PLANO DE GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TIC

COMPANHIA DOCAS DO RIO DE JANEIRO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO - SUPTIN

SUMÁRIO

1. INTRODUÇÃO

1.1. A Companhia Docas do Rio de Janeiro (CDRJ) possui importância estratégica como agente governamental, provedor de infraestrutura portuária, contribuindo para o fomento e o desenvolvimento do Comércio Exterior do Estado e do País.

1.2. Diante da relevância da atividade portuária,, verifica-se a necessidade da Companhia de se manter em constante desenvolvimento, de forma a atender cada vez melhor às expectativas da sociedade quanto à qualidade dos serviços prestados.

1.3. Esse processo requer o emprego contínuo de recursos computacionais que garantam o funcionamento da CDRJ de forma permanente.

1.4. Nesse cenário, faz-se necessário o estabelecimento de uma estratégia que possibilite a continuidade dos serviços de TIC essenciais à operação portuária, incluindo mecanismos de contingência, continuidade e recuperação dos serviços informatizados.

2. TERMOS E ABREVIAÇÕES

2.1. As siglas, abreviações e termos técnicos usados neste documento são apresentados na tabela a seguir:

TERMOS	DESCRIÇÃO
BACKUP	Cópia de segurança
CDRJ	Companhia Docas do Rio de Janeiro
CGTI	Comitê Gestor de Tecnologia da Informação
CMMI	Sigla em inglês para *Capability Maturity Model Integration* - modelo de referência que contém práticas específicas para melhoria de processos
DIRAFI	Diretoria Administrativo-Financeira
DIREXE	Diretoria Executiva
Framework	Conjunto de diretrizes e melhores práticas
GERCOS	Gerência de Estruturação e Construção de Soluções
GERSOL	Gerência de Operação de Soluções
IaaS	*Infrastructure as a Service* - é um modelo de Computação em Nuvem que disponibiliza recursos computacionais como processamento, memória, armazenamento, banco de dados e servidores acessados via Internet ou por uma rede privada
IN	Instrução Normativa
ITIL	Abordagem padronizada para o Gerenciamento de Serviços de TI
Minfra	Ministério da Infraestrutura
PCTI	Plano de Continuidade de Serviços de TIC

PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PEI	Planejamento Estratégico Institucional
PAC	Plano de administração de crises
PCO	Plano de continuidade operacional
PRD	Plano de recuperação de desastres
PTV	Plano de testes e verificação
PLABS	Plano Anual de Aquisição de Bens e Serviços
RESTAURAÇÃO	ou *Restore* é ação de recuperar os dados armazenados em determinado dispositivo durante a rotina de backup, garantindo que todas as informações gravadas estejam intactas
SERVIDOR	Computador com sistema de computação centralizada que fornece serviços a uma rede de computadores (clientes)
SNPTA	Secretaria Nacional de Portos e Transportes Aquaviários
SUAITE	Supervisão de Apoio à Infraestrutura e Telecomunicações
SUPTIN	Superintendência de Tecnologia da Informação
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação

3. OBJETIVOS

3.1. O Plano de Continuidade de Serviços de TIC – PCTIC – tem como objetivo o estabelecimento dos procedimentos necessários para assegurar a continuidade dos serviços tecnológicos considerados de caráter crítico para a CDRJ, definindo as ações a serem tomadas em casos de incidentes ou desastres que resultem em indisponibilidade, incluindo acidentes naturais, intencionais, bem como falhas sistêmicas ou humanas que possam ocorrer durante o processo, tentando prever e mitigar os danos e riscos.

4. METODOLOGIA DE TRABALHO

4.1. O Plano de Gestão de Continuidade de Serviços de TIC foi elaborado com base nos principais frameworks de governanca de TIC e a partir de pesquisas em documentos de instituições públicas e privadas relacionados ao tema.

5. DOCUMENTOS DE REFERÊNCIA

5.1. IN.GERSOL.10.006 - Gerir o armazenamento o backup e a restauração de arquivos da rede corporativa da CDRJ.

5.2. Política de Segurança de TI da CDRJ.

6. VIGÊNCIA

6.1. Este Plano terá vigência de 4 (quatro) anos, devendo ser reavaliado a cada 2 (dois) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

7. PAPÉIS E RESPONSABILIDADES

7.1. Compete a DIREXE:

7.1.1. Garantir os recursos necessários para estabelecer, implementar, operar e manter o PCTIC aprovado pelo CGTI.

7.2. Compete ao CGTI:

7.2.1. Aprovar o PCTIC e seus planos de ação complementares, avaliando-o periodicamente e zelando por sua qualidade e efetividade.

7.2.2. Encaminhar o PCTIC para ciência e deliberação da DIREXE.

7.2.3. Avaliar a relação custo/benefício das estratégias de continuidade propostas, dos planos de ação que compõem o PCTIC e decidir sobre sua implementação.

7.2.4. Desenvolver a cultura de Gestão de Continuidade de Serviços de TIC.

7.2.5. Definir as estratégias de comunicação às alçadas superiores da CDRJ e às áreas afetadas, além de entidades externas relacionadas, durante todo o período de crise.

7.2.6. Aprovar cronograma anual de testes.

7.3. Compete à SUPTIN:

7.3.1. Avaliar e validar os planos de ação elaborados pelas suas gerências subordinadas em parceria com as áreas correlatas, propondo ajustes, se necessário.

7.3.2. Propor diretrizes e estratégias de segurança da informação para o PCTIC e seus respectivos planos de ação.

7.3.3. Supervisionar a elaboração, implementação, testes e atualização dos planos de ação.

7.3.4. Propor melhorias na implantação de novos controles relativos ao PCTIC .

7.3.5. Atuar como interface entre o corpo técnico e as áreas interessadas ou afetadas pela não Continuidade dos Serviços de TI.

7.4. Compete a equipe de desastre e recuperação (EDR), formada por técnicos e analistas de TI:

7.4.1. Identificar, documentar e informar ao CGTI sobre os riscos que possam comprometer a continuidade das atividades críticas, sugerindo estratégias de mitigação adequadas a sua manutenção e recuperação.

7.4.2. Documentar e publicar o processo de Continuidade de Serviços de TI.

7.4.3. Elaborar os planos de ação previstos no PCTIC .

7.4.4. Acompanhar o processo de implementação da estratégia de continuidade de TI, em função dos riscos operacionais envolvidos.

7.4.5. Elaborar cronograma de testes e executá-los, realizando melhorias, quando necessário.

7.4.6. Administrar a contingência quando da interrupção de atividades, com base nos planos desenvolvidos.

7.5. Compete a GERSOL:

7.5.1. Prover a infraestrutura de Tecnologia da Informação necessária à execução dos procedimentos essenciais durante um desastre ou crise.

7.5.2. Dotar a CDRJ de mecanismos de segurança no ambiente principal e alternativo.

7.5.3. Elaborar estratégias de backup compatíveis com o nível de criticidade do sistema e/ou serviço.

7.5.4. Elaborar estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.

7.5.5. Analisar e mapear a quantidade de dados perdidos, bem como o seu tempo de recuperação, em caso de incidentes dessa natureza.

7.6. Compete a GERCOS:

7.6.1. Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre ou crise.

7.7. Compete à GERMAP:

7.7.1. Garantir a climatização adequada das salas de equipamentos de TI.

7.7.2. Garantir o funcionamento adequado do sistema de energia elétrica, incluindo os aspectos de estabilização e continuidade.

7.7.3. Tratar como prioridade e dentro de suas competências regimentais quaisquer necessidades de reparos que possam ocasionar dano às salas de equipamentos de TI.

7.8. Compete a GERSET:

7.8.1. Prover e manter o sistema de proteção contra incêndios.

7.9. Compete ao Encarregado de proteção de Dados:

7.9.1. Informar à Autoridade Nacional de Proteção de Dados, e ao titular do dado, qualquer evento que possa comprometer a segurança e o sigilo de dados pessoais.

8. PROCESSO DE GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

8.1. O processo de gestão de continuidade de serviços de TI tem por finalidade definir e documentar as estratégias de recuperação de desastres e de continuidade dos serviços de TIC de modo a restabelecê-los dentro do prazo especificado e acordado com a área de negócio.

8.2. Para o presente documento, inicialmente realizou-se uma ampla avaliação de impactos, incluindo os serviços essenciais à operação do negócio da Companhia, os recursos tecnológicos associados e suas dependências, além dos riscos inerentes ao ambiente de TIC. Em seguida, foram estabelecidas estratégias de continuidade, considerando todo o ambiente tecnológico disponível e os testes a serem realizados.

8.3. A partir dessas premissas, foram desenvolvidos os 4 (quatro) planos de ação complementares, com o objetivo de permitir a recuperação, contingência e continuidade dos serviços de TI durante a ocorrência de incidentes, a saber:

8.3.1. Plano de administração de crises (PAC);

8.3.2. Plano de continuidade operacional (PCO);

8.3.3. Plano de recuperação de desastres (PRD) e;

8.3.4. Plano de testes e verificação (PTV).

8.4. Os planos de ação supracitados serão detalhados posteriormente, no formato de anexo.

9. ANÁLISE DE IMPACTO NO NEGÓCIO

9.1. A partir da análise de impacto no negócio é possível identificar quais processos são essenciais ao funcionamento da CDRJ e, dessa forma, avaliar quais os serviços de TI precisam ser restabelecidos com celeridade, após a ocorrência de um incidente ou desastre. Esta avaliação deve considerar os processos organizacionais definidos como mais críticos para a Companhia. A tabela abaixo apresenta os processos organizacionais que serão tratados no PCTIC.

Processos Organizacionais Críticos			
Sistema	**Área**	**Processo Organizacional**	**Criticidade**
SSA (StarSoft Applications)	SUPFIN	Gestão Financeira	ALTA
		Gestão Contábil	
		Gestão Orçamentária	
	GERAIP	Gestão Patrimonial	
SUPERVIA DE DADOS	GERQUA	Gestão e Controle da Operação Portuária	ALTA
SIGEP (Faturamento nos Portos)	SUPRIO/GERNIT/SUPITA/ GERANG	Gestão e Controle da Operação Portuária	ALTA
STAq (AIS) - Sistema de Tráfego Aquaviário	GERQUA/SUPRIO/GERNIT SUPITA/GERANG	Gestão e Controle da Operação Portuária	ALTA
Serviço de Radiocomunicação	SUPGUA/GERQUA/ SUPRIO/GERNIT/SUPITA/ GERANG	Controle da Operação Portuária	ALTA
Programação de navios	GERQUA	Gestão e Controle da Operação Portuária	MÉDIA
SUPERVIA DE DADOS WEB (LocaWeb)	SUPRIO/SUPITA	Gestão e Controle da Operação Portuária	ALTA
Movimento de carga RIO	GERFOP/GERIME	Gestão e Controle da Operação Portuária	ALTA
Sistema de Relatórios Estatísticos de Movimentação nos Portos da CDRJ	GERIME	Gestão e Controle da Operação Portuária	ALTA
SGAD - Sistema de Gerenciamento Docas	SUPGUA	Gestão de acesso às instalações portuárias	ALTA
Portal de agendamento rodoviário	CDRJ	Gestão de acesso ao porto do Rio de Janeiro	MÉDIA
On guard	SUPGUA	Gestão de acesso ao porto do Rio de Janeiro	ALTA
Benner	GERARH	Gestão de Pessoas	ALTA
		Gestão de Benefícios	
		Pagamento de Pessoal	
Site Institucional	CDRJ	Comunicação Social e Responsabilidade Social Atendimento a Clientes Externos / Ouvidoria-Geral Gestão de Materiais e Serviços Gestão de Concurso Público	MÉDIA
Internet	CDRJ	Todos	ALTA
Intranet	CDRJ	Comunicação Social e Responsabilidade Social Controle Interno	MÉDIA
ISPS - CODE	SUPGUA	Controle de Segurança Portuária	ALTA
Sistema de pesagem	GERATE	Gestão de cargas	MÉDIA

9.2. Adicionalmente, deve-se avaliar a interdependência entre os serviços de TI responsáveis pela sustentação dos processos organizacionais, conforme se observa abaixo:

PRIORIDADE	SERVIÇO/SISTEMA	CRITICIDADE	CORRELAÇÃO
1	Internet	alta	Link de acesso
2	Servidor SQL Server	alta	Benner
			SIGEP
			ShipsGP
			SSA
3	SSA	alta	Internet
4	PSP	alta	Internet
5	Supervia de dados	alta	MPLS
			DNS
			Oracle
6	SIGEP	alta	MPLS
			Servidor SQL Server
7	STAq (AIS)	alta	Internet
			DNS
8	Radiocomunicação	alta	Internet
9	Programação de Navios	alta	Internet
			DNS
			STAq (AIS)
10	Supervia web	alta	Internet
			DNS
11	SGAD	alta	Internet
			DNS
12	Portal de agendamento rodoviário	alta	Internet
			DNS
			SGAD
13	Controle de Acesso	alta	SGAD
14	Benner	alta	Internet
			DNS
15	SEI	média	Internet
			Active Directory
16	E-mail institucional	média	Internet
			DNS
			Exchange local
17	Site institucional	média	Internet
			DNS
18	Telefonia Móvel	média	**
19	Sistema de controle de carga	baixa	Internet
			DNS
20	VPN	baixa	Firewall

			Internet
			Active Directory

9.3. Os serviços de TI elencados na tabela constante do item 9.2 poderão ser alterados e atualizados de acordo com as mudanças no cenário interno e externo da Companhia. Para a elaboração do presente documento, foi realizada a análise de impacto dos serviços de TI existentes no ano de 2021.

10.AVALIAÇÃO DE IMPACTO DOS SERVIÇOS DE TI

10.1. Após a etapa de identificação, verifica-se a necessidade de avaliar qual seria o impacto da interrupção dos serviços mais relevantes da área de TIC no âmbito CDRJ, após a ocorrência de um incidente. Para isso, serão utilizadas as seguintes métricas de negócio:

***RPO ou Recovery Point Objective**: Diz respeito à quantidade de informação que é tolerável perder, no caso de uma parada nas operações. Está diretamente relacionado com o intervalo de tempo de execução de backup.*

O resultado geral da configuração de uma RPO baixa depende do volume de dados, das soluções de backup disponíveis e da capacidade de toda a infraestrutura de TI da Organização.

***RTO ou Recovery Time Objective**: Período de tempo desejado necessário para realizar todas as tarefas de recuperação após uma parada ou pane. Isso inclui download dos dados, reinstalações, atualizações etc. O RTO reflete as necessidades comerciais globais do negócio, é uma medida de quanto tempo a empresa pode sobreviver com a infraestrutura de TI e serviços interrompidos, sendo uma boa prática automatizar o máximo do processo de restauração das operações.*

***MTD ou Maximum Tolerable Downtime:** Define a quantidade total de tempo que um processo de negócios pode ser interrompido sem causar quaisquer consequências inaceitáveis. Esse valor será definido entre a SUPTIN e as áreas de negócio.*

10.2. Nesse contexto, os objetivos de recuperação devem ser coerentes com as exigências e necessidades de cada serviço, nos quais os mecanismos de backup e recuperação deverão ser baseados. Atualmente, o RTO padrão utilizado pela CDRJ é o descrito no item 5.3 da IN 10.006, na qual foi estabelecida a periodicidade diária para realização de backup. Entretanto, a SUPTIN deverá envidar esforços para estabelecer RTO's mais específicos e aderentes ao nível de criticidade de cada serviço.

10.3. A tabela abaixo apresenta a avaliação de impacto dos serviços de TI, obtida a partir da análise de criticidade e dependência entre os serviços de TI:

Recurso/ Serviço	Criticidade	RPO	RTO	MTD	Impacto

					Financeiro	Legal	Imagem	Operacional
Internet	alta	**	4 horas	8 horas	indefinido	indefinido	indefinido	alto
Servidor SQL Server	alta	24 horas	6 horas	8 horas	alto	indefinido	indefinido	alto
SSA	alta	24 horas	4 horas	18 horas	alto	indefinido	indefinido	médio
PSP	alta	indefinido	4 horas	8 horas	alto	indefinido	indefinido	alto
Supervia de dados	alta	24 horas	4 horas	8 horas	alto	indefinido	indefinido	alto
SIGEP	alta	24 horas	4 horas	18 horas	alto	indefinido	indefinido	alto
STAq (AIS)	alta	24 horas	6 horas	8 horas	indefinido	alto	médio	alto
Radiocomunicação	alta	**	4 horas	8 horas	indefinido	alto	médio	alto
Programação de Navios	alta	24 horas	6 horas	18 horas	indefinido	indefinido	médio	alto
Supervia web	alta	indefinido	4 horas	24 horas	indefinido	indefinido	médio	médio
SGAD	alta	24 horas	4 horas	18 horas	indefinido	indefinido	médio	médio
Portal de agendamento rodoviário	alta	indefinido	4 horas	18 horas	indefinido	indefinido	médio	médio
on-guard	alta	24 horas	4 horas	24 horas	indefinido	indefinido	alto	médio
Benner	alta	24 horas	4 horas	18 horas	alto	médio	indefinido	baixo
SEI	média	**	4 horas	48 horas	indefinido	alto	indefinido	baixo
E-mail institucional	média	indefinido	indefinido	48 horas	indefinido	médio	médio	médio
Site institucional	média	24 horas	4 horas	24 horas	indefinido	indefinido	alto	médio
Telefonia Móvel	média	**	4 horas	48 horas	indefinido	indefinido	indefinido	baixo
Sistema de controle de carga	baixa	24 horas	4 horas	48 horas	indefinido	indefinido	indefinido	médio
VPN	baixa	**	4 horas	48 horas	baixo	indefinido	indefinido	baixo

11. ANÁLISE DE RISCOS

11.1. Riscos e ameaças afetam os serviços essenciais de TI e devem ser identificados, avaliados, tratados, monitorados, controlados e documentados, de forma a mitigar o impacto de sua ocorrência na continuidade de serviços de TI. A análise apresentada a seguir detalha o risco, suas causas, consequências, probabilidade de ocorrência, impacto e controle a serem observados para garantir a continuidade de serviços de TI.

11.1.1. Riscos ambientais

Risco:	Incêndio
Causa:	• Ações humanas • Curtos-circuitos • Queimadas
Consequência:	• Indisponibilidade de recursos e serviços informatizados; • Dano físico nos equipamentos.
Probabilidade:	Baixa
Impacto:	Alto
Controle:	• Sistemas de combate a incêndio adequados para datacenters • Presença de extintores de incêndio

	• Programas de capacitação contra incêndios para todos os colaboradores

Risco:	Interrupção de energia elétrica
Causa:	• Falha no sistema de distribuição de energia por parte do provedor do serviço • Curtos-circuitos • Falha humana • Defeito em algum dos componentes do circuito elétrico (disjuntores, fusíveis, etc.)
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos
Probabilidade:	Média
Impacto:	Médio
Controle:	• Instalação de nobreaks e geradores • Manutenção preventiva/ corretiva na rede elétrica • Realização de testes para verificação das condições dos mecanismos de proteção

Risco:	Presença de água e/ou umidade nas salas de equipamento
Causa:	• Entupimento ou vazamento no sistema hidráulico do ambiente próximo às salas de equipamentos ocasionando infiltrações • Entupimento no sistema de drenagem dos aparelhos de ar-condicionado • Alagamentos causado por fortes chuvas
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos
Probabilidade:	Alta
Impacto:	Médio
Controle:	• Contratação de serviço de manutenção predial • Contratação de serviço de manutenção preventiva/ corretiva dos sistemas de refrigeração

Risco:	Desastres naturais
Causa:	• Chuvas • Vendavais • Tempestades Atmosféricas • Alagamentos • Raios
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos
Probabilidade:	Médio
Impacto:	Médio
Controle:	• Adoção de infraestrutura remota redundante (própria ou contratada)

Risco:	• Climatização inadequada da sala de equipamentos
Causa:	• Sistema de refrigeração defeituoso ou mal dimensionado
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos causado por superaquecimento

Probabilidade:	Média
Impacto:	Baixo
Controle:	• Instalação de sistema redundante de refrigeração • Contratação de serviço de manutenção preventiva/ corretiva dos sistemas de refrigeração

11.1.2. Riscos tecnológicos

Risco:	Indisponibilidade do serviço de internet/ MPLS devido a falhas internas
Causa:	• Falha nos equipamentos de rede (roteadores, switches, firewalls) • Configuração incorreta dos equipamentos de rede • Rompimento no cabeamento existente
Consequência:	• Indisponibilidade de recursos e serviços informatizados
Probabilidade:	Baixa
Impacto:	Médio
Controle:	• Manutenção preventiva nos equipamentos de rede • Aquisição de reserva técnica de equipamentos e componentes de rede • Adoção de ambiente de teste para aplicação de novas configurações

Risco:	Falha ou indisponibilidade no sistema de radiocomunicação
Causa:	• Falha nos equipamentos de rede (roteadores, switches, firewalls) • Configuração incorreta dos equipamentos de rede • Rompimento no cabeamento existente
Consequência:	• Dificuldade na comunicação imediata com agentes internos e externos ligados à operação portuária
Probabilidade:	Baixa
Impacto:	Médio
Controle:	• Inclusão de repetidoras redundantes no contrato • Definição de SLAs mais agressivos

Risco:	Indisponibilidade dos recursos de segurança (antivírus, firewall, etc.)
Causa:	• Falta de recursos financeiros para aquisição de equipamentos • Falha no planejamento para a contratação de recursos de segurança
Consequência:	• Roubo ou perda de informações • Indisponibilidade de recursos e serviços informatizados
Probabilidade:	Baixa
Impacto:	Alto
Controle:	• Capacitação na gestão de contratos e planejamento de contratações, tornando o processo mais eficiente

Risco:	Falha nos componentes de hardware dos datacenters
Causa:	• Queima de componentes eletrônicos dos equipamentos
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos
Probabilidade:	Média
Impacto:	Médio

Controle:	• Monitoramento das condições ambientais que acarretam redução no tempo de vida útil dos equipamentos • Aquisição de reserva técnica de itens mais sensíveis • Controle de obsolescência

Risco:	Falha no mecanismo de restauração de backups
Causa:	• Erros de comunicação na rede; • Quedas ou oscilações de energia; • Falhas na execução dos Jobs de backup
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Perda de informação
Probabilidade:	Média
Impacto:	Alto
Controle:	• Monitoramento diário dos relatórios de backup • Realização de testes periódicos de restauração

Risco:	Sistemas Operacionais defasados
Causa:	• Falta de recursos financeiros para aquisição de novas licenças; • Falha no planejamento para a aquisição de novas licenças. • Evolução tecnológica incompatível com processos de aquisição de instituições públicas
Consequência:	• Falha na disponibilidade de sistemas e recursos decorrente de incompatibilidade tecnológica
Probabilidade:	Baixa
Impacto:	Médio
Controle:	• Capacitação na gestão de contratos e planejamento de contratações, tornando o processo mais eficiente • Manutenção do inventário de ativos atualizado

Risco:	Indisponibilidade do sistema de CFTV
Causa:	• Falha ou defeito nos dispositivos que compõem a solução; • Término do contrato de outsourcing;
Consequência:	• Acesso indevido ao porto do Rio de Janeiro; • Maior incidência de roubos e furtos; • Perda da certificação da Conportos;
Probabilidade:	Baixa
Impacto:	Alto
Controle:	• Contratação/ renovação de sistema de CFTV, incluindo os serviços de manutenção e reposição de peças • Capacitação na gestão de contratos e planejamento de contratações, tornando o processo mais eficiente

Risco:	Indisponibilidade do sistema de controle de acesso
Causa:	• Falha ou defeito nos dispositivos que compõem a solução; • Término do contrato de outsourcing;
Consequência:	• Acesso indevido ao porto do Rio de Janeiro; • Maior incidência de roubos e furtos;

	• Engarrafamentos oriundos da adoção de procedimentos mecânicos (controle em papel) para acesso ao porto • Perda da certificação da Conportos; • Comprometimento da imagem institucional
Probabilidade:	Baixa
Impacto:	Alto
Controle:	• Contratação/ renovação de sistema de CFTV, incluindo os serviços de manutenção e reposição de peças • Capacitação na gestão de contratos e planejamento de contratações, tornando o processo mais eficiente

11.1.3. Riscos Humanos

Risco:	Ataques cibernéticos
Causa:	• Falha humana relacionada a configuração das regras de segurança dos firewalls e antivírus. • Falta de atualização do antivírus instalados nos endpoints devido problemas de conexão com o servidor. • Ausência de sistema de monitoramento de vulnerabilidades. • Manutenção de sistemas operacionais desatualizados ligados a rede de dados; • Vulnerabilidades ou erros de configuração em equipamentos, serviços e sistemas operacionais; • Falta de sistema de monitoramento de vulnerabilidades; • Falta de treinamento dos colaboradores em conscientização sobre segurança cibernética;
Consequência:	• Roubo ou perda de informações; • Vazamento de informações críticas da CDRJ e/ou seus colaboradores • Indisponibilidade de recursos e serviços informatizados. • Comprometimento da imagem institucional
Probabilidade:	Médio
Impacto:	Alto
Controle:	• Contratação de SOC; • Manutenção dos recursos de atualização automática dos softwares de proteção contra invasão; • Revisões periódicas nas regras de filtragem do firewall; • Revisões periódicas nas regras de filtragem do e-mail • Plano de Capacitações periódicas relacionadas ao tema.

Risco:	Ataques Internos
Causa:	• Manutenção das credenciais de acessos de colaboradores, após transferência compulsória de setor ou exoneração; • Roubo ou furto de equipamentos decorrente de acesso indevido; • Atos de Vandalismo
Consequência:	• Roubo ou perda de informações; • Vazamento de informações críticas da CDRJ e/ou seus colaboradores • Indisponibilidade de recursos e serviços informatizados. • Comprometimento da imagem institucional
Probabilidade:	Baixo

Impacto:	Alto
Controle:	• Manutenção dos recursos de atualização automática dos softwares de proteção contra invasão; • Revisões periódicas nas regras de filtragem do firewall; • Revisões periódicas nas permissões de acesso dos usuários; • Manutenção periódica no sistema de CFTV e controle de acesso às dependências da Companhia; • Utilização de fechadura biométrica nos datacenters; • Encaminhamento imediato das informações relativas às transferências, suspensões e exonerações por parte da GERARH e GERCAR à GERSOL; • Plano de Capacitações periódicas relacionadas ao tema

Risco:	Ausência de profissionais capacitados na área de segurança de Tecnologia da Informação
Causa:	• Ausência de capacitação de empregados; • Baixo efetivo técnico na empresa
Consequência:	• Roubo ou perda de informações decorrente da existência de recursos de proteção mal configurados • Indisponibilidade de recursos e serviços informatizados
Probabilidade:	Média
Impacto:	Alto
Controle:	• Treinamento contínuo da equipe • Contratação de serviços de suporte especializados para recomposição de equipe técnica • Contratação de serviço de instalação e configuração agregado à aquisição dos recursos de segurança.

12.ESTRATÉGIAS DE CONTINUIDADE DE SERVIÇOS DE TIC

12.1. A SUPTIN deverá adotar estratégias de continuidade de serviços de TIC que possibilitem a recuperação total ou parcial, podendo considerar as seguintes opções:

12.1.1. **Warm site**: consiste na produção de cópias de segurança dos sistemas essenciais, armazenados em local alternativo, podendo este ser um site secundário da CDRJ ou contratado, na modalidade IaaS;

12.1.2. **Mirrored site:** consiste da disponibilização de uma réplica de recursos e componentes de TIC, tais como links de internet, servidores, firewalls, dispositivos de armazenamento, etc., que deverão receber atualizações em tempo real ou em intervalos planejados e configurados para entrar em produção, em caso de interrupção. Após correção do problema, o espelhamento deverá ser restaurado, de forma que ambos voltem a estar compatíveis. Por se tratar de uma técnica que requer a duplicação de um ambiente, trata-se da alternativa mais onerosa e com

maior necessidade de suporte, sendo comumente adotada para os sistemas de alta criticidade, cujo impacto financeiro da interrupção do serviço justifica a sua adoção.

12.2. Além das estratégias mencionadas a CDRJ deverá observar as seguintes práticas:

12.2.1. Distância mínima entre o site principal e de backup de, no mínimo, 5 km;

12.2.2. Configuração de site de backup sem balanceamento de carga, a fim de se evitar ataques cibernéticos;

12.2.3. Realização de testes periódicos de serviços de TIC;

12.2.4. Atualização periódica do parque tecnológico e;

12.2.5. Replicação de aspectos de segurança lógica e física no site backup.

13.TESTES

13.1. Para garantir a efetividade dos procedimentos previstos neste PCTIC, faz-se necessário a realização de testes, que deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.

13.2. A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da Superintendência de Tecnologia da Informação.

13.3. Ao final dos testes, deverá ser emitido relatório formal apresentando os resultados obtidos, sugestões de implementação de melhorias nos procedimentos e na adoção de novas tecnologias disponíveis, quando necessário. A área de tecnologia da informação será a responsável pela elaboração e encaminhamento do relatório para ciência do CGTI, que, com base nessa documentação, poderá emitir pareceres sobre a necessidade de revisão do PCTIC.

14.ATIVAÇÃO E ENCERRAMENTO

14.1. O plano de gestão de continuidade de serviços de TI deverá ser administrado, avaliado, acionado e encerrado no âmbito da Superintendência de Tecnologia da Informação.

14.2. A ativação do PCTIC deverá ocorrer quando da ocorrência de algum dos cenários de desastres, testes ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

14.3. A tabela abaixo apresenta a lista de contatos dos principais atores envolvidos na solução do incidente ou desastre, na eventualidade de acionamento do plano de gestão de continuidade de serviços de TI. Estes contatos referem-se às áreas envolvidas na execução dos planos de ação que complementam o PCTIC.

Setor	E-mail	Telefone
SUPTIN - Superintendência de Tecnologia da Informação	suptin@portosrio.gov.br	a definir
GERSOL - Gerência de Operação de Soluções	gersol@portosrio.gov.br	(21) 99390-8613
GERCOS - Gerência de Estruturação e Construção de Soluções	gercos@portosrio.gov.br	(21) 969801394
Suporte	suporte@portosrio.gov.br	(21) 99977-4971

14.4. O encerramento da execução do PCTIC poderá ocorrer após a execução dos planos de ação que garantirão a continuidade dos Serviços de TI.

14.5. Após o encerramento deste plano a Diretoria de Tecnologia da Informação deverá guardar informações históricas para futuras análises.

15.DOCUMENTOS RELACIONADOS

15.1.1. ANEXO I: Plano de administração de crises (PAC);

15.1.2. ANEXO II: Plano de continuidade operacional (PCO);

15.1.3. ANEXO III: Plano de recuperação de desastres (PRD) e;

15.1.4. ANEXO IV: Plano de testes e verificação (PTV).

ANEXO I

PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

O plano de administração de crises especifica as ações ante os cenários de desastres. As ações incluem administrar, gerir, eliminar ou neutralizar os impactos inerente ao relacionamento entre os envolvidos e/ou afetados, até a superação da crise.

Para fins de entendimento, considera-se "desastre" um evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

OBJETIVOS

1. Garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de um desastre.
2. Orientar todos os colaboradores sobre as condutas que serão tomadas.
3. Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido. Informar aos clientes com esclarecimentos condizentes com o ocorrido em tempo hábil. Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para a superação da crise.

EXECUÇÃO DO PLANO

COMUNICAÇÃO

Na ocorrência de um desastre será necessário entrar em contato com diversas áreas e, em especial, as mais afetadas, para informá-las de seu efeito na continuidade dos serviços e tempo estimado para recuperação. Nesse cenário, o CGTI deverá atuar como uma interface entre o setor de tecnologia da informação e áreas interessadas ou afetadas pela não continuidade de serviços de TIC, repassando as informações pertinentes.

A comunicação ocorrerá da seguinte forma:

- **Comunicar as autoridades:** Deve-se comunicar as autoridades competentes em caso de desastre que envolva risco às pessoas, fornecendo informações de localização, natureza, magnitude e impacto do desastre.

TELEFONES ÚTEIS	
ENTIDADE	**CONTATO**
Polícia Militar	190
SAMU	192
Corpo de Bombeiros	193
Polícia Civil	197
Defesa Civil	199
Polícia Federal	194
Capitania dos Portos do Rio de Janeiro	(21) 2197-2554

- **Comunicar os setores responsáveis**: Além da comunicação aos responsáveis, deverá informar também:
  a) Natureza, impacto e abrangência da catástrofe;
  b) Ações de contingência em andamento;
  c) Processos / sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais).

- **Comunicar fornecedores / prestadores de serviços.**
- **Comunicar colaboradores externos.**

RECURSOS NECESSÁRIOS

Para a administração de crises deverá ser utilizado como ferramenta eletrônica de monitoramento e controle o e-mail institucional de forma a documentar todas as ações realizadas. Além deste recurso poderão ser utilizados o sistema de informação SEI e o Site Institucional.

ATIVIDADES ENVOLVIDAS

Cenário	Atividade	Responsável
Pré-crise	Informar ao CGTI sobre o incidente ocorrido, esclarecendo as condições da ocorrência e ações previstas subsequentes.	SUPTIN
	Informar aos agentes internos e externos sobre a ocorrência do incidente e as ações que estão sendo tomadas pela área de TIC.	Membros do CGTI
Crise	Identificar o problema. Registrar o motivo por que ocorreu. Registrar quando ocorreu o problema. Registrar as consequências em curto e médio prazos. Registrar quem são os responsáveis pelo ocorrido. Registrar se houve outras ocorrências. Registrar quem está envolvido na apuração da ocorrência. Registrar as medidas que já foram tomadas.	GERCOS e GERSOL
Pós-crise	Elaborar relatório de crise.	GERCOS e GERSOL
	Atualizar o PAC.	SUPTIN
	Registrar a solução para a crise no inventário de crises.	

ENCERRAMENTO DO PAC

Uma vez validado o retorno das funções essênciais do sistema e sua total estabilidade, bem como a estabilidade do datacenter, se esse for o caso, a SUPTIN entrará em contato com o GCTI que, por sua vez, informará a todos os envolvidos descritos neste plano, provendo as

informações de retorno e o status dos serviços essenciais, devendo emitir um parecer relatando as atividades realizadas para restabelecimento dos serviços.

ANEXO II

PLANO DE CONTINUIDADE OPERACIONAL (PCO)

O Plano de Continuidade Operacional descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços e restabelecer o funcionamento dos principais ativos que suportam as operações de TI, reduzindo o tempo de queda e os impactos provocados por um eventual desastre.

OBJETIVOS

1. Garantir ações de continuidade durante e depois da ocorrência de uma crise ou desastre, tratando-se apenas de ações de contingência, destinados a manter a continuidade dos processos de negócios e serviços vitais. É através deste, que as equipes de processos saberão como agir na falta ou na falha de algum componente que o suporte, garantindo assim a continuidade do processo, reduzindo os seus impactos.
2. Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações e sistemas essenciais.
3. Estabelecer controles, regras e procedimentos alternativos que possibilitem a continuidade das operações de TIC durante uma crise ou cenário de desastre.
4. Definir os formulários, checklist e/ou relatórios a serem entregues pelas equipes ao executar a contingência.

EXECUÇÃO DO PLANO

Identificada a ocorrência de um incidente, crise ou desastre, a GERSOL, responsável pelas operações e backups, deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. Após a avaliação de impacto de desastre, a equipe em exercício deverá informar à SUPTIN a respeito da avaliação e decisão sobre o acionamento do plano e início das ações de contingência que, em caso de anuência deverá:

1. Coordenar prazos e orquestrar as ações de contingência.
2. Informar as equipes de ações de contingência com a priorização dos serviços essenciais.

ATIVIDADES ENVOLVIDAS

Atividade	Responsável
Avaliar o impacto de perda de dados	GERSOL
Identificar ativos de informações afetados	
Mapear os dados a recuperar	
Estimar volume de dados, perdas e tempo de recuperação	
Executar procedimentos de recuperação	
Testar procedimentos de restauração de dados	

Documentar procedimentos, sugerindo melhorias, quando necessário	SUPTIN/GERSOL

ENCERRAMENTO DO PLANO

O plano será encerrado assim que for validado o funcionamento dos sistemas essenciais e do Datacenter, se esse for o caso, relatando a sua estabilidade e a sua normalidade. Após esse processo, será emitido um parecer da equipe responsável, informando o que ensejou o acionamento do plano, as atividades realizadas e os recursos que foram utilizadas para então, comunicar ao CGTI sobre a estabilidade do ambiente.

ANEXO III

O Plano de Recuperação De Desastres descreve os cenários de inoperância e seus respectivos procedimentos, para que, uma vez definindo as atividades prioritárias para restabelecer o nível de operação dos serviços, controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação.

OBJETIVOS

1. Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.
2. Estabelecer procedimentos de comunicação e mobilização adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas que causem impacto nas rotinas operacionais relacionadas a Tecnologia da Informação.
3. Aplicar ações necessárias para correção e/ou eliminação do problema de forma a garantir o nível adequado de funcionamento dos recursos, serviços e sistemas informatizados da CDRJ.
4. Possibilitar a avaliação dos danos aos ativos, serviços essenciais e conexões do datacenter.
5. Prover meios para a recuperação de danos aos ativos.
6. Evitar desdobramentos de outros incidentes na instalação principal.
7. Restabelecer o serviço/sistema essencial no datacenter principal dentro do prazo tolerável.

EXECUÇÃO DO PLANO DE RECUPERAÇÃO

Para que o plano transcorra como planejado, a equipe da GERSOL deverá executar os seguintes passos: Identificar e listar todos os ativos danificados da ocorrência do desastre;

1. Identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, WAN ou com o provedor de serviços;
2. Mapear quais os serviços foram descontinuados, contendo as informações de perda de ativo e de conexão.
3. Elaborar um cronograma de recuperação das aplicações, levando em consideração as seguintes aplicações para recuperação:
   a) Substituição dos ativos e equipamentos;
   b) Reconfiguração de ativos e equipamentos
   c) Teste de ambiente.

ENCERRAMENTO DO PLANO

O plano será encerrado assim que os procedimentos de recuperação forem realizados por todas as equipes. Ao término de todos os procedimentos, as informações de recuperação de serviços serão consolidadas em parecer específico, informando o horário de reestabelecimento de cada serviço, equipamentos adquiridos e/ou realocados, se for o caso, fornecedores que tiveram de ser acionados procedimentos de recuperação realizados, entre outras informações relevantes.

ANEXO IV

PLANO DE TESTES E VERIFICAÇÃO (PTV)

Os testes deverão ser formalmente registrados observando as necessidades de aprimoramento que, quando identificadas, deverão ser alvo de plano de ação por parte do responsável pelas ações de correções e (ou) adequações que visem a acrescentar melhorias na sua utilização. A área de TI poderá realizar os seguintes tipos de testes:

a) **Simulação do teste:** conduzido assim que o plano de gestão de continuidade de serviço de TI for concluído, através de simulação dos procedimentos por todas as pessoas relevantes para a execução das ações contidas no plano de ação, de forma a avaliar o entendimento e a integração das atividades.

b) Teste total: conduzido assim que o plano de gestão de continuidade de serviço de TI for concluído. Deverá ser realizado de forma periódica. Deverá envolver as áreas de negócio para acompanhar e validar os testes de restauração dos serviços.

c) **Teste parcial:** não substitui a necessidade do teste total, mas poderá ser realizado como complemento do teste total, em um espaço de tempo menor e em uma escala menor com somente alguns serviços ou componentes de TI.

d) **Teste de cenário:** deverá simular condições específicas, eventos e cenários de risco.

RECURSOS UTILIZADOS

Para a realização dos testes e validação dos serviços de TI, a área de TI deverá configurar um ambiente de testes contendo minimamente:

a) Virtualização de servidores;
b) Link de Internet;
c) Principais serviços implantados pela área de TI.