JUCERJA

Junta Comercial do Estado do Rio de Janeiro

Secretaria Estadual de Desenvolvimento Econômico, Indústria, Comércio e Serviços

GOVERNO DO ESTADO RIO DE JANEIRO

PLANO DE CONTINUIDADE DE NEGÓCIOS

VISÃO GERAL

Descrição	Documentação de Segurança da Informação
Documentos Complementares	Política de Backup da JUCERJA Plano de Gestão de Incidentes de Segurança - Anexo da ETI-JUCERJA
Elaboração	2024
Motivação	Norma ABNT NBR 1599-1 POSIC-JUCERJA, Portaria JUCERJA N. 2021/2022
Previsão de Revisão	Até 3 anos
Revisão Extraordinária	A qualquer tempo

CONTROLE DE VERSÃO

1. PCN – 2024 Elaboração do documento					
Data	**Versão**	**Atualização**	**Motivação/ Justificativa**	**Descrição**	**Autor**

EQUIPE DE TIC RESPONSÁVEL PELO PCN

Principal responsável do NSTIC/RJ - JUCERJA
Aldo Fernandes Ávila – Superintendente de Informática - Id. 5128984-9
Representante da Coordenação de TIC
Felipe Barreiros dos Santos - Id. 4331725-1
Representante da Assessoria de Redes
Glauco Renato N. Costa - Id. 4325992-8
Representante da Assessoria de Suporte
Roberto F. Nibra Calomeni - Id. 4366896-8
Ricardo Alves da Silva - Id. 4147518-6
Darllan Guimarães do Nascimento - Id. 5136993-1
Representante da Assessoria de Desenvolvimento
Charles Santos de Andrade - id. 4356687-1
Representante da Assessoria de Banco de Dados
Luiz Fernando Floresta de Miranda -id. 4415029-6

EQUIPE DAS ÁREAS DE NEGÓCIOS RESPONSÁVEL PELO PCN

Representante da atividade fim da JUCERJA
Gabriel de Oliveira Voi - id. 5106185-6
Gustavo de Andrade Ventura Vallim - id. 4349317-3

Sumário

1. INTRODUÇÃO

1.1. Apresentação

A Junta Comercial do Estado do Rio de Janeiro – JUCERJA, autarquia da administração indireta do poder executivo estadual, vinculada à Secretaria de Estado de Desenvolvimento Econômico, Indústria, Comércio e Serviços do Estado do Rio de Janeiro, na qualidade de órgão orquestrador e responsável pela integração tecnológica entre todos os entes públicos, das três esferas de governo, que compõem o ecossistema de registro e licenciamento empresarial no Estado do Rio de Janeiro, por meio deste plano, busca aprimorar o *compliance de TIC*, assim como, dotar esse ecossistema de um planejamento técnico orientado ao enfrentamento de crises originadas em incidentes e/ou desastres cibernéticos que possam impactar a disponibilidade, integridade e confiabilidade dos serviços tecnológicos que oferece.

Com este prisma, neste plano são disponibilizados procedimentos, recursos e contatos das equipes técnicas responsáveis pelo tratamento e respostas a incidentes, assim como, elementos que permitem ações pontuais da Alta Administração junto aos órgãos externos quando for o caso.

Não obstante o planejamento, este plano reúne ainda informações sobre os ativos / serviços críticos de TIC e os serviços críticos de negócio que devem ser prontamente restabelecidos à sociedade e ao ecossistema de registro e licenciamento empresarial em caso de incidentes e/ou desastres.

O Plano de Continuidade de Negócios é o instrumento que tem como propósito nortear todas as atividades inerentes ao enfrentamento de crises relacionadas a incidentes ou desastres cibernéticos que afetem os serviços da Instituição, de modo que seja possível, em prazos razoáveis, restabelecer a operação parcial e plena da Instituição.

1.2. Motivações e Benefícios do Planejamento

Não obstante a Norma ABNT NBR 1599-1 que "*estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN). Cujo propósito é fornecer uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização além de obter confiança nos negócios da organização com clientes e outras organizações. Ela permite também que a organização avalie sua capacidade de GCN de uma maneira consistente e reconhecida. Para ser usada por qualquer pessoa que seja responsável pelas operações de negócios ou serviços, passando por todos os níveis da organização.*" O aprimoramento do *Compliance é um objetivo que* também permeia o Plano Diretor de Tecnologia da Informação e Comunicações da JUCERJA, neste específico, no que diz respeito ao *compliance* de TIC.

Esta Iniciativa, sobretudo, visa dotar a Instituição de mecanismos e processos que permitam adotar ações objetivas, efetivas e eficazes em situações de incidentes ou desastres, resguardando o interesse público quanto ao objetivo finalístico do órgão, fornecendo estratégias para garantir que serviços essenciais sejam identificados, para garantir sua preservação até o retorno da situação normal de funcionamento da instituição.

1.3. Documentos Complementares

a) Política de Segurança da Informação da JUCERJA – Portaria JUCERJA N. 2041/2022
b) Política de Backup da JUCERJA – Portaria JUCERJA N.
c) Plano de Gestão de Incidentes de Segurança - Anexo A da Portaria JUCERJA/SUPINF Nº 02
d) Plano de Gestão de Violação de Dados EVERY (Relatório de Riscos aferidos e Plano de ação consolidado)

1.4 Metodologia Utilizada

A metodologia utilizada para a elaboração deste documento baseou-se em documentos de referência, com as devidas adaptações, considerando as reais necessidades da JUCERJA e os normativos internos atinentes à Tecnologia da Informação, alinhando este plano ao modelo de estratégia de governança de TIC adotado na Instituição.

1.5 Objetivo

Estabelecer cenários para situações inesperadas ou incidentes, quer sejam operacionais, desastres ou crises, além de formas de gerenciar os impactos imediatos de um incidente de interrupção, com foco em:

a) bem-estar dos públicos internos e externos conforme a política de comunicação adotada no órgão;
b) alternativas estratégicas, táticas e operacionais para responder à interrupção;
c) prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
d) detalhes sobre como e em que circunstâncias o órgão irá se comunicar com as partes interessadas.

O PCN fornece normas e padrões para que o órgão consiga recuperar, retomar e dar continuidade aos seus processos de negócios, em especial, os mais cruciais, evitando que eles sofram danos maiores.

Este plano seguirá o Modelo "*Plan-Do-Check-Act*" (PDCA) para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente.

2. FERRAMENTAS

Não obstante o eventual acionamento de recursos externos e/ou de outras unidades organizacionais, são designadas como ferramentas para operacionalizar o PCN, todos os normativos de segurança da informação, assim como, as equipes e recursos de TIC da Superintendência de Informática.

Somam-se às ferramentas, outros recursos de validação e aferição de desempenho, tais como:

a) Rotinas de validação;
b) Indicadores de desempenho.

No que diz respeito aos indicadores de desempenho, são adotados os mesmos indicadores elaborados para o Plano de Gestão de Incidentes de Segurança na medida de fazer referência aos mesmos objetivos.

As rotinas de validação se referem a procedimentos técnicos realizados pela ETI-JUCERJA, porém, neste plano, sem demonstração ou detalhamento dos recursos utilizados, visto que se referem a matéria de acesso exclusivo e restrito aos técnicos da Superintendência de Informática.

3. PLANO DE CONTINUIDADE DE NEGÓCIOS - PCN

3.1 Objetivo

Estabelecer diretrizes e procedimentos que possibilitem, em tempo razoável, a recuperação e restabelecimento dos serviços institucionais por ocasião de incidentes de segurança que desaguem na indisponibilidade parcial ou total dos serviços e recursos tecnológicos da JUCERJA.

3.2 Escopo

O Plano de Continuidade de Negócios – PCN abrange as estratégias necessárias à continuidade dos serviços de TIC críticos e essenciais: contingência, continuidade e recuperação. Está voltado a estabelecer continuidade aos processos definidos como críticos pela área de TIC e pela Instituição, neste específico, os serviços essenciais da JUCERJA.

O PCN contempla medidas voltadas à continuidade, contingência e recuperação dos serviços essenciais de TIC. Considerando o estágio atual de maturidade institucional na gestão de riscos, o plano foca nos cenários mais críticos, priorizando serviços cuja interrupção impactaria diretamente os objetivos estratégicos da organização.

Em decorrência do atual estágio de maturidade da organização, relativamente aos processos da Gestão da Continuidade de Negócios, assim como, ainda se encontrarem em fase embrionária a Metodologia de Análise de Riscos e Análise de Impacto nos Negócios, a amplitude do plano se limita aos riscos mais efetivos da JUCERJA, caracterizados com base em serviços tecnológicos de sustentação dos objetivos finalísticos da Instituição.

3.3 Principais Riscos

A concepção deste plano considera uma abordagem realista baseada em lições aprendidas e nas vulnerabilidades identificadas nos ambientes físicos e lógicos da JUCERJA. A categorização dos riscos foi estruturada para possibilitar respostas proporcionais e eficazes diante de falhas elétricas, ataques cibernéticos, falhas de backup e indisponibilidade de ativos / serviços críticos.

O Plano de Continuidade de Negócios – PCN foi concebido para acionamento em eventuais ocorrências de incidentes e/ou desastres que representem risco a continuidade dos serviços tecnológicos, conforme abaixo descrito:

Incidente ou desastre	Possíveis causas
Interrupção de energia elétrica	• Causada por fator externo à rede elétrica do prédio com duração superior a 2hs; • Causada por fator interno que comprometa a rede elétrica do prédio com risco ou caracterização de incêndio, curto circuito e infiltrações; • Indisponibilidade de No Break para sustentar os ativos do Data Center por prazo superior a sua capacidade.
Indisponibilidade de backup	• Indisponibilidade de cópias de segurança dos dados; • Comprometimento da integridade dos dados.
Indisponibilidade de rede lógica	• Rompimento de fibra óptica decorrente de obras públicas, desastres ou acidentes; • Mal funcionamento de switches; • Mal funcionamento dos *appliances* de *firewall;* • Interrupção de conectividade dos serviços de internet por falha ou abandono de operadora de internet contratada.

Indisponibilidade de servidores e/ou storages	• Rompimento de fibra óptica ou conexões lógicas dos equipamentos; • Mal funcionamento de switches; • Mal funcionamento dos *appliances* de processamento e/ou armazenamento.
Ataque cibernético externo	• Ataque virtual nacional ou internacional que vença as barreiras de segurança e comprometa o desempenho ou disponibilidade das configurações, serviços e dados.
Ataque cibernético interno	• Ataque virtual interno, que vença as barreiras de segurança e, por acionamento de usuário interno, comprometa o desempenho ou disponibilidade da rede, dos sistemas, das configurações, serviços e dados.
Ações desautorizadas	• Acesso de pessoa desautorizada ao Data Center; • Inobservância, por parte dos usuários internos, das orientações e recomendações de segurança; • Acesso a recursos tecnológicos ou sistêmicos, não aderentes as atividades do usuário.

3.4 Papéis e Responsabilidades

Definição de todos papéis e responsabilidades dos agentes e autoridades envolvidos no Plano de Continuidade de Negócios – PCN.

Objeto	Responsável	Responsabilidade
Segurança da Informação	Gestor de Segurança da Informação	• Normatizar e atualizar as normas de segurança da informação; • Coordenar a elaboração e gestão do PCN; • Acionar o PCN em caso de incidente; • Subsidiar a Superintendência de Informática e a Alta Administração de informações relativas à continuidade do negócio.
Tratamento e resposta a Incidentes	Responsável pelo Tratamento e Resposta a Incidentes de Segurança	• Solicitar os recursos necessários à ETI-JUCERJA • Subsidiar ao Gestor de Segurança da Informação as informações necessárias à tomada de decisão; • Acompanhar o desenvolvimento do trabalho da ETI-JUCERJA.
Plano de Gestão de Incidentes de Segurança	ETI-JUCERJA Equipe de Tratamento e Resposta a Incidentes de Segurança	• Prospectar e avaliar a necessidade de recursos tecnológicos para prevenção de incidentes; • Monitorar os ambientes tecnológicos; • Alertar sobre a possibilidade ou ocorrência de incidentes; • Manter registros sobre alertas e incidentes reportados; • Operacionalizar o PCN; • Restabelecer os ambientes tecnológicos em tempo razoável.
Backup – Cópias de Segurança	Assessoria de Banco de Dados	• Assegurar a manutenção dos backups internos e externos;

		• Assegurar a disponibilidade, integridade e veracidade dos backups internos e externos; • Assegurar o licenciamento e atualização das ferramentas de backup e restore; • Atuar em conjunto com a ETI-JUCERJA para restabelecer os ambientes e dados institucionais; • Assegurar a manutenção de perfis de acesso às bases de dados em conformidade com as boas práticas de gestão de Banco de Dados.
Identificação dos ativos críticos de TIC	Superintendente de Informática	• Manter atualizadas as informações sobre os ativos críticos de TIC; • Prover os recursos e mecanismos e tecnologias necessárias às atividades de garantia e manutenção dos ativos;
Identificação dos serviços críticos de TIC	Superintendente de Informática	• Manter atualizadas as informações sobre os serviços críticos de TIC; • Prover os mecanismos e tecnologias necessárias às atividades do Gestor de Segurança da Informação e ao Agente Responsável pelo Tratamento e Resposta a Incidentes; • Prover os mecanismos e tecnologias necessárias às atividades do DPO.
Identificação dos serviços críticos (Áreas de Negócio e Meio)	Gestores das áreas finalísticas	• Identificar, manter atualizadas e fornecer, ao Gestor de Segurança da Informação, informações sobre os serviços críticos da Instituição; • Notificar o Gestor de Segurança da Informação sobre a ocorrência de anomalias sistêmicas detectadas nos serviços tecnológicos ou violações de segurança ocorridas em suas respectivas áreas.
Operacionalizar o PCN	Superintendência de Informática	• Adotar os procedimentos necessários ao atendimento das solicitações do Gestor de Segurança da Informação, sobre prevenção, tratamento e resposta a incidentes; • Viabilizar os meios e recursos necessários para que as equipes de TIC atuem colaborativamente com a ETI-JUCERJA; • Assegurar acesso a todos os recursos tecnológicos necessários ao enfrentamento de incidentes; • Solicitar apoio externo, quando necessário, para enfrentamento de crises ocasionadas por incidentes; • Mobilizar, quando necessário, outras unidades para atuarem em apoio a ETI-JUCERJA; • Manter a Alta Administração informada sobre o andamento dos trabalhos e, após a superação do evento de crise, encaminhar relatório de incidentes.
Publicidade institucional	Assessoria de Comunicação	• Com base nas orientações da Alta Administração, prover comunicações aos usuários internos e externos sobre incidentes de segurança;

		• Acompanhar a repercussão de incidentes nas mídias sociais, jornais e outras; • Emitir relatório de impacto relativo a imagens institucional frente ao incidente.

3.4.1 Identificação dos ativos críticos

São considerados como ativos críticos institucionais todos os hardwares instalados no Data Center do Ed. Sede da JUCERJA, assim como, os ativos de rede distribuídos nos respectivos pavimentos.

3.4.2 Identificação dos serviços críticos

São considerados serviços críticos institucionais todos os sistemas internos e o SEI, responsáveis pelas atividades meio e fim da Instituição.

Sistema/Serviço	Tecnologia
SEI	Externo
SRE	Interno
GED	Interno
E-mail	Interno
Fale Conosco	Interno

3.5 Acionamento do Plano de Continuidade de Negócios - PCN

O PCN será acionado quando da ocorrência de algum dos cenários de incidentes, desastres, insurgência ou ocorrência de um risco desconhecido que tenha explorado alguma vulnerabilidade não tratada ou ignorada.

O evento deverá ser registrado no sistema de chamados onde serão consignadas as informações pertinentes e acionadas as equipes técnicas necessárias.

O plano também poderá ser invocado em casos de testes ou por determinação do Gestor de Segurança da Informação em conjunto com o Responsável pelo Tratamento e Respostas a Incidentes da JUCERJA.

Em casos de emergência ou iminente interrupção de serviços, detectada pela ETI-JUCERJA, o acionamento poderá ser realizado pela ETI sem provimento imediato das formalidades atinentes aos processos de enfrentamento. Nesse caso, os integrantes da ETI-JUCERJA, após acionamento, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes caso necessário.

3.5.1 Árvore de Acionamento de Contatos

A lista de contatos para acionamento dos diversos atores envolvidos na operacionalização e suporte do PCN se encontra no ANEXO I e deverá ser atualizada sempre que ocorrer alteração em quaisquer itens elencados.

3.5.2 Protocolo de Tratamento do PCN

O protocolo de tratamento dos eventos definidos neste Plano de Continuidade de Negócios - PCN é composto de fases ou macroprocessos que se encontram definidos e desmembrados em subprocessos específicos para cada área de atuação, quando da ocorrência de um desastre. A sequência das atividades está representada abaixo, genericamente, conforme segue:

a) Identificação e declaração de desastres;
b) Ativação do processo de Disaster Recovery - DR;
c) Comunicar o desastre;
d) Avaliação da corrente e prevenção de mais danos;
e) Ativação da solução de Contingência;
f) Estabelecer operações de TI;
g) Reparação e reconstrução da instalação principal;
h) Retorno das operações para o Ambiente principal.

3.5.3 Estratégias de Continuidade de Negócio:

As estratégias de continuidade de negócios definem os processos macro que deverão ser seguidos para que as providências necessárias possam ser adotadas até o restabelecimento dos serviços, contemplando as ações iniciais e as ações pós-crise.

a) Estratégia de administração de crise

b) Estratégia de continuidade operacional parcial

c) Estratégia de recuperação de desastres

d) Estratégia de cópias de segurança – Backup

3.5.3.1 Estratégia de Administração de Crise:

Responsáveis:
SI - Superintendente de Informática
GSI - Gestor de Segurança da Informação
RTI - Responsável pelo tratamento e resposta a incidentes
ETI – Equipe de tratamento e resposta a incidentes
AC - Assessor de Comunicação

Objetivo:
Definir as atividades das equipes envolvidas e gerenciamento das **ações de contingência e comunicação** durante e após a ocorrência de um incidente ou desastre, com intuito de minimizar impactos, até a superação da crise, objetivando:

- Minimizar transtornos sobre os desdobramentos do incidente e estimular o esforço em conjunto para superação da crise;
- Orientar a Alta Administração e os colaboradores com informações e procedimentos de conduta;
- Informar a sociedade e, quando for o caso, as instâncias competentes, em tempo e com esclarecimentos condizentes com o ocorrido.

Execução:

Na ocorrência de um desastre será necessário entrar em contato com todas as áreas, principalmente as afetadas, para informá-las do efeito na continuidade dos serviços e tempo de recuperação. A Superintendência de Informática será responsável por contatar estas unidades e passar as informações pertinentes a cada setor, assim como ao DPO, que avaliará a necessidade de comunicar o incidente à autoridades externas, da seguinte forma:

a) Comunicar à Alta Administração

A Superintendência de Informática encaminhará notificação dirigida à Alta Administração e ao DPO, fornecendo informações da natureza, magnitude e impacto do desastre, ficando a cargo do DPO avaliar e, quando necessário, promover a comunicação às autoridades de controle externas.

b) Comunicação Interna

Após a reunião de alinhamento com os líderes técnicos responsáveis (SI, GSI, RTI e ETI), a Assessoria de Comunicação elaborará comunicação para acionar as partes envolvidas e afetadas de modo a manter todos informados sobre a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos.
A Assessoria de Comunicação deverá manter comunicação interna ostensiva com intuito de que as unidades do órgão sejam informadas da ocorrência de um incidente e, eventual, inatividade dos serviços.

c) Comunicação Externa e Mídias

A Assessoria de Comunicação, com aval da Presidência, deverá fornecer informações pertinentes aos usuários externos: cidadãos e outros órgãos, por meio de publicações em meios oficiais e de ampla divulgação com informações sobre o ocorrido.

d) Comunicar retorno das operações

O GSI deve emitir um parecer relatando as atividades realizadas e comunicar a Superintendência de Informática quando ocorrer o retorno das operações à normalidade, que por sua vez, informará a Alta Administração, ao DPO, à Assessoria de Comunicação.

3.5.3.2. Estratégia de Continuidade Operacional Parcial:

Responsáveis:
SI - Superintendente de Informática
COOTI – Coordenação de TI
ASSRE – Assessoria de Redes
ASSBD – Assessoria de Banco de Dados
Outros – Sob demanda do SI

3.5.3.2.1 Serviços críticos de Tecnologia da Informação e Comunicação:

- **Conectividade**

Links
Firewall
Rede lógica (física)
e-mail

- **Infraestrutura física específica**

Routers
Firewall
Switches

Objetivo:
Reunir os meios e recursos necessários para continuidade dos serviços críticos de TIC por ocasião de um incidente ou desastre, de modo que a operação de TIC possa ser mantida ativa até a recuperação plena do incidente.

Prazo: Até 48 horas
O prazo de disponibilização dos serviços críticos de TIC levam em conta ações que exijam a participação de

equipes e/ou recursos externos providas por serviços de sustentação e suporte contratados e/ou eventuais recursos adicionais.

Atividade	Recurso	Serviço	Metas de Prazos
Reativação	Links de internet	Conectividade	Até 24h
Reativação	Links de internet	Conectividade	Até 24h
Reativação	Firewall	Segurança	Até 48h
Reativação	Rede	Conectividade	Até 48h

3.5.3.3. Estratégia de Recuperação de Desastre:

Responsáveis:
SI - Superintendente de Informática
COOTI – Coordenação de TI
ASSRE – Assessoria de Redes
ASSBD – Assessoria de Banco de Dados
Outros – Sob demanda do SI

Infraestrutura específica

Backup interno
Link da INFOVIA
Backup externo (PRODERJ)
Appliances que compõem a infraestrutura do Data Center
Outros – Eventuais Sob demanda das equipes ETI-JUCERJA e infraestrutura

Objetivo:
Com base nos processos de restabelecimento dos recursos de armazenamento e processamento, adotar medidas para o restabelecimento dos serviços de negócio, de modo que a Instituição possa retomar os níveis normais de operação.

Prazo: Até 216 horas
O prazo de disponibilização dos serviços críticos institucionais leva em conta a finalização das ações relativas ao restabelecimento dos serviços críticos de TIC cumulativamente. Itens que exijam a participação de equipes e/ou recursos externos estão contemplados nos prazos definidos.

Atividade	Recurso	Serviço	Metas de Prazos
Reativação	e-mail	e-mail	Até 96h
Restabelecimento	Armazenamento, Processamento e Backup	Infraestrutura	Até 120h
Restabelecimento	Sistemas internos	Ativos internos	Até 144h

Restabelecimento	Integração	Ativo Finalístico	Até 168h
Restabelecimento	Portal	Ativo Finalístico	Até 216h

A priorização do restabelecimento dos serviços críticos institucionais observa a criticidade de cada serviço em relação ao negócio, que é medida com base na quantidade de unidades internas que utilizam o serviço, seguida da observação sobre o tipo de tecnologia utilizada para sustentar o recurso e, por fim, o impacto externo.

Essa metodologia permite que os serviços institucionais, críticos e não críticos, sejam restabelecidos com o menor impacto possível aos usuários internos e externos.

A matriz de Análise de Impacto no Negócio está disponível no ANEXO II.

3.5.3.4. Estratégia de Cópias de Segurança – Backup

Responsáveis:
SI - Superintendente de Informática
GSI – Gestor de Segurança da Informação
COOTI – Coordenação de TI
ASSRE – Assessoria de Redes
ASSBD – Assessoria de banco de Dados

Recursos físicos:
Link da INFOVIA
Serviços de backup externo (PRODERJ)
Serviços de backup interno
Appliances e softwares que compõem a infraestrutura de backup da JUCERJA

Objetivo:
Estabelecer os procedimentos e prazos de realização dos Backup e Restore como medida de restabelecimento dos serviços institucionais, priorizando os serviços críticos de TIC que sustentarão o restabelecimento dos serviços críticos de negócio.

Não obstante a Política de Backup adotada pela Instituição, que define os prazos e procedimentos atinentes aos backups e restores de dados e serviços. Por ocasião de um incidente / desastre a priorização dos procedimentos será definida pelas equipes responsáveis pelos procedimentos de restabelecimento dos serviços para continuidade de negócio, observando os prazos definidos na estratégia de recuperação de desastre.

Execução:
As equipes ETI-JUCERJA e de Infraestrutura deverão apresentar, para aprovação do GSI, um plano de recuperação dos ambientes tecnológicos, priorizando os serviços críticos de TIC e de negócios, observando os prazos definidos na estratégia de recuperação de desastre.

A Assessoria de Banco de Dados e a Assessoria de Redes, com base nas recomendações do GSI, adotarão os procedimentos adequados ao restabelecimento dos serviços críticos de TIC e de negócios

A execução do plano de recuperação deverá observar as melhores práticas em gestão de incidentes e governança de TI, utilizando ferramentas adequadas de versionamento, controle de mudanças e rastreamento de atividades. A formalização das ações e a posterior elaboração de relatórios técnicos visam a transparência e a melhoria contínua do processo.

Cada uma das equipes envolvidas no tratamento e restabelecimento dos serviços críticos de TIC, ao final dos procedimentos e após o restabelecimento pleno da operação da Instituição, deverá elaborar relatório técnico, pormenorizado, por meio do qual seja possível identificar causas, efeitos e resultados do incidente / desastre.

A ETI-JUCERJA deverá assegurar a manutenção e guarda das informações geradas ao longo de todos os procedimentos, assim como, dos relatórios.

O GSI deverá elaborar relatório conclusivo à Alta Administração sobre o incidente / desastre, inclusive, quando for o caso, propondo a adoção de medidas e/ou recursos de segurança para mitigar reincidência das causas do incidente / desastre.

4. Ações Complementares

A Superintendência de Informática deverá promover todas as ações e diligências necessárias à mitigação dos riscos apontados neste documento, de modo que eventuais fragilidades sejam superadas e os riscos sejam minimizados ou extintos.

A Presidência da JUCERJA caberá priorizar e prover os recursos orçamentários necessários às ações de enfrentamento dos riscos apontados pela Superintendência de Informática.

ANEXO I

Árvore de Acionamento de Contatos

Sigla	Descrição	Celular - Ramal	e-mail
Alta Administração	Presidente	**5434**	**sergio.romay@jucerja.rj.gov.br**
Alta Administração	Vice-Presidente	**5448**	**alexandre.velloso@jucerja.rj.gov.br**
Alta Administração	Secretário geral	**5420**	**gabriel.voi@jucerja.rj.gov.br**
Alta Administração	Superintendente de Adm. e Finanças	**5470**	**lincoln.murcia@jucerja.rj.gov.br**
Alta Administração	Superintendente Registro e Comércio	**5410**	**gustavo.vallim@jucerja.rj.gov.br**
Alta Administração	Superintendente de Controle Interno	**5484**	**paulo.henriques@jucerja.rj.gov.br**
Alta Administração	Superintendente de Informática	**5404/ (21)96818-3000**	**aldo.avila@jucerja.rj.gov.br**
COOTI	Coordenador de TIC	**5405/ (21)99596-6809**	**felipe.barreiros@jucerja.rj.gov.br**
ASSRE	Assessoria de Redes (infraestrutura)	**5403/ (21) 99263-3835**	**glauco.renato@jucerja.rj.gov.br**
ASSSUP	Assessoria de Suporte	**5407/ (21) 99362-8199**	**roberto.calomeni@jucerja.rj.gov.br darllan.guimaraes@jucerja.rj.gov.br**
ASSDEV	Assessoria de Dev (Dev e **integração**)	**5412**	**charles.andrade@jucerja.rj.gov.br**
ASSBD	Assessoria Banco de Dados	**5407**	**luiz.fernando@jucerja.rj.gov.br**
GSI	Gestor de Segurança da Informação	**5404**	**aldo.avila@jucerja.rj.gov.br**
RTI	Responsável pelo Tratamento e Resposta a Incidentes	**5405**	**felipe.barreiros@jucerja.rj.gov.br**
ETI-JUCERJA	Equipe de Tratamento e Resposta a Incidentes.	**5405**	**felipe.barreiros@jucerja.rj.gov.br**

DPO	Encarregado LGPD	**5438**	**william.rocha@jucerja.rj.gov.br**
ASSCOM	Assessoria de Comunicação	**5441**	**alessandra.niskier@jucerja.rj.gov.br**
Vigilância	Responsável pelo serviço de vigilância	**5414**	**wagner.lourenco@grupobrasilforte.com.br**
Portaria	Responsável pela Portaria (chaves)	**5414**	**wagner.lourenco@grupobrasilforte.com.br**
Suporte	Microsoft	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Red Hat	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Switches	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Hauwei	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Dell	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Palo Alto	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Net Backup	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Veeans	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	VMWare	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	MySQL	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Computadores – desktop	**5407**	**roberto.calomeni@jucerja.rj.gov.br**
Suporte	Impressoras	**5490**	**kauan.franco@jucerja.rj.gov.br**
Suporte	Scanners	**5490**	**kauan.franco@jucerja.rj.gov.br**
Suporte	Projetores	**5490**	**kauan.franco@jucerja.rj.gov.br**
Suporte	**Manutenção Predial**	**5481**	**ana.cardoso@jucerja.rj.gov.br**
Suporte	Manutenção Rede Lógica	**5406**	**darllan.guimaraes@jucerja.rj.gov.br**
Suporte	HSM	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	Link de Internet – Data Corpore	**5407**	**ricardo.alves@jucerja.rj.gov.br**
Suporte	Link INFOVIA backup externo - Claro	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	PRODERJ	**5403**	**glauco.renato@jucerja.rj.gov.br**
Suporte	SEI	**5484**	**paulo.henriques@jucerja.rj.gov.br**

ANEXO II

Análise de Impacto no Negócio

Sistema/Serviço	Tecnologia	Unidades Dependentes
SEI	Externo	39
SRE	Interno	35
GED	Interno	27
E-mail	Interno	16
Fale Conosco	Interno	12
SIAFI	Externo	12
CONVERJ	Externo	10
SIGFIS (E-TCE)	Externo	8
SIGA	Externo	8
Correios	Externo	7
SIGRH	Externo	6
Almoxarifado	Interno	4
PJE	Externo	3
Assinador Livre - TJ	Externo	3
SIAUDI	Externo	3
JUCERJA RH	Interno	3
SISRFF	Externo	3
Almoxarifado Virtual	Externo	3
S. Contratos	Externo	2
OUVERJ	Externo	1
SIPLAG	Externo	1
PIERJ	Externo	1
Elastic	Interno	1
BioAC	Interno	1
VPN Serpro	Interno	1
Jucerja-AR	Interno	1
Assinador Serpro	Interno	1
Intranet	Interno	1

ANEXO III

Sistemas Institucionais

Sistemas Estratégicos Prioritários

Os sistemas abaixo são considerados essenciais para a operação institucional, desempenhando papel central nos processos, na integração de serviços e no atendimento ao público. Por esse motivo, merecem destaque e atenção prioritária.

Criticidade alta

- GED
- Portal
- Protocolo Web
- SRE
- Regin Central
- Fale Conosco
- SAED
- Certidão Online
- Formulário SEFAZ
- Integrador
- Integrador – Serviços RFB
- Regin Instituição
- Formulário de Legalização
- Formulário de Viabilidade
- Integrador – Envio de Dados
- Login – JUCERJA
- Regin Cartório
- Regin Vistoria
- Requerimento Estadual
- Requerimento Municipal
- Digitalizador
- Documento Digital

Criticidade Média

- Extranet
- CAE
- Intranet
- Login – Gov.br
- Segurança

Criticidade baixa

- Portaria

Sistemas de Apoio e Operacionais

Os sistemas listados a seguir exercem funções complementares e operacionais, apoiando áreas administrativas, técnicas, de segurança, atendimento e gestão interna.

- GLPI
- Elastic
- Monitoramento Empresarial
- Portal de Assinaturas
- Procuradoria
- Proteção de CPF
- Recursos Humanos (RH)
- SGC – Contratos
- Visualizador de Assinaturas
- Controle de Certificado
- Atendpro
- AR – Certificado Digital
- App
- Almoxarifado
- Acompanhamento de Protocolo
- Controle de Qualidade
- Deferidor DBE