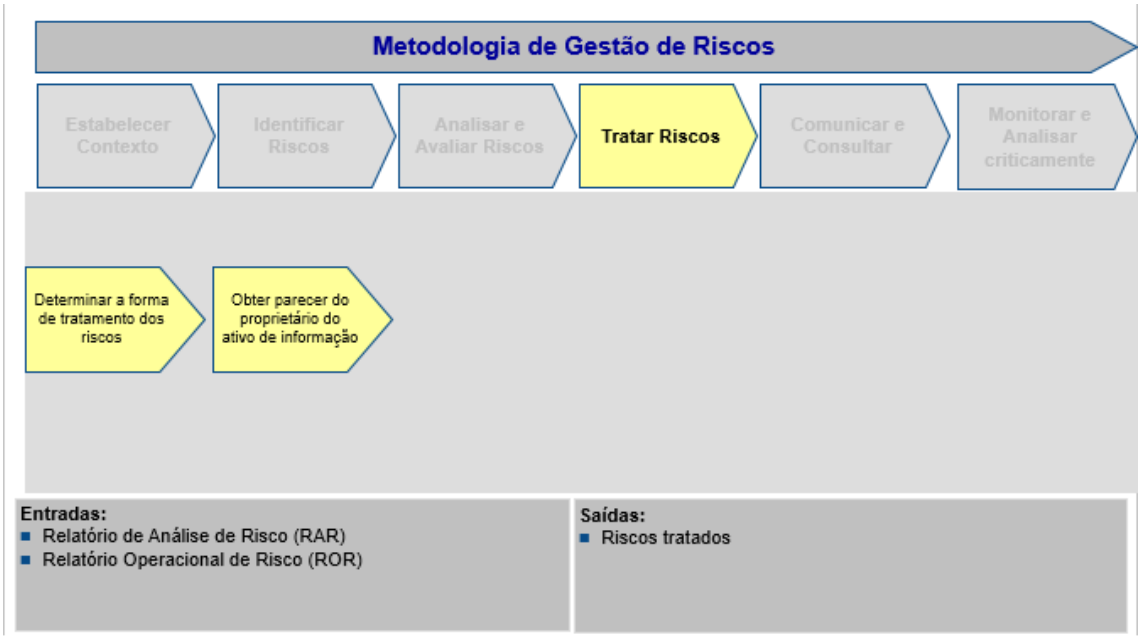


Figura 14 – Metodologia de Gestão de Riscos

12.2.12.1. Em relação ao subprocesso “Determinar a forma de tratamento de risco”, para cada risco identificado deverá ser informada a ação de tratamento. A solução automatizada da contratada deve informar detalhadamente toda as informações de tratamento para cada risco identificado. Estas informações devem estar descritas no Relatório Operacional de Risco (ROR).

12.2.12.2. O subprocesso de tratamento de risco é realizado após os subprocessos de estabelecimento do contexto e análise/avaliação de riscos. Ao final, a Contratada deverá fazer uma análise crítica dos resultados a fim de verificar a situação dos trabalhos desenvolvidos. Caso essa análise se mostre insatisfatória, deve-se retornar ao início do processo, para ajustes.

12.2.12.3. O Contratante deverá emitir parecer sobre os riscos identificados nos

ativos de informação sob sua responsabilidade. Este poderá concordar ou não em relação aos riscos identificados.

12.2.12.4. O Contratante é responsável pelo tratamento dos riscos dos ativos sob a sua responsabilidade.

12.2.12.5. A Contratada deverá tratar os riscos dos ativos sob a sua responsabilidade, como por exemplo, dos equipamentos de monitoração de redes.

12.2.13. Subprocesso COMUNICAR E CONSULTAR - A Gestão de Riscos pode ter diversas partes interessadas. Essas partes devem ser identificadas e seus papéis e responsabilidades delimitados. Os riscos serão comunicados para os seus respectivos responsáveis. Assim, o subprocesso de comunicar e consultar se encarrega de proporcionar essa comunicação, sendo composta de duas etapas: a primeira relativa à identificação das partes interessadas e a outra efetivamente associada à comunicação, ambas ilustradas na figura 15.

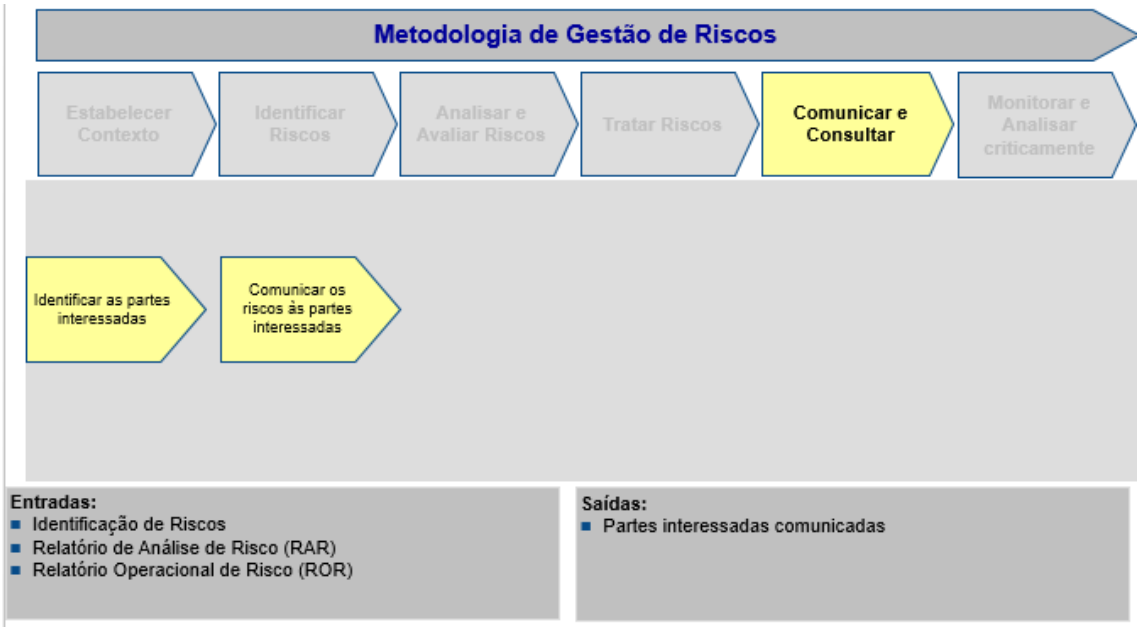


Figura 15 – Comunicar e Consultar os Riscos.

12.2.13.1. A comunicação do risco é uma troca interativa, documentada formalmente, contínua e intencional de informações, conhecimentos e percepções sobre como os riscos devem ser gerenciados.

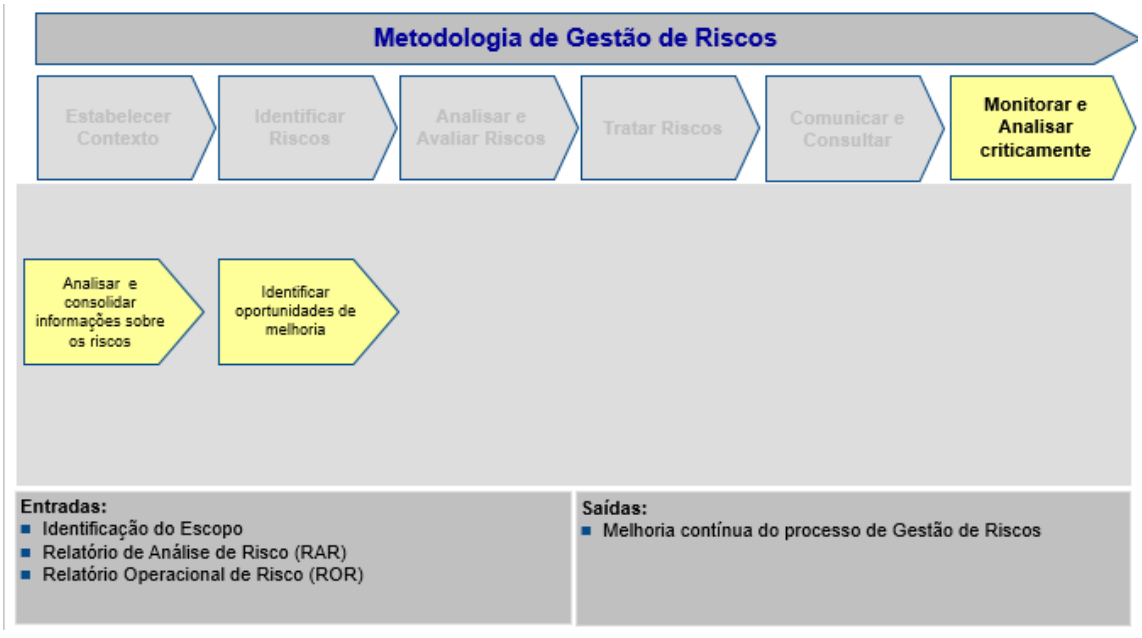
12.2.13.2. A comunicação é realizada entre a Contratada, a Contratante e as partes interessadas nas decisões dos processos de negócio que estão no contexto da análise e avaliação de riscos, por isso as partes interessadas deverão ser identificadas e documentadas.

12.2.13.3. A Contratada é a responsável pela comunicação com as partes interessadas.

12.2.13.4. No que tange à comunicação dos riscos às partes interessadas, esta etapa deverá abordar com o máximo de detalhes os riscos encontrados, informando:

- A existência da ameaça, vulnerabilidade e risco;
- A natureza e forma de ação;
- A estimativa de probabilidade;
- Sua severidade e consequências possíveis; e
- Tratamento e aceitação de riscos.

12.2.14. Subprocesso MONITORAR E ANALISAR CRITICAMENTE - Intrínseco a todo processo, a retroalimentação é necessária para corrigir e aperfeiçoar o próprio processo. Assim, permite detectar possíveis falhas nos resultados, monitorar os riscos, os controles de segurança da informação e verificar a eficácia do processo de Gestão de Riscos. Subdivide-se em duas etapas,



conforme ilustrado na figura 16.

Figura 16 – Monitorar e Analisar Criticamente o processo de Gestão de Riscos

12.2.14.1. Após o tratamento dos riscos, é necessário consolidar informações sobre o processo e identificar oportunidades de melhoria.

12.2.14.2. Na etapa de “Analisar e Consolidar Informações sobre os Riscos" deve-se identificar e quantificar os indicadores do processo no documento de Relatório Executivo da Análise.

12.2.14.3. Quanto à etapa “Identificar Oportunidades de Melhoria”, deve-se analisar as informações consolidadas do processo, através dos seus indicadores, e identificar oportunidades de melhoria.

12.3. A Contratada deverá prover a solução automatizada com as seguintes características:

- Para quantificar os riscos associado a um ativo, a solução automatizada deve utilizar métricas diferentes de acordo com o tipo de informação que se queira analisar. São elas: Índice de Riscos, Índice de Segurança, Índice de Não Conformidade e Índice de Conformidade.

- Possibilitar a classificação das medidas de segurança conforme métricas de probabilidade, impacto e importância do ativo.

- Possibilitar análises de riscos baseado em Catálogo de Riscos, a partir da classificação e categorização dos riscos.

- Os projetos de riscos em ativos devem ser criados para determinar o nível de exposição dos ativos do Contratante às ameaças existentes e quantificar o impacto ao qual a organização estará sujeita se as vulnerabilidades dos ativos forem exploradas por essas ameaças. Os projetos devem ser visualizados, criados, editados, fechados, cancelados, excluídos e reabertos.

- Deve ser possível criar diferentes tipos de escopo por projeto de análise de risco a ser executado.

- Devem existir diferentes tipos de consultas: as que consolidam os resultados das análises de riscos, as que exibem os resultados das análises de riscos para os requisitos mapeados aos controles, as que exibem estatísticas de entrevistas realizadas nos ativos, as que exibem informações sobre a situação geral dos controles ou as que também utilizam os resultados das análises de riscos.

- Possibilitar a criação de entrevistas - com a geração de formulário web customizado - em diferentes formatos, para a coleta de informações da análise de risco em pessoas, processos, ambientes e tecnologia, com a possibilidade de monitorar o recebimento, o preenchimento e o envio das respostas das entrevistas e incluir um revisor para aprovar as respostas.

- Devem existir coletores automáticos para a análise em ativos tecnológicos, nas principais tecnologias (Sistemas Operacionais, Bancos de Dados, Servidores Web, Ferramenta de Escritório, Firewall, Roteadores, Switches etc), conforme lista de verificação requeridos no próximo requisito.

- Permitir a inclusão de fotos e arquivos de evidências em análises de riscos.

- A solução automatizada deve possibilitar a geração de diferentes tipos de relatórios (Relatório Técnico de Riscos, Relatório Gerencial de Riscos, Relatório Executivo de Riscos).

- Deve possibilitar a total customização de relatórios incluindo: formatação, inclusão e exclusão de campos, inserção de gráficos etc.

- Deve poder gerar os relatórios nos formatos RTF, PDF e Planilha.

- Deve possibilitar o agendamento da geração de relatórios por período, com o envio de alerta por correio eletrônico.

13. CENTRO DE MONITORAMENTO DE SEGURANÇA CIBERNÉTICA DE REDES DE TELECOMUNICAÇÕES

13.1. Objetivo do Serviço:

13.1.1. Este documento descreve o módulo de Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações referente a arquitetura de serviços que comporá a Gestão Integrada do projeto Rio Digital.

13.1.2. O objeto desta contratação visa monitorar e controlar os ativos de rede de telecomunicações, além de tratar os incidentes cibernéticos que forem identificados pelo centro de monitoramento de segurança cibernética, este centro terá capacidade de gerenciar integralmente toda a arquitetura e componentes envolvidos na prestação do serviço contratado.

13.1.3. Este centro de monitoramento irá subsidiar com informações e dados coletados o processo de gestão de indicadores do Rio Digital.

13.2. Metodologia de trabalho do Centro de Monitoramento de Segurança Cibernética

13.2.1. A Contratada deve implementar o Centro de Monitoramento de acordo com as diretrizes da Norma brasileira ABNT NBR ISO/IEC 27032:2015 - Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética.

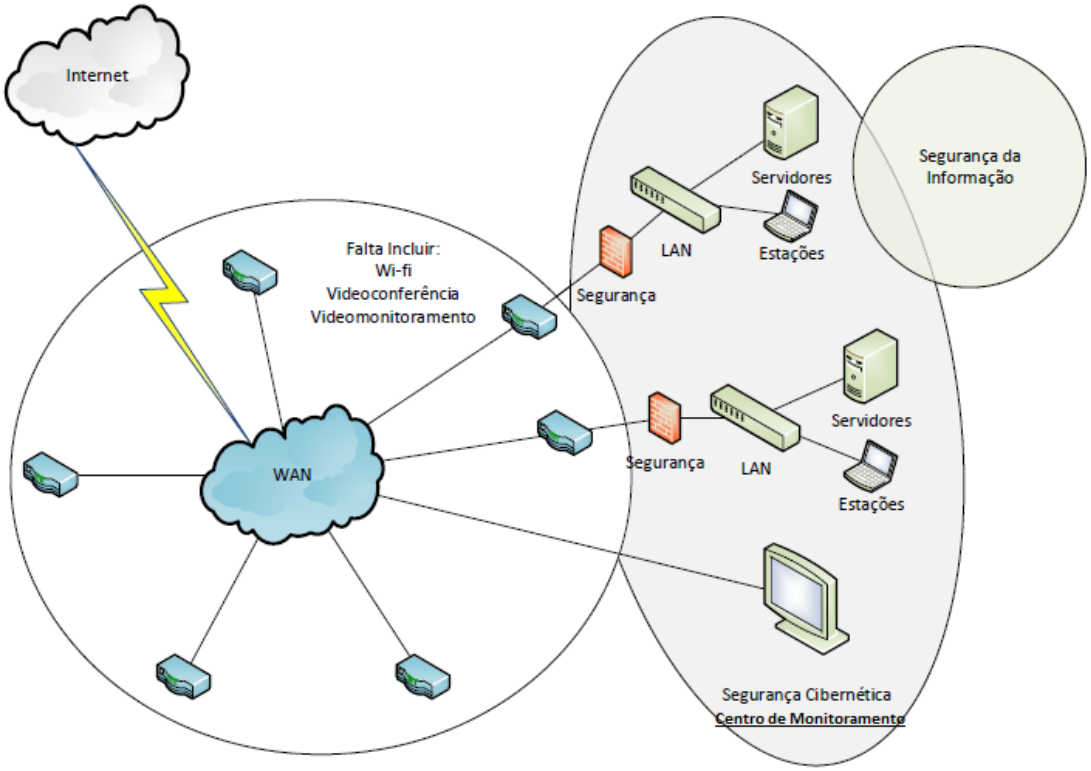
13.2.2. A Contratada deve implementar o Centro de Monitoramento de Segurança Cibernética com 5 funções, utilizando como modelo de referência o Framework de Infraestrutura crítica de Segurança Cibernética do National Institute of Standards and Technology (NIST), que sintetiza os fatores impulsionadores a fim de guiar as atividades e serve de base para que a Contratante considere formalmente o risco de segurança como parte do seu processo de gerenciamento de riscos. Essas funções sintetizam as atividades necessárias para atingir resultados específicos em matéria de segurança cibernética; as funções simultâneas e contínuas: identificação, proteção, detecção, resposta e recuperação. Segue abaixo as principais definições:

- **Identificação** - Desenvolver a compreensão organizacional para gerir o risco para sistemas, ativos, dados e capacidades. As atividades da função identificação são fundamentais para o uso eficaz da Infraestrutura do Centro de Monitoramento, e para entender o contexto empresarial e os recursos que suportam. Os riscos de segurança cibernética relacionados permitem que a Contratante possa se concentrar e priorizar seus esforços, de acordo com a sua estratégia e necessidades de negócios.
- **Proteção** - Desenvolver e implementar as salvaguardas apropriadas para garantir a entrega de serviços da infraestrutura crítica. A função de proteção suporta a capacidade de limitar ou conter o impacto de um potencial incidente de segurança cibernética.
- **Detecção** - Desenvolver e implementar as atividades apropriadas para identificar a ocorrência de um incidente de segurança cibernética, por intermédio de um monitoramento contínuo das ameaças.
- **Resposta** - Desenvolver e implementar as atividades apropriadas a tomar medidas para conter um incidente segurança que esteja ocorrendo. Contendo assim, o impacto que possa trazer prejuízos para o Contratante.
- **Recuperação** - Desenvolver e implementar as atividades adequadas para restaurar quaisquer recursos ou serviços que foram prejudicadas devido a um incidente de segurança cibernética.

13.2.3. Por intermédio da metodologia acima, a Contratada deve implementar uma Segurança Cibernética com um tempo de reação adequado para tratar os

incidentes, por intermédio de emissão de alarmes cibernéticos. Algumas das atividades que podem vir a ser implementadas no centro de monitoramento estão descritas a seguir:

- Implementar um monitoramento com Videowall ou TV´s para monitoramento em tempo real das ameaças cibernéticas.
- Implementar dispositivos de conectividade para a rede de telecomunicações do Centro. Os links de comunicação do centro devem ser redundantes.
- O centro deve monitorar a disponibilidade de todos os seus ativos e os ativos da contratante sob a sua responsabilidade.
- O Centro deve implementar um storage para armazenamento de logs de dados e verificação de eventos de segurança cibernética.
- Reduzir e controlar as saídas para a Internet, registrar e monitorar dispositivos móveis e acessos por celular são cruciais para evitar o bypass da segurança de perímetro como Firewall, IPS.
- O Monitoramento contínuo 24/7/365 é imprescindível para o acompanhamento em tempo real dos incidentes de rede e de segurança cibernética provendo a remediação oportuna e tempestiva para cada potencial dano aos requisitos básicos de segurança já citados. Detectar e reagir reduz o tempo de resposta à incidentes, minimiza as janelas de vulnerabilidades e mantém a disponibilidade dos serviços para os clientes finais da Contratante. O tempo de reação em um centro de monitoramento é o elemento fundamental para atingir com sucesso o seu objetivo, de proteção da rede de telecomunicação.
- Configurar os controles de segurança e otimizar os links MPLS são fundamentais para a confidencialidade do tráfego passante, inclusive em ligações VOIP e Vídeos conferências, bem como mantém o tráfego em uso com prioridades (QoS).
- Uma gestão de ameaças (Inteligência Cibernética) é muito importante para priorizar ações defensivas e reduzir o sucesso de ataques cibernéticos. Para tal, um monitoramento de ameaças (Cyber Threat Intelligence) em fontes abertas (OSINT) é recomendado para a Infraestrutura das redes de telecomunicações.
- Com todas essas medidas preventivas, reativas e antecipativas, constrói-se uma metodologia de monitoramento cibernético em tempo real baseada em alarmes.
- Os alarmes cibernéticos devem possuir uma leitura executiva, facilitar o processo decisório e o estabelecimento de contramedidas pré-concebidas e/ou adaptativas, envolvendo o Comitê Gestor, quando necessário.
- Por último, o estabelecimento de mecanismos de defesa contra ameaças avançadas, atualmente, deixou de ser um investimento e passou a ser uma necessidade cada vez mais urgente para a Contratante, pois as redes de telecomunicações apresentam alto risco de ataques cibernéticos.



13.2.4. Segue abaixo de forma gráfica, um diagrama de onde o Centro de Monitoramento irá trabalhar executando suas funções e serviços.

Figura 17 – Centro de Monitoramento – Segurança Cibernética

13.2.5. A implementação do Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações deve englobar, no mínimo, os seguintes passos e capacidades:

- Capacitação e disponibilização de profissionais para operação do centro;
- Softwares necessários para suporte da operação do centro;
- Inventário de todos os ativos de TIC diretamente envolvidos na prestação do serviço;
- Identificação da situação de cada ativo / componente / sistema inventariado através da aplicação de questionários para identificação de riscos e não conformidades;
- Monitoramento em tempo real em Telas apropriadas de todos os ativos envolvidos;
- Apresentação de alarmes visuais da ocorrência de problemas;

- Abertura e acompanhamento de trouble tickets para a resolução de problemas;
- Despacho de técnicos de campo para resolução de problemas;
- Monitoramento dos acordos de nível de serviços (SLAs) do serviço, este tema estará sendo detalhado no capítulo de Gestão de SLA do Termo de referência;
- Geração de relatórios e estatísticas.

13.2.6. Além dos serviços já descritos neste documento, o Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações deve ter implementado, no mínimo, os seguintes serviços:

- Monitoramento de rede, de tráfego, performance e anomalias.
- Monitoramento de ameaças cibernéticas.
- Gestão de Ativos em conformidade com a Norma ABNT NBR ISO 55000:2014 - Gestão de ativos — Visão geral, princípios e terminologia e na ABNT NBR ISO 55002:2014 - Gestão de ativos — Sistemas de gestão — Diretrizes para a aplicação da ABNT NBR ISO 55001.
- Gestão de Riscos em conformidade com a Norma ABNT NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes.
- Gestão de Conformidade que visa verificar a conformidade de leis, regulamentos da administração estadual e órgãos de controle e procedimentos internos da infraestrutura da Contratante.
- Gestão de Continuidade de Negócios em conformidade com a ABNT NBR ISO 22301:2013 - Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos.
- Gestão de Segurança da Informação em conformidade com a ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e na ABNT NBR ISO/IEC 27011:2009 - Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.
- Governança de Tecnologia da Informação e Comunicação em conformidade com as diretrizes da ABNT NBR ISO/IEC 38500:2009 - Governança corporativa de tecnologia da informação e com o Control Objectives for Information and Related Technology (Cobit) versão 5.
- Gestão de projetos em conformidade com as diretrizes da Norma brasileira ABNT NBR ISO 21500:2012 - Orientações sobre gerenciamento de projeto e o Project Management Body of Knowledge (PMBOK).
- Gestão de indicadores em conformidade com a ABNT NBR ISO/IEC 27004:2010 -

Tecnologia da informação — Técnicas de segurança — Gestão da segurança da informação — Medição para envio para o Comitê Gestor.

- Gestão de serviços em conformidade com as diretrizes de implantação do Information Technology Infrastructure Library (ITIL) na sua versão 3.0.

13.3. A contratada deve implementar uma solução automatizada para otimizar a gestão dos softwares e hardwares citados no capítulo 13 deste documento.

13.4. Montagem do Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações.

Considerando a necessidade de um ambiente físico na cidade do Rio de Janeiro para implantar o Centro de Monitoramento de Segurança Cibernética de Redes de Telecomunicações.

Incluindo no mínimo:

Preparação de toda a infraestrutura física para a montagem do centro:

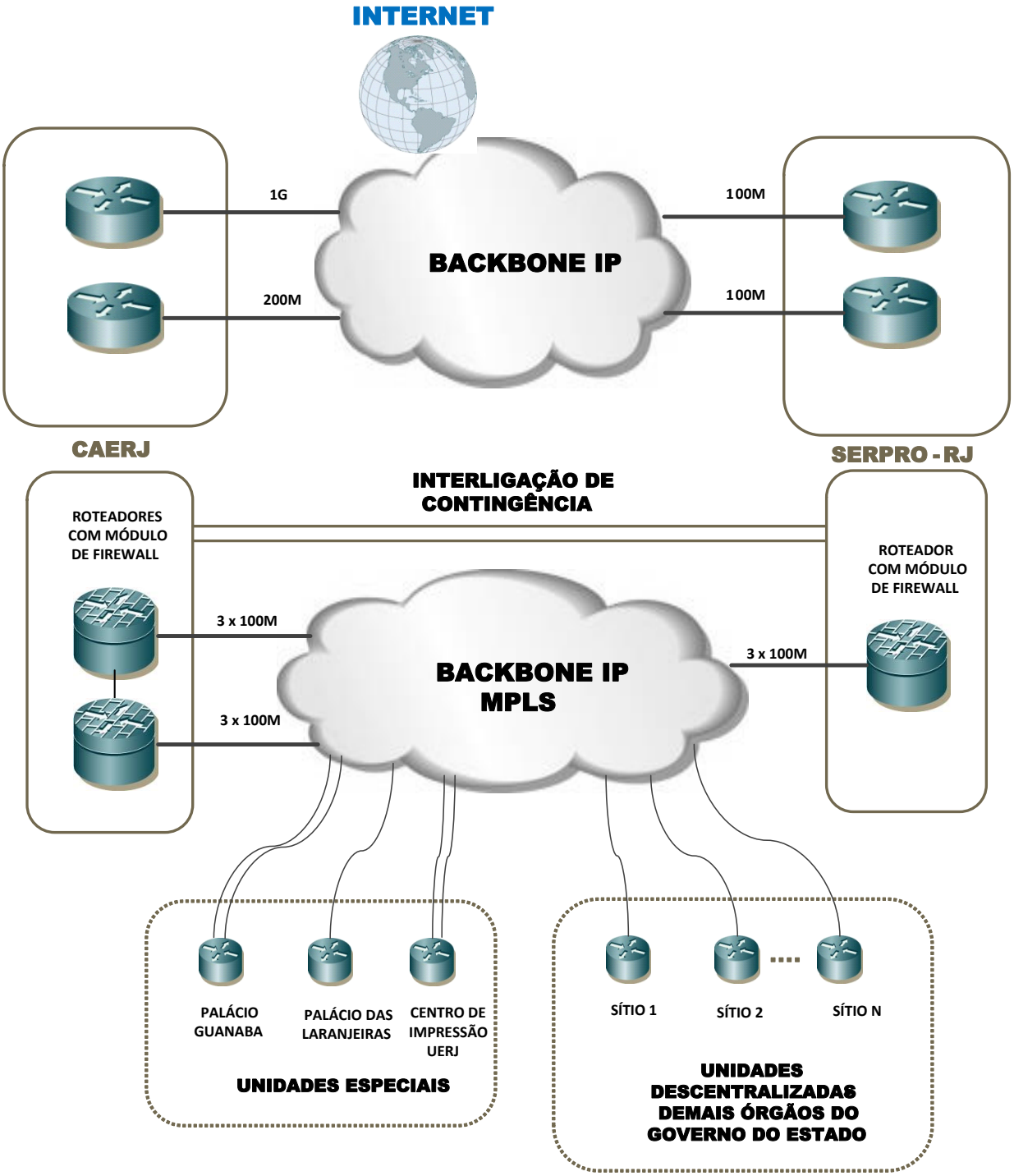
- Hidráulica
- Ambiente de trabalho
- Climatização
- Infraestrutura predial
- Incidentes de segurança
- Energia e circuitos elétricos
- Controle de acesso e segurança física do prédio onde será alocado o Centro
- Cabeamento estruturado
- Mobiliário de mesas e cadeiras

A Contratada deverá propor a adequação do ambiente ofertado pela Contratante para tal finalidade, após a devida vistoria.

14. REDE ATUAL

14.1. Topologia

A seguir, o desenho esquemático da topologia atual da rede de comunicação de dados.


INTERNET
1G
200M
BACKBONE IP
100M
100M
CAERJ
SERPRO - RJ
INTERLIGAÇÃO DE CONTINGÊNCIA
ROTEADORES COM MÓDULO DE FIREWALL
ROTEADOR COM MÓDULO DE FIREWALL
3 x 100M
3 x 100M
BACKBONE IP MPLS
3 x 100M
PALÁCIO GUANABA
PALÁCIO DAS LARANJEIRAS
CENTRO DE IMPRESSÃO UERJ
UNIDADES ESPECIAIS
SÍTIO 1
SÍTIO 2
SÍTIO N
UNIDADES DESCENTRALIZADAS DEMAIS ÓRGÃOS DO GOVERNO DO ESTADO

O Core da Rede Governo contempla os Datacenter Principal e site de Contingência.

- Site Principal – Localizado no município do Rio de Janeiro
- Site Contingência – Localizado no município do Rio de Janeiro

  Os endereços serão fornecidos no tempo oportuno.

14.2. As Unidades Especiais da Rede Governo comtemplam os seguintes sites:

- **Palácio Guanabara:** Rua Pinheiro Machado, SN, Laranjeiras, Rio de Janeiro – RJ.
- **Palácio das Laranjeiras:** Rua Paulo Cesar de Andrade, 407, Laranjeiras, Rio de Janeiro – RJ.
- **Centro de Impressão UERJ:** Rua São Francisco Xavier, 524, Maracanã, Rio de Janeiro – RJ.

15. MODELO DE CONTRATAÇÃO

15.1. O objeto deste certame engloba a formação de Ata de Registro de Preços para futura prestação de serviços.

15.2. Deverá ser celebrado pela Licitante vencedora com o PRODERJ um Contrato Principal que servirá de base para a adesão de todos os Órgãos da administração direta e indireta do Governo do Estado do Rio de Janeiro.

15.3. Os Contratos de cada Órgão com a Licitante vencedora serão termos aditivos ao Contrato Principal. Deste modo, seu término de vigência deverá obedecer a do Contrato Principal.

15.4. Tomando como base as características atuais da Rede Governo do Estado do Rio de Janeiro, e considerando a expectativa de crescimento a utilização dos serviços providos hoje, optou-se por registrar patamares de larguras de banda que poderão ser contratados oportunamente de acordo com a necessidade e o perfil de tráfego dados.

15.5. Os serviços serão prestados conforme especificado neste TERMO DE REFERÊNCIA e respeitando tabela de formação de preços do edital.

15.6. Deverá ser registrado o valor mensal unitário para cada item.

15.7. Observar que a Licitante deverá se comprometer com o atendimento eventual de expansão de bandas e serviços, a adição de futuros endereços durante a vigência do contrato, nas mesmas condições técnicas e de preços oferecidos para o objeto do Edital, respeitados os limites legais e técnicos.

15.8. Os endereços foram levantados no momento da elaboração do TERMO DE REFERÊNCIA e podem sofrer alterações ao longo da execução do projeto e do Contrato.

15.9. De forma a permitir a análise da viabilidade e correto dimensionamento dos custos e despesas provenientes da solicitação, a CONTRATADA deverá providenciar a elaboração do Projeto Executivo contendo o plano de implantação desses serviços.

15.10. Os serviços contemplados neste edital incluídos no Anexo A - Catálago de serviços poderão ser cancelados em até 2% de todo o edital considerando a viabilidade técnica e/ou manutenção do equilíbrio técnico-financeiro do contrato a ser estabelecido com a licitante vencedora.

15.11. Outros tipos de serviços e funcionalidades não relacionadas na presente descrição do Termo de Referência mais que sejam complementares as existentes poderão ser objeto de aditivo contratual.

16. LEIS, NORMAS E REGULAMENTOS APLICÁVEIS

O presente TERMO DE REFERÊNCIA guarda fundamento nos seguintes normativos:

16.1. Lei nº 8.666/1993: Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

16.2. Lei nº 10.520/2002: Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.

16.3. Decreto nº 3.555/2000: Regulamenta a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

16.4. Decreto n° 7.892/2013: Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993.

17. DA QUALIFICAÇÃO TÉCNICA

Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto desta licitação, por meio da apresentação de:

17.1. Atestado ou declaração de capacidade técnica de pessoa Jurídica Pública ou Privada, em nome da Licitante, que comprove a prestação de serviços de rede Corporativa IP MPLS para cliente abrangendo a quantidade de circuitos previstos no Edital, velocidades e tecnologias.

17.2. Atestado ou declaração de capacidade técnica, em nome da licitante, que comprove a prestação de serviços de acesso à internet abrangendo quantidade de tecnologias, acessos, velocidades.

17.3. Declaração que comprove a capacidade de troca de tráfego do Backbone IP da Contratada com outros Backbone conforme especificado no Edital.

18. PROJETO EXECUTIVO

18.1. O Projeto Executivo deve conter, no mínimo, as seguintes informações:

- Projeto técnico de implantação dos serviços denominado Relatório de Organização e Planejamento;
- Cronograma de implantação dos serviços;
- Escopo dos serviços;
- Descrição da equipe técnica responsável pela gestão de implantação indicando funções e responsabilidades;
- Descrição dos níveis de serviço acordados;
- Riscos identificados;
- Plano de comunicação.

18.2. Este item deverá estar em conformidade com as diretrizes do Project Management Office ou similar do Rio Digital.

18.3. Uma vez apresentado, o projeto executivo será submetido à aprovação da equipe técnica do Estado do RJ, que detectará os ajustes, se necessários. A CONTRATADA deverá corrigi-lo e reapresentá-lo em até no máximo 15 (quinze) dias úteis.

19. OBRIGAÇÕES DA CONTRATADA

19.1. A CONTRATADA será responsável pela prestação dos serviços contemplados neste Edital, conforme prazos, especificações, garantias e ritos estabelecidos neste TERMO DE REFERÊNCIA.

19.2. A CONTRATADA ficará obrigada a manter sigilo sobre todas as informações referentes à solução implantada, bem como acerca das instalações da Rede Governo, sendo vedada qualquer divulgação destas informações sem prévia autorização, por escrito, do Órgão responsável.

19.3. A CONTRATADA deverá assinar o documento Termo de Confidencialidade e Sigilo e entregá-lo ao PRODERJ com firmas reconhecidas em cartório, até a data marcada para a reunião (Kick-off) do projeto.

Consiste em condição para a prestação de todos os serviços, estabelecendo sigilo das informações do ambiente da CONTRATANTE, com acesso mínimo e restrito aos técnicos designados para a prestação dos serviços.

19.4. Respeitar a Política de Segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.

19.5. Destaca-se que o CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

19.6. Para cada um dos acessos contratados deverão ser prestados serviços de ativação dos circuitos de comunicação de dados, bem como instalação e configuração dos equipamentos.

19.7. A passagem doa cabos para prestação dos Serviços serão de responsabilidade da CONTRATADA, sendo recomendada vistoria para verificação das condições de infraestrutura predial do Backbone da Rede Governo.

19.8. A contratada deverá disponibilizar uma equipe capacitada para elaborar o Projeto Executivo e acompanhar todo o processo de implantação do RIO DIGITAL. A

19.9. A implantação dar-se-á após a aprovação do Projeto Executivo e do cronograma alinhado entre as partes.

19.10. Toda informação referente à CONTRATANTE que a CONTRATADA vier a tomar conhecimento por necessidade de execução dos serviços ora contratados não poderá ser divulgada a terceiros sem autorização expressa do PRODERJ.

19.11. A CONTRATANTE terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação, que devem ser gerados e entregues de acordo com os padrões e formatos definidos pela CONTRATANTE.

19.12. Os recursos de TIC não poderão ser utilizados pela CONTRATADA para realização de atividades alheias aos serviços previstos ou englobados nesta contratação.

19.13. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinente à execução dos serviços, que venham porventura serem solicitados pelo PRODERJ.

20. OBRIGAÇÕES DA CONTRATANTE

20.1. A CONTRATANTE responderá pela gestão contratual e a fiscalização da entrega dos itens da contratação.

20.2. A CONTRATANTE compromete-se a proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitindo o acesso dos técnicos, prepostos ou representantes da CONTRATADA às dependências da CONTRATANTE.

20.3. Promover os pagamentos dentro dos prazos estipulados.

20.4. Prestar as informações e os esclarecimentos solicitados pela CONTRATADA para a fiel execução do contrato.

20.5. A CONTRATANTE deverá prover as condições de infraestrutura física em seu ambiente, como tubulações, energia elétrica e climatização adequada para que o serviço possa ser prestado pela CONTRATADA.

21. PROCEDIMENTOS DE ACEITAÇÃO DOS SERVIÇOS

21.1. A aceitação dos serviços em carácter Provisório ou Definitivo pela PRODERJ deve obedecer aos procedimentos descritos neste item.

21.2. O recebimento Provisório ou Definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo instrumento de contrato.

21.3. A Aceitação Provisória dar-se-á em até 10 (dez) dias após a entrega do serviço no endereço contratado, considerando a condição de operação normal do serviço durante este período.

21.4. A Aceitação em Definitivo dar-se-á em até 20 (vinte) dias após a disponibilização do Serviço pela CONTRATADA, através da emissão do TAD (Termo de

Aceitação Definitivo).

21.5. A autorização para pagamento dos serviços contratados será autorizada pelo PRODERJ após a emissão do TAD.

22. CRONOGRAMA DOS EVENTOS

22.1. Além dos prazos previstos nesse TERMO DE REFERÊNCIA, a CONTRATADA deverá cumprir os eventos básicos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos:

MARCOS	PRAZOS (DIAS)	EVENTO	RESPONSÁVEL
D	0 (zero)	Assinatura do contrato entre o PRODERJ e a empresa Licitante vencedora.	PRODERJ e CONTRATADA
D1	D + 20	Entrega do Projeto Executivo e dos Planos de Implantação.	CONTRATADA
D2	D1 + 10	Aprovação do Projeto Executivo e dos Planos de Implantação.	PRODERJ
D3	D2 + 120	Instalação e configuração dos enlaces contratados para Rede IP MPLS	CONTRATADA
	D2 + 120	Instalação e configuração do Serviço Internet da Rede Governo	CONTRATADA
D4	D3 + 30	Recebimento definitivo, autorização para emissão de faturamento e início do período de execução dos serviços.	PRODERJ e CONTRATADA

Tabela 1 – Cronograma dos Eventos

22.2. Os tempos considerados na tabela deverão ser contados em dias corridos.

22.3. Os prazos considerados na tabela foram dimensionados de modo a garantir a manutenção da conectividade da rede e resguardar o impacto causado por eventuais indisponibilidades na troca de Operadoras de telecomunicações.

22.4. A autorização para o pagamento mensal de cada circuito será efetuada, somente após o recebimento do serviço de modo definitivo.

23. DAS PENALIDADES

23.1. O atraso injustificado no prazo de entrega do Projeto Executivo de 30 (trinta) dias

corridos da data de assinatura do contrato, poderá acarretar multa no valor de 0,2% (dois décimos por cento) sobre o somatório mensal dos links constantes no Projeto Executivo, por dia de atraso, limitado a 9% (nove por cento), quando poderão ser tomadas ações administrativas com vistas à rescisão do contrato, por descumprimento total da obrigação. Caso o Projeto Executivo seja rejeitado pelo PRODERJ na hipótese prevista no Projeto Básico e seus Encartes, a CONTRATADA terá 5 dias corridos para readequar, após este prazo incidirá a multa prevista na presente cláusula.

23.2. Os atrasos injustificados no prazo de instalação e configuração dos enlaces aprovados no projeto executivo, excluindo-se as apresentações de relatórios, poderá causar multa no valor de 0,2 (dois décimos por cento) sobre o valor mensal de cada link em atraso limitados a 18%. Em função da quantidade dos links fora do prazo poderão ser tomadas ações administrativas com vistas à rescisão do contrato, por descumprimento total da obrigação.

23.3. Os atrasos injustificados nos prazos previstos no item Requisitos de Implantação dos Encartes Técnicos por período superior a 120 (cento e vinte) dias caracterizará o descumprimento total da obrigação, punível com as sanções previstas neste documento.

23.4. Havendo solicitação de prorrogação dos prazos, este somente será concedido nos casos previstos no Art. 57, §1, da Lei nº 8.666/93, em caráter excepcional, sem efeito suspensivo, e deverá ser encaminhado por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela CONTRATADA, de acordo com a lei.

23.5. Eventual pedido de prorrogação deverá ser encaminhado para a GRT – Gerência de Rede e Telecomunicações do PRODERJ, situado no Rio de Janeiro-RJ.

23.6. Nos casos de não atendimento dos indicadores de qualidade de serviços, conforme estabelecido no Projeto Básico e seus Encartes, que acarrete na indisponibilidade dos serviços, serão efetuados descontos proporcionais automáticos pelos serviços não prestados.

23.7. Serão aplicadas sanções pelo descumprimento dos Níveis Mínimos de Serviço (NMS) caso não sejam observados os prazos máximos para o retorno da disponibilidade regular dos serviços, sem prejuízo dos descontos sobre a fatura mensal, segundo os seguintes critérios.

23.7.1. Para o indicador “Índice de Disponibilidade Mensal do Enlace (IDM)”, cada 0,1% (um décimo por cento) abaixo da métrica correspondente de cada tipo de enlace, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

23.7.2. Para o indicador “Taxa de Erro de Bit (TrErr)”, sempre que houver aferição e este se encontrar em descordo com o nível de serviço contratado, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

23.7.3. Para o indicador “Taxa de Perda de Pacotes (TPP)”, sempre que houver aferição e este se encontrar em descordo com o nível de serviço contratado, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

23.7.4. Para o indicador “Retardo da Rede (Retardo)”, sempre que houver aferição e este se encontrar em descordo com o nível de serviço contratado, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

23.7.5. Para o indicador “Prazo para Reparo / Restabelecimento de um Enlace (PR)”, cada 1 (uma) hora acima da métrica estabelecida no nível de serviço contratado, será aplicado desconto correspondente a 2,0% (um por cento), calculado sobre o valor mensal do circuito afetado.

23.7.6. Para o indicador “Prazo para Alteração de Configuração de Roteadores (PAC)”, para cada 1% do prazo estipulado em atraso, para o nível de serviço contratado, será aplicado desconto correspondente a 2,0% (um por cento), calculado sobre o valor mensal do circuito afetado.

23.7.7. Para o indicador “Prazo para Alteração de Taxa de Transmissão de um Enlace (PAT)”, cada 1 (um) dia acima da métrica estabelecida no nível de serviço contratado, será aplicado desconto correspondente a 2,0% (um por cento), calculado sobre o valor mensal do circuito afetado.

23.7.8. Para o indicador “Prazo para Alteração a Novos Endereços (PAN)”, cada 1 (um) dia acima da métrica estabelecida no nível de serviço contratado, será aplicado desconto correspondente a 2,0% (um por cento), calculado sobre o valor mensal do circuito afetado.

23.7.9. As multas mensais cumulativas em cada circuito serão limitadas ao valor mensal do circuito contratado.

23.7.10. As multas serão cumulativas dentro de cada mês e não excederão a 30% (trinta por cento) do valor mensal do contrato. Atingido esse limite, poderão ser tomadas ações administrativas com vistas à rescisão do contrato, por descumprimento da obrigação contratual, sem prejuízo das demais sanções previstas no contrato.

23.7.11. Essas sanções poderão ser aplicadas cumulativamente com as demais sanções previstas no contrato, não terão caráter compensatório e sua cobrança

não isentará a CONTRATADA da obrigação de indenizar eventuais perdas e danos.

23.7.12. A sanção aplicada à CONTRATADA e os prejuízos por ela causados à CONTRATANTE poderão ser deduzidos de qualquer crédito a ela devido, cobrados direta ou judicialmente.

23.7.13. O valor da multa poderá ser descontado do pagamento a ser efetuado à CONTRATADA:

23.7.13.1. Se o valor a ser pago à CONTRATADA não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.

23.7.13.2. Se os valores do pagamento e da garantia forem insuficientes, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial.

23.7.14. Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA à CONTRATANTE, este será encaminhado para inscrição em dívida ativa.

23.7.15. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até 10 (dias) dias úteis, contado da solicitação da CONTRATANTE, a partir do qual se observará o disposto nos itens da Cláusula Garantia deste contrato.

24. FATURAMENTO

24.1. A fatura da prestação mensal dos serviços deverá ser única por CONTRATANTE e discriminada por tipo de serviço e acessos contratados, instalados e operacionais, incluindo a localidade, endereço, designação e velocidade do circuito.

24.2. A CONTRATADA deverá disponibilizar, mensalmente, o espelho da fatura detalhando os serviços referentes ao mês anterior em até 10 (dez) dias úteis antes do vencimento para conferência e atesto.

24.3. O gestor do Contrato da CONTRATANTE deverá informará as discrepâncias, através de documento oficial em 10 (dez) dias úteis após o recebimento do espelho da fatura citado no item anterior.

24.4. A CONTRATADA só emitirá a segunda via das faturas após solicitação formal pela CONTRATANTE.

24.5. A CONTRATADA deverá disponibilizar o Relatório do Nível de Serviço em meio digital e discriminado por órgão, localidade, tipo de serviço e acessos contratado.

24.6. A CONTRATADA deverá disponibilizar as informações (tabelas e/ou demonstrativos) que identifiquem a metodologia empregada no cálculo dos custos de instalação e manutenção dos acessos e serviços.

24.7. A CONTRATADA não poderá cobrar quaisquer valores para serviços de instalação e desinstalação.

24.8. As penalidades aplicadas e decorrentes das discrepâncias verificadas pelo não atendimento do nível de serviço acordado, deverão ser creditadas na fatura do mês subsequente do respectivo Contrato.

25. VIGÊNCIA DO CONTRATO

25.1. O prazo de vigência do contrato decorrente do Registro de Preços inicia-se na data de sua assinatura, estendendo-se por 12 (doze) meses com possibilidade de prorrogação por igual período até o limite de 60 meses.

25.2. O prazo de entrega dos produtos e execução dos serviços considera que os componentes do objeto licitado se agrupam em serviços de natureza contínua.

25.3. Os reajustes que a CONTRATA fará jus deverão ser anuais, sendo que o índice reajuste deverá ser aquele pactuado em contrato.

25.4. O índice do reajuste a ser aplicado será segundo o IST apurado no período de anual do contrato e o mesmo será aplicado a todos os termos aditivos do contrato mãe nesta data.

26. ANEXOS DO TERMO DE REFERÊNCIA

Este termo de referencia possui quatro anexos:

- Anexo A: Catalogo de Serviços.
- Anexo B: Níveis de Serviço
- Anexo C: Endereços de Atendimento Rede MPLS
- Anexo D: Endeços de Atendimento - Serviços de Internet

Todo o conteúdo destes anexos é suportado pela estrutura de Gestão Integrada descrita neste termo de referência.