PDTIC

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

2021-2024

HOSPITAL DE CLÍNICAS
PORTO ALEGRE RS

CGTIC
Coordenadoria de Gestão da Tecnologia da Informação e Comunicação

EQUIPE DE ELABORAÇÃO

Coordenador de Gestão de Tecnologia da Informação e Comunicação (CGTIC)
André Mena Ávila

Chefe do Serviço de Gestão de Negócio (SGN)
Paula Luisa Broenstrup Correa

Chefe do Serviço de Gestão de Tecnologia (SGT)
Renato Falsarella Malvezzi

Chefe do Serviço de Sustentação e Relacionamento (SSR)
Marina Delazzeri

Supervisor de Gestão de Contratos e Aquisições (SuCon)
Luiz Marcos Zambonato

Supervisor de Gestão de Portfólio, Projetos e Inovação (SuGePPI)
Edson Rodrigues Bicca

Analista Webdesigner da Seção de Desenvolvimento e Operação (SeDOps)
Guilherme Mendes Pereira

SUMÁRIO

1. INTRODUÇÃO

A Tecnologia da Informação e Comunicação (TIC) está cada vez mais inserida nos negócios das instituições, gerando valor e qualidade aos processos de trabalho, produtos e serviços das organizações. Soluções de TIC são implementadas visando processos mais eficientes, com flexibilidade das rotinas e desenvolvimento de serviços mais inovadores alinhados à estratégia institucional.

A visão estratégica de TIC permite não apenas a sustentação dos objetivos organizacionais, mas, também, por meio da otimização de atividades, eliminação de barreiras de comunicação e melhoria do processo decisório, viabilizando novas oportunidades para ampliação e evolução dos serviços oferecidos. Assim, o planejamento torna-se indispensável para que haja uma maior eficiência e um melhor aproveitamento dos recursos.

No Hospital de Clínicas de Porto Alegre (HCPA) as orientações estratégicas de TIC definidas pela Diretoria Executiva estão documentadas no Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) e devem ser desdobradas no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). O PETIC atual tem vigência de 2021 a 2024 e foi elaborado sob coordenação do Comitê de Governança Digital (CGD) e aprovado pela Diretoria Executiva em 29/12/2021.

Foram utilizados como referência para elaboração do presente PDTIC o Guia de Governança de TIC v2.0 e o Guia de PDTIC do SISP v2.0 elaborados pela Secretaria de Tecnologia da Informação (STI) do Ministério do Planejamento, Orçamento e Gestão (MP), na condição de órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

2. OBJETIVO

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) tem o objetivo de desdobrar as estratégias do PETIC, em alinhamento com o Plano de Negócios e Gestão Estratégica (PNGE), contendo o diagnóstico, o planejamento e a gestão dos recursos e processos, definindo estratégias e o plano de ação para atender as necessidades de Tecnologia da Informação e Comunicação (TIC) do HCPA.

3. METODOLOGIA

O processo de elaboração do PDTIC contou com a participação de lideranças e funcionários da Coordenadoria de Gestão da Tecnologia da Informação e Comunicação (CGTIC), bem como com contribuições das áreas de negócio e diretorias representadas no Comitê de Governança Digital (CGD) do HCPA. Através de reuniões periódicas, realizou-se o planejamento, diagnóstico do ambiente e necessidades de TIC, análise das estratégias formuladas no PETIC, aplicação de conhecimentos técnicos e apoio em guias referenciais de boas práticas de mercado.

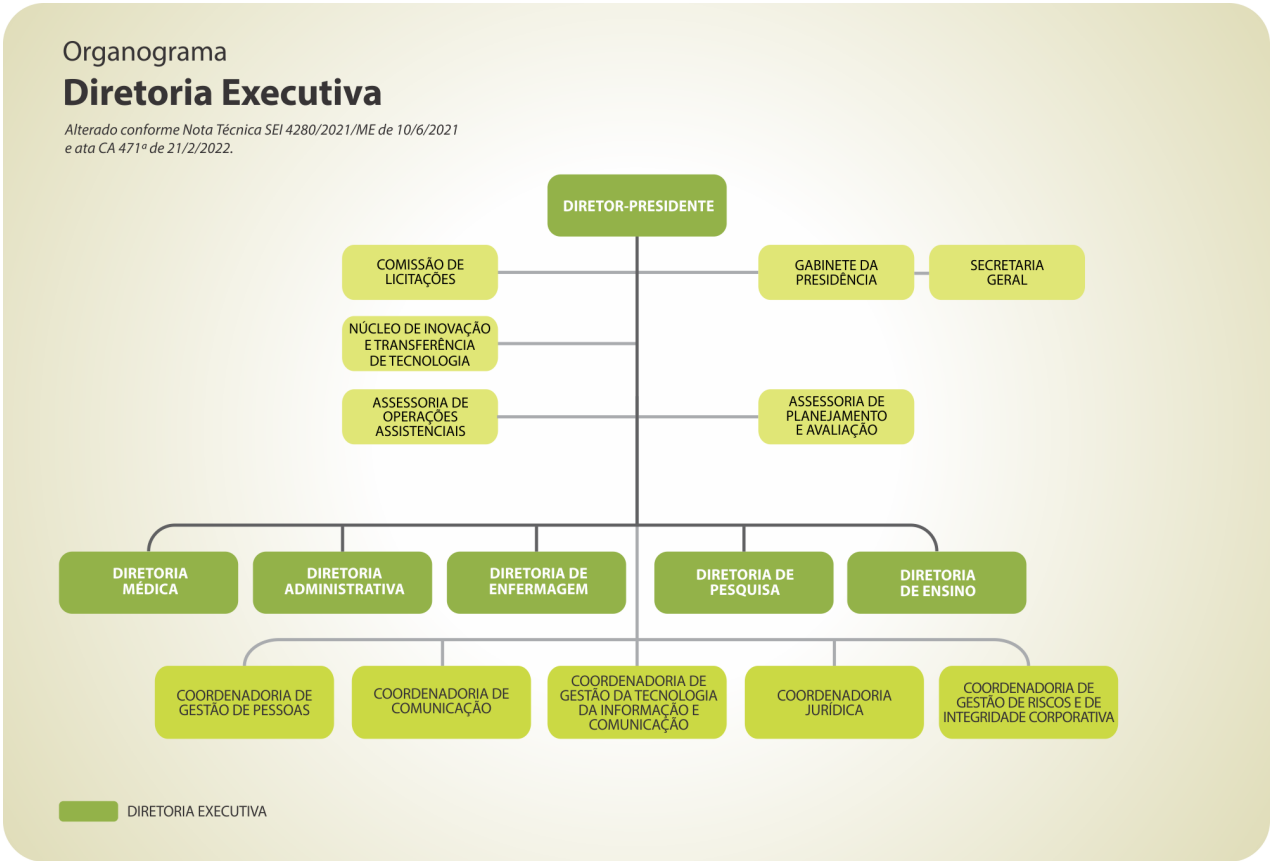
A tabela abaixo apresenta as principais etapas do processo de elaboração do PDTIC:

Fase	Descrição	Status
1	Recebimento do PETIC 2021-2024 aprovado pela Diretoria Executiva	**Concluído**
2	Diagnóstico da situação de TIC	**Concluído**
3	Elaboração do PDTIC	**Concluído**
4	Apresentação e aprovação do PDTIC pelo Comitê de Governança Digital	**Concluído**

4. CONTEXTO DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

O HCPA possui longo histórico de produção e reconhecimentos na área de Tecnologia da Informação e Comunicação em Saúde. O primeiro registro na estrutura do hospital data do ano de 1977 com a criação do Serviço de Processamento de Dados, atualmente Coordenadoria de Gestão da Tecnologia da Informação e Comunicação (CGTIC), vinculada à Presidência.

4.1. Posição da CGTIC no organograma da Diretoria Executiva



4.2. Organograma interno da CGTIC

Organograma
interno da CGTIC

4.3. Missão CGTIC

Prover soluções digitais com agilidade, qualidade e segurança à realização da Missão Institucional.

4.4. Visão CGTIC

Maximizar e qualificar a experiência em saúde com a transformação digital.

4.5. Comitê de Governança Digital

O HCPA, com base no Decreto 8.638/2016 que instituiu a política de Governança Digital no âmbito da Administração Pública Federal (APF), criou em 17 de Janeiro de 2017 o Comitê de Governança Digital (CGD), com composição representativa das diretorias e diversas áreas da Instituição. O CGD representa estrategicamente a Diretoria Executiva do HCPA e tem por objetivo elaborar, propor e acompanhar as

políticas relativas à Governança Digital que representem as necessidades de TIC da Instituição e que sejam fonte geradora de benefícios à sociedade.

4.6. Composição de pessoal e descrição sumária das atividades e funções das áreas que compõem a CGTIC

O quadro de pessoal da CGTIC é composto por 97 profissionais conforme detalhamento abaixo e funcionograma da área com os respectivos objetivos:

Ocupação	Total
Analista de Négocio	26
Analista de Desenvolvimento de TI	12
Assistente de Microinformática e Oficina	11
Assistente Técnico de Rede	9
Analista de Suporte em Infraestrutura	8
Analista Administrador de Banco de Dados	5
Chefe de Seção	5
Supervisor	4
Analista Consultor de Projetos	3
Chefe de Serviço	3
Analista de Business Intelligence	3
Analista de Arquitetura de Sistemas	2
Analista de Segurança da Informação	2
Técnico Secretariado	1
Webdesigner	1
Auxiliar de Enfermagem Reabilitado	1
Coordenador	1
Total geral	**97**

4.6.1. Coordenadoria de Gestão da Tecnologia da Informação e Comunicação (CGTIC)

A CGTIC tem como objetivo prover os serviços de Tecnologia da Informação e Comunicação (TIC) às áreas do HCPA para potencializar as atividades de assistência, gestão, ensino e pesquisa, em consonância com o PETIC e o PNGE. Compete à CGTIC:

- Garantir o alinhamento de TIC com o negócio do Hospital;
- Conceber, especificar, desenvolver, integrar e aperfeiçoar as soluções de TIC;
- Gerenciar e executar projetos de TIC;
- Projetar, implantar e prestar suporte técnico à infraestrutura de TIC;
- Gerenciar os contratos com empresas prestadoras de serviços em TIC e fornecedoras de hardwares e softwares;
- Propor e gerir normas técnicas para segurança da informação e utilização dos ativos de TIC;
- Gerenciar o parque de ativos de TIC sob sua gestão;
- Garantir agilidade, confidencialidade, integridade e disponibilidade dos aplicativos, dos serviços e das informações institucionais armazenadas no âmbito da TIC do HCPA;
- Fomentar iniciativas de Inovação e acompanhar as tendências do mercado de TIC;
- Apoiar as áreas de negócio, na definição dos recursos de TIC, no uso dos sistemas de software e no gerenciamento de projetos de negócio com TIC;
- Elaborar memoriais descritivos, pareceres, aceites e outros documentos técnicos da área de TIC;
- Preservar a integridade técnica dos equipamentos de TIC sob sua gestão;

- Atuar no relacionamento externo com parceiros da Comunidade AGHUse;
- Representar institucionalmente o HCPA em atividades relacionadas a TIC.

4.6.1.1. Supervisão de Gestão de Portfólio, Projetos e Inovação (SuGePPI)

Compete à Supervisão de Gestão de Portfólio, Projetos e Inovação, o planejamento, acompanhamento e atuação permanente na execução dos projetos de negócio com TIC, adotando metodologias e práticas em gerenciamento de projetos, visando garantir o atendimento pleno, com qualidade, escopo, prazo e orçamento definido. Cabe, também à SuGePPI, propor iniciativas e programas para incentivar e premiar a prática da inovação na CGTIC.

4.6.1.2. Supervisão de Gestão de Contratos e Aquisições (SuCon)

Compete à Supervisão de Gestão de Contratos e Aquisições, as atividades relacionadas ao processo de aquisições e contratações, condução ou apoio à elaboração de editais, especificações técnicas, orçamentação e relacionamento técnico com fornecedores em aquisições ou contratações, bem como apoiar os gestores de contratos no acompanhamento permanente da boa execução, vigência, medições, aplicação de penalidades e demais boas práticas na gestão dos contratos.

Seus integrantes também atuam junto às Comissões Institucionais de Fiscalização de Contratos, instituídas através do PLA-0049 da

Administração Central - Plano de Gerenciamento e Fiscalização de Contratos.

4.6.1.3. Serviço de Gestão de Tecnologia (SGT)

Compete ao Serviço de Gestão de Tecnologia, realizar atividades técnicas de desenvolvimento de aplicativos, a operação e o monitoramento dos serviços de TIC, a gestão de banco de dados, a atualização e segurança da infraestrutura de TIC e a gestão do datacenter.

4.6.1.3.1. Seção de Desenvolvimento e Operações (SeDOps)

Compete à Seção de Desenvolvimento e Operações, a gestão da equipe técnica de desenvolvedores e arquitetura de software, garantindo as boas práticas, metodologia e integração com a operação de sistemas (DevOps), assegurando que as atividades multiprofissionais (desenvolvimento, bancos de dados, infraestrutura etc.) atuem de forma harmônica para a otimização de resultados.

4.6.1.3.1.1. Supervisão de Monitoramento e Controle (SuDevOps)

Compete à Supervisão de Monitoramento e Controle, a realização de atividades de automação e otimização dos processos de

atualização de software, gerência de configuração, testes automatizados e garantia da qualidade do desenvolvimento.

4.6.1.3.2. Seção de Infraestrutura e Segurança (SeISeg)

Compete à Seção de Infraestrutura e Segurança de TIC, prestar suporte técnico, projetar e implantar infraestrutura, visando garantir a operacionalidade dos serviços de TIC da Instituição com segurança, qualidade e alta disponibilidade. Responsável pela proposição, gestão e monitoramento de normas e políticas, visando garantir a confidencialidade, integridade e disponibilidade das informações no âmbito da TIC.

4.6.1.3.2.1. Supervisão de Gestão de Datacenter (SuDat)

Compete à Supervisão de Gestão de Datacenter, o monitoramento da alta disponibilidade dos serviços de TIC (24 horas x 7 dias por semana), a execução de rotinas operacionais, a responsabilidade pela segurança física do datacenter e da CGTIC e pela integridade e manutenção da rede física de TIC.

4.6.1.4. Serviço de Sustentação e Relacionamento (SSR)

Compete ao Serviço de Sustentação e Relacionamento, ser a entrada principal da CGTIC para contatos oriundos dos usuários e parceiros internos e externos, garantindo a sustentação dos serviços de TIC com qualidade e satisfação dos usuários. Deverá conduzir

proativamente ações de divulgação, capacitação, medição dos níveis de satisfação e utilização adequada dos serviços, realizando a gestão e correção de incidentes, assim como, desenvolvimento de melhorias, de forma alinhada com as definições e orientações estratégicas.

4.6.1.4.1. Seção de Sustentação e Relacionamento Interno (SeRI)

Compete à Seção de Sustentação e Relacionamento Interno, a condução das atividades do Serviço no âmbito interno do HCPA com conhecimento negocial e resolutividade, buscando a satisfação da comunidade interna.

4.6.1.4.1.1. Supervisão de Gestão de Ativos (SuAt)

Compete à Supervisão de Gestão de Ativos, a garantia do funcionamento pleno da infraestrutura de usuários finais (microinformática, impressoras, softwares utilitários, etc.), com controle, suporte e manutenção de qualidade.

4.6.1.4.2. Supervisão de Sustentação e Relacionamento Externo (SuREx)

Compete à Supervisão de Sustentação e Relacionamento Externo, garantir as entregas, incidentes e dúvidas dos parceiros que fazem parte da Comunidade AGHUse, realizando ações proativas de relacionamento em busca da satisfação nos atendimentos

prestados aos parceiros externos, servindo como elo de ligação com todas as áreas internas multidisciplinares do HCPA.

4.6.1.5. Serviço de Gestão de Negócio (SGN)

Compete ao Serviço de Gestão de Negócio, a concepção negocial para desenvolvimento, integração e aperfeiçoamento das soluções de TIC, utilizando metodologias e boas práticas de qualidade e produtividade, visando dotar o HCPA de sistemas otimizados, atualizados e de alta diferenciação no atendimento às exigências negociais. Realiza a gestão das demandas de projetos solicitadas, junto às áreas de Negócio.

4.6.1.5.1. Seção de Sistemas Assistenciais (SeAs)

Compete à Seção de Sistemas Assistenciais o planejamento dos projetos bem como a realização das atividades do Serviço na abrangência de sistemas assistenciais e de apoio assistencial. Deverá primar pela transferência de conhecimento negocial para as equipes de sustentação e relacionamento, bem como prestar apoio a estas quando necessário.

4.6.1.5.2. Seção de Sistemas Administrativos (SeAd)

Compete à Seção de Sistemas Administrativos, a realização das atividades do Serviço na abrangência de sistemas administrativos. Deverá primar pela transferência de conhecimento negocial para as equipes de sustentação e relacionamento, bem como prestar apoio a estas quando necessário.

4.7. Indicadores estratégicos, táticos e operacionais

A seguir estão apresentados os indicadores a serem acompanhados pela CGTIC ao longo da vigência do presente PDTIC, em alinhamento com o PETIC 2021-2024:

4.7.1. Indicadores que integram o PNGE e o PETIC (Estratégicos)

Indicador	Periodicidade	Meta		
		2022	2023	2024
Eixo 1 - Estabelecer uma cultura baseada em dados para tomada de decisão				
Atingir o nível AMAM 4 de maturidade da HIMSS Analytics	Anual	>= 70% estágios 1 e 2	>= 70% estágios 1 a 3	>= 70% até estágio 4
Ação:	Estruturar o Centro de Ciência de Dados (anexo 1)			
Eixo 2 - Aprimorar a governança de dados e TIC				
Ação:	Estruturar o Núcleo de Saúde Digital			

4.7.2. Indicadores que integram o PETIC (Táticos)

Indicador	Periodicidade	Meta		
		2022	2023	2024
Eixo 3 - Garantir a sustentabilidade das TICs				
Entrada de documentos de prontuário em papel no SAMIS	Mensal	<= 200 Kg	<= 150 Kg	<= 100 Kg
Taxa de contribuição dos parceiros da comunidade para o AGHUse (em MPs*)	Trimestral	>= 120	>= 140	>= 160

Eixo 4 - Primar pela Transformação Digital				
Taxa de Crescimento da Solução AGHUse (em MPs*)	Trimestral	>= 1300	>= 1350	>= 1400
Atingir o estágio 6 de maturidade do EMRAM da HIMSS	Anual	100% estágio 4	100% estágio 5	100% estágio 6

*** MPs = Macropontos**

4.7.3. Indicadores definidos no PDTIC (Operacionais)

Indicador	Periodicidade	Meta	Área
Eixo 3 - Garantir a sustentabilidade das TICs			
Comprometimento das despesas diretas de TIC em relação ao total das despesas diretas do HCPA	Mensal	Entre 2% e 3%	CGTIC
Taxa de editais vantajosos ao HCPA com redução do preço orçado	Semestral	50 %	SuCon
Taxa de contratos prorrogados em até 30 dias antes do vencimento	Anual	100 %	SuCon
Taxa de contribuição dos parceiros da comunidade para o AGHUse	Trimestral	>= 120 MPs	CGTIC
Taxa de contribuição dos parceiros da comunidade para o AGHUse com o apoio da SuREx			SSR
Garantir que os servidores da CGTIC estejam protegidos (antivírus instalado)	Anual	>= 95 %	SGT
Eixo 4 - Primar pela Transformação Digital			
Taxa de crescimento em projetos da solução AGHUse	Mensal	>= 67,6 %	SGN
Taxa de crescimento em sustentação da solução AGHUse	Mensal	>= 27 %	SSR
Taxa de crescimento em tecnologia da solução AGHUse	Mensal	>= 5,4 %	SGT

Taxa de projetos entregues conforme planejado	Trimestral	>= 70 %	CGTIC
Taxa de projetos de negócio entregues conforme planejado			SGN
Taxa de projetos de tecnologia entregues conforme planejado			SGT
Taxa de projetos com GPs entregues conforme planejado			SuGePPI
Taxa de projetos AGHUse entregues conforme planejado	Trimestral	>= 80 %	SuGePPI
Redução na abertura de incidentes	Mensal	<= 213	CGTIC
Taxa de MPs desenvolvidos que tiveram o envolvimento da Fábrica de Qualidade	Mensal	>= 75 %	SGT
Atendimentos dentro do SLA (Acordo de Nível de Serviço)	Mensal	>= 85 %	CGTIC
Atender com o SLA positivo os incidentes de projeto			SGN
Atender com o SLA positivo os incidentes e serviços de sustentação			SSR
Atender com o SLA positivo os incidentes e serviços de tecnologia			SGT
Atender com o SLA positivo as dúvidas de parceiros	Mensal	>= 95%	SSR
Participação de projetos com HIMSS EMRAM	Anual	>= 30 %	SGN
Aumentar a segurança corporativa e de TI com o certificação da HIMSS	Anual	>= 50 %	SGT
Taxa de Modernização da rede sem fio do bloco A	Anual	>= 50 %	SGT
Taxa de disponibilidade do AGHUse	Mensal	>= 99,8 %	SGT

5. SITUAÇÃO ATUAL DA TIC NO HCPA

5.1. SISTEMAS

5.1.1. Sistemas internos (desenvolvidos pelo HCPA)

AGHUse® - Sistema de Gestão em Saúde

O AGHUse é o sistema de gestão em saúde desenvolvido no HCPA, registrado como propriedade intelectual no Instituto Nacional da Propriedade Industrial (INPI) na modalidade "Programa de Computador" através do processo BR 51 2016 000359-6, publicado na revista INPI Nº 2378 de 02 de Agosto de 2016 (pág. 366).

O AGHUse é também disponibilizado para utilização por outras instituições como software de código aberto, sem custos de licenciamento. Atividades prestadas pelo HCPA para outras instituições, tais como treinamentos técnicos ou negociais, apoio na implantação etc., são objeto de cobrança, tendo por pré-requisito a assinatura de instrumentos específicos como contrato ou termo de cooperação.

Em termos de funcionalidades, o AGHUse começou a ser desenvolvido ainda nas décadas de 70/80, com tecnologia mainframe (computador de grande porte). Com o passar dos anos foram necessárias incorporações de novas tecnologias e atualizações, sendo que por volta do ano 2000 foi realizada uma grande atualização tecnológica do sistema, migrando da tecnologia mainframe para tecnologia em baixa plataforma (microcomputadores), quando o sistema passou a ser denominado AGH - Aplicativos para Gestão Hospitalar.

No ano de 2009, por solicitação do Ministério da Educação (MEC), foi iniciado o projeto AGHU - Aplicativo de Gestão para Hospitais Universitários, com o objetivo de disseminar em todos os Hospitais Universitários Federais ligados ao MEC o modelo de gestão utilizado no HCPA, quando foi então iniciada a migração tecnológica do sistema AGH para uma tecnologia de código aberto (linguagem de programação Java e compatibilidade com banco de dados PostgreSQL). Atualmente, o sistema AGHU, em suas várias versões, encontra-se instalado em cerca de 40 hospitais universitários federais em todo o país integrantes da rede Ebserh.

Com o crescimento e robustez do AGHUse, o HCPA tem demandado esforços no sentido da consolidação de uma comunidade de desenvolvimento colaborativo com a participação das instituições que optam pela adoção do AGHUse. Ao integrarem a comunidade e terem acesso aos códigos fontes e ao ecossistema de desenvolvimento, comprometem-se, como contrapartida, desenvolver colaborativamente novas funcionalidades e incorporá-las no sistema para que fique disponível para uso de todos. A Comunidade AGHUse foi formalmente instituída em 08 de Agosto de 2017, através de ato da Presidência do HCPA e conta atualmente com 8 (oito) instituições:

- Hospital de Clínicas de Porto Alegre (HCPA),
- Exército Brasileiro (EB),
- Força Aérea Brasileira (FAB),
- Marinha do Brasil (MB),
- Secretaria da Saúde do Estado da Bahia (SESAB),
- Universidade Estadual de Campinas (UNICAMP),
- Universidade Federal do Rio de Janeiro (UFRJ) e
- Universidade Federal do Rio Grande do Sul (UFRGS) - Faculdade de Odontologia.

A tabela abaixo apresenta as principais funcionalidades presentes no sistema AGHUse:

Funcionalidade	Descrição
Assistenciais	
Ambulatório administrativo	Possibilita a gestão do processo administrativo do atendimento ambulatorial, permitindo a configuração das agendas ambulatoriais e marcação de consultas.
Ambulatório assistencial	Contempla o registro do atendimento assistencial do paciente no ambulatório, permitindo o registro da anamnese, evolução, receitas, atestados, exames, prescrição médica, consultoria ambulatorial, alta e agendamento da consulta de retorno.
Anamnese e Evolução	Registra a história clínica do paciente e a evolução do tratamento por todos os profissionais de saúde.
Certificação Digital	Tecnologia incorporada nos documentos que exigem assinatura do profissional de saúde e que garante autenticidade, integridade e validade jurídica dos documentos que compõem o Prontuário Eletrônico do Paciente, utilizando certificados digitais dos profissionais e eliminando a necessidade de impressão.
Checagem Beira Leito	Contempla o suporte ao processo de aprazamento e administração de prescrições médicas e de cuidados de enfermagem à beira do leito.
Cirurgia e Procedimento Diagnóstico Terapêutico (PDT)	Permite a realização do planejamento cirúrgico, escala de cirurgias, descrição cirúrgica, nota de sala e monitoramento do fluxo de pacientes dentro do centro cirúrgico.
Comissões	Suporta o trabalho de comissões hospitalares como a comissão de residência, prontuários, medicamentos e outras.
Controle de Infecção	Permite o acompanhamento de casos de infecção do hospital através da inclusão de notificações de infecções e gerenciamento de leitos de isolamento.
Controles do Paciente	Compreende o registro dos sinais vitais, balanço hídrico e outros controles essenciais para o acompanhamento do estado geral do paciente.
Emergência	Permite o registro do atendimento do paciente desde a triagem e classificação de risco até a saída da emergência.

Escalas de Risco	Permite realizar o registro das escalas assistenciais de risco e a visualização do histórico no POL.
Exames	Compreende o fluxo de solicitação de exames, coleta, execução, confecção do laudo e visualização do mesmo.
Farmácia	A partir das prescrições médicas, realiza o processo de triagem e dispensação de medicamentos pelo farmacêutico. Através da integração com o módulo de estoque, possibilita o registro de movimentação direta de consumo do material.
Fisiatria	Permite prescrever, agendar e acompanhar a execução das modalidades e equipes necessárias ao paciente para tratamento fisiátrico.
Internação	Realiza a gestão das internações, contemplando todas as operações: gestão de leitos, transferência de paciente, alta administrativa, entre outros.
Nutrição	Permite o gerenciamento da prescrição dietética, elaborada pela nutricionista, baseada na prescrição médica. Possibilita a elaboração do mapa de dietas, instrumento de trabalho dos técnicos de nutrição.
Pacientes	Realiza a entrada do paciente no sistema através do cadastramento dos seus dados e geração das etiquetas de identificação, podendo haver abertura de prontuário ou não. Para os pacientes com prontuário, através do módulo é possível a gestão do prontuário, controle de movimentação, substituição, unificação e alteração da situação do cadastro.
Perinatologia	Realiza o registro do atendimento perinatal desde o acompanhamento de gestações, pré-parto, parto, nascimento e intercorrências.
Prescrição de Diálise	Presta suporte ao tratamento de diálise desde o atendimento ambulatorial até a internação.
Prescrição de Enfermagem	Realiza o registro das ordens de cuidados de enfermagem.
Prescrição Médica	Possibilita ao médico assistente o registro das ordens médicas que serão executadas por diversos profissionais da saúde, incluindo: dieta, cuidados, medicamentos, soluções, nutrição parenteral total, consultorias, procedimentos etc.
Prontuário On-Line	Contempla as informações clínicas do paciente, englobando todos os atendimentos realizados no hospital, classificados por tipo de informação: internações, cirurgias, exames realizados, procedimentos, diagnósticos.

Quimioterapia	Presta suporte ao tratamento de quimioterapia desde o atendimento ambulatorial até a internação.
Transplantes	Apoia a gestão dos programas de transplantes de órgãos e tecidos, possibilitando controle da doação, oferta de órgãos e gerenciamento da lista de pacientes.
Administrativos	
Compras	Compreende a gestão do processo de compra de materiais e serviços através de processo público de licitação, pregão eletrônico, desde a solicitação até a entrega do material. Permite a programação de entregas pelo fornecedor, empenho do orçamento e integração com o Siafi e com o Controle de Qualidade através do parecer técnico.
Custo Absorção	Implementa a forma de custeio por absorção, possibilitando obter os custos dos tratamentos por produtos assistenciais.
Custos Contábeis	Efetua os cálculos na ótica contábil para realizar a distribuição de despesas na forma de custeio por absorção.
Engenharia	Permite a gestão de solicitações de chamados de manutenção da engenharia desde a abertura, acompanhamento de execução e encerramento. Também permite o planejamento e geração das manutenções periódicas (preventivas e calibrações) de equipamentos e serviços.
Escalas Profissionais	Permite elaborar as escalas de profissionais de saúde, como plantões e turnos de trabalho.
Estoque	Controla o fluxo de materiais, proporcionando a entrega no local correto, no momento exato, na devida quantidade através da gestão de materiais do almoxarifado, nota de recebimento, ajustes, transferências, devoluções, requisição de materiais e ponto de pedido com geração automática de reabastecimento. Possibilita a consignação e administração de materiais de órtese e prótese, assim como produção interna de materiais de farmácia, gráfica e rouparia.
Faturamento	Captura as informações necessárias para fechamento das contas hospitalares e gera os arquivos para interfaceamento com os sistemas de informações ambulatorial e hospitalar do Ministério da Saúde.

Financeiro	Permite o gerenciamento e controle das atividades financeiras. Garante a Previsão Orçamentária para suprir as necessidades de consumo de materiais e serviços, a administração, tributação, liquidação e contabilização das Notas Fiscais, o pagamento de títulos e a integração com o SIAFI.
Investimentos	Possibilita o gerenciamento dos investimentos desde a solicitação até a conclusão pela Comissão de Investimentos do HCPA.
OPME	Gerenciamento do fluxo de autorização / utilização de órteses/próteses.
Ordens de Manutenção	Gerenciamento e controle das ordens de manutenção de bens patrimoniais e serviços integrados ao sistema corporativo.
Patrimônio	Contempla o controle dos bens imobilizados que ingressam com relação à quantidade, movimentação, localização e cálculo de depreciação.
Pesquisa	Compreende o processo de submissão, avaliação e gestão de projetos de pesquisa.
Interoperabilidade	
AGFA Enterprise Image (PACS)	Permite o armazenamento, processamento e acesso às imagens médicas.
Bionexo / Plannexo	Permite adequar os níveis de estoque, ampliando o número de parâmetros a serem considerados na compra, auxiliando na redução de estoques e mantendo-os em níveis mais adequados.
Datasus	Permite a interoperabilidade com os diversos sistemas do Datasus, como o CADSUS, E-SUS, SIA, SIGTAP, SISCOLO, etc.
Dispensário Eletrônico	Permite a provisão e dispensação de medicamentos e materiais nas unidades de internação.
Epimed	Permite a interoperabilidade para gestão e análise de indicadores da UTI, através de benchmarking exclusivo e análises preditivas para auxiliar na tomada de decisões.
Exames na Internet	Permite a interoperabilidade dos laudos de exames para disponibilização de acesso na Internet.

GERCON / GERINT / GERPAC	Estabelece a Interoperabilidade com os sistemas do complexo regulador da Secretaria Municipal de Saúde de Porto Alegre.
Liquid	Permite a gestão eletrônica de documentos digitalizados.
Monitores Multiparamétricos	Permite a interoperabilidade dos controles do paciente através dos monitores multiparamétricos.
PagTesouro	Permite a interoperabilidade do processamento de pagamentos digitais com a Secretaria do Tesouro Nacional.
Papelaria	Permite a interoperabilidade do suprimentos com o sistema do fornecedor de material de escritório.
RealBlood	Permite a interoperabilidade dos registros sanguíneos realizados no banco de sangue.
REINF	Permite a escrituração fiscal digital de retenções e outras informações fiscais.
SIAFI	Permite a interoperabilidade do controle, processamento e execução, financeira, patrimonial e contábil com o Sistema Integrado de Administração Financeira do Governo Federal.
SIAPE	Permite a interoperabilidade com o Sistema Integrado de Administração de Recursos Humanos do Governo Federal.
STARH	Permite a interoperabilidade dos registros de colaboradores com relação a sua situação funcional.
Supply Station	Permite a provisão e registro dos materiais consumidos em procedimentos cirúrgicos.
TISS	Permite a interoperabilidade com as operadoras de saúde através do padrão TISS da ANS.

Meu Clínicas - O aplicativo do paciente do HCPA

Com o objetivo de entregar uma nova tecnologia com foco no paciente que tenha utilidade para sua assistência à saúde, preservando a privacidade e a segurança através da interoperabilidade, agilidade e sustentabilidade, além de oferecer uma interface de relacionamento do paciente com o HCPA e melhorar a sua experiência, facilitando o acesso aos recursos em saúde da instituição, foi criado o aplicativo Meu Clínicas para atender necessidades específicas dos pacientes, com o acesso às suas informações de forma fácil, ágil e amigável, evitando deslocamentos até o HCPA, possibilitando o distanciamento social durante a pandemia.

O aplicativo permite a facilidade e segurança de acesso à aplicação através do localizador único HCPA, viabilizando acesso ao histórico e comprovante de consultas, atualização cadastral, resultados de exames e receitas (com controle de utilização e dispensação pelas farmácias), auto agendamento de consultas, acesso fácil nas catracas do ambulatório do HCPA através do cartão do paciente (CNS), solicitação de documentos de prontuário, pesquisas de experiência do paciente, assinatura do termo de aceite à Lei Geral de Proteção de Dados (LGPD), a disponibilização das etiquetas de materiais implantáveis OPME. Além da versão web, encontra-se disponível nas lojas Google Play e Apple Store.

AGHUse Mobile

AGHUse Mobile

O AGHUse Mobile foi criado com o objetivo de disponibilizar as informações do prontuário do paciente com o uso de dispositivos móveis através da rede wi-fi do HCPA.

O aplicativo permite o acesso à lista de pacientes internados, consulta à evolução, diagnósticos, anamnese, prescrição, alergias, conduta de

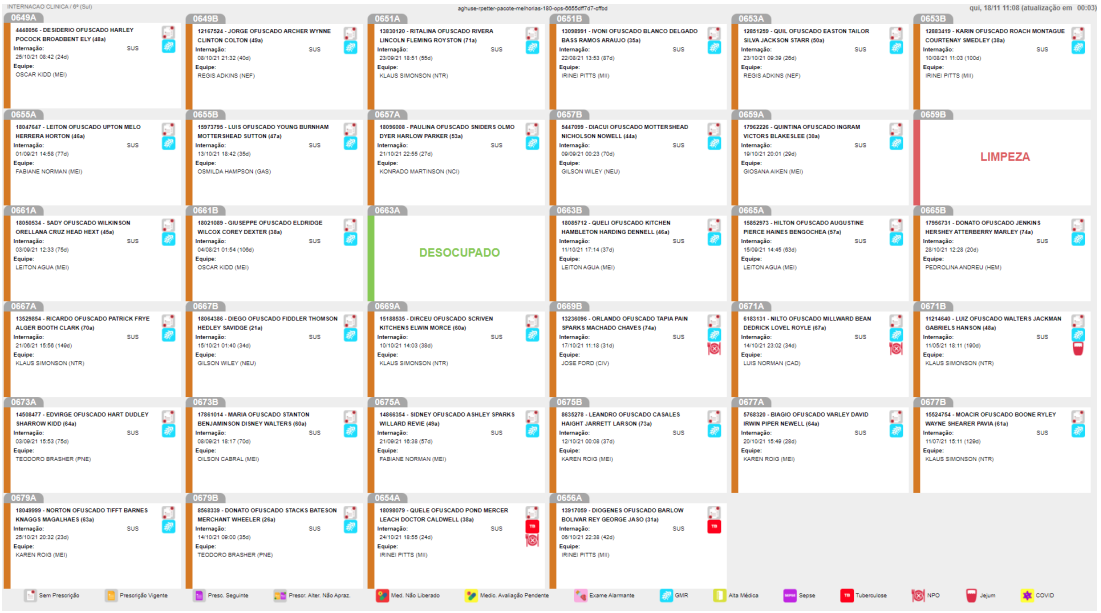
educação, resultados e visualização das imagens de exames, fluxograma e registro dos sinais vitais e balanço hídrico.

Painel de Pacientes

Painel de Pacientes

O Painel de Pacientes foi criado com o objetivo de informatizar os quadros de pacientes existentes nas unidades de internação constituídos de papéis coloridos, recados e registros à mão, com uso de mini computadores (Raspberry Pi) visando a otimização dos espaços nas unidades e também a redução de custo na aquisição dos equipamentos. O painel possibilita a visualização de leitos de uma unidade de internação específica, de um andar / ala com as diversas unidades vinculadas ou de unidades agrupadas, com as informações em tempo real do censo de pacientes, assim como, através de ícones, a visualização do status da prescrição, dos medicamentos que necessitam de parecer para aprovação ou com parecer

não liberado para administração, resultados de exames alarmantes, pacientes portadores de germes multirresistentes (GMR), sepse, tuberculose, covid, pacientes em NPO, jejum, com alta médica.



Troca de Senha

O Troca de Senha é uma aplicação web utilizando as mais modernas tecnologias de software com arquitetura de microsserviços com as funcionalidades correspondentes ao módulo de Segurança do AGHUse, possibilitando a atribuição e automatização de perfis de acesso e troca de senha.

Portal BASE - Informações Gerenciais

O Portal BASE foi criado para ser a interface visual padrão de acesso às informações gerenciais do hospital focada em agilizar a navegação entre menus, cubos e visões de forma fácil e interativa. O BASE possibilita o acesso unificado tanto para dashboards como interação com os cubos dinâmicos e é um sistema voltado para as lideranças do HCPA com o foco em visões de dados e informações gerenciais para a tomada de decisão, bem como acompanhamento de indicadores estratégicos.

5.1.2. Sistemas externos

Para atender a complexidade das necessidades de sistemas no HCPA, além do AGHUse são necessários diversos outros sistemas para atender principalmente demandas especialistas. Abaixo a relação dos principais sistemas externos contratados:

Sistema	Fornecedor
PACS (Sistema de Imagens Médicas)	AGFA Healthcare Brasil
Gestão de RH Starh Management Tools do HCPA	Datasys Sistemas em Informática SC Ltda
Hospedagem de resultados de exames na Internet	Deferrari Sistemas Informática Ltda
SA (Suite Strategic Advisor)	Interact Solutions
Liquid GED	Rede Imagem - Tecnol, Consul Sistemas Ltda
Sênior Ronda - ponto e acesso	Ruá Sistemas Automatizados Ltda.
SAPIENS - gestão empresarial	Sênior Sistemas S/A
Contas a Receber	SISPRO Software
Bionexo / Plannexo	Bionexo
RealBlood (Banco de Sangue)	TDSA Comércio de Software Ltda.
Interfaceamento de Exames	VFR Indústria Comércio e Serviços Sistemas
Epimed	Epimed Solutions
UpToDate / Lexicomp	Wolters Kluvers
Dispensário Eletrônico / Supply Station	Grifols Brasil Ltda
Qualitor - Plataforma de Service Desk	Qualitor Software e Serviços de Informática S/A
CME16	Hinno Technology
REDCap	Software Livre
Moodle	Software Livre
SAELE	Software Livre
SEI - Sistema Eletrônico de Informações	Software Livre

5.1.3. Apoio externo para o desenvolvimento de sistemas

Para fazer frente à grande demanda de desenvolvimento no sistema AGHUse, o HCPA conta com o apoio de uma fábrica de software externa, uma fábrica de qualidade e uma empresa para mensuração do desenvolvimento realizado em pontos de função conforme descritos na tabela abaixo:

Atividade	Fornecedor	Contrato	Data de assinatura	Vigência máxima
Fábrica de Software	CTIS Tecnologia S/A.	278231	07/02/2020	07/04/2025
Credenciamento		278311		
Fábrica de Qualidade	Deltapoint Consultoria e Treinamento	278321	03/02/2020	22/04/2025
Mensuração do desenvolvimento em Pontos de Função	TI Métricas Serviços LTDA.	112128	16/11/2018	20/11/2022

5.1.4. Posicionamento atual do desenvolvimento

As atividades de desenvolvimento realizadas no HCPA são mensuradas em macropontos (MP) que representam o macro dimensionamento de funcionalidades do sistema que podem ser percebidas pelo usuário, como por exemplo, uma nova tela com poucos campos e uma única tabela é mensurada com uma estória simples (1 MP). Estórias complexas com muitos cálculos e acesso a várias tabelas podem ser médias (3 MPs) ou complexas (5 MPs). Abaixo tabela com a definição do macro dimensionamento conforme tipo de tarefa e complexidade:

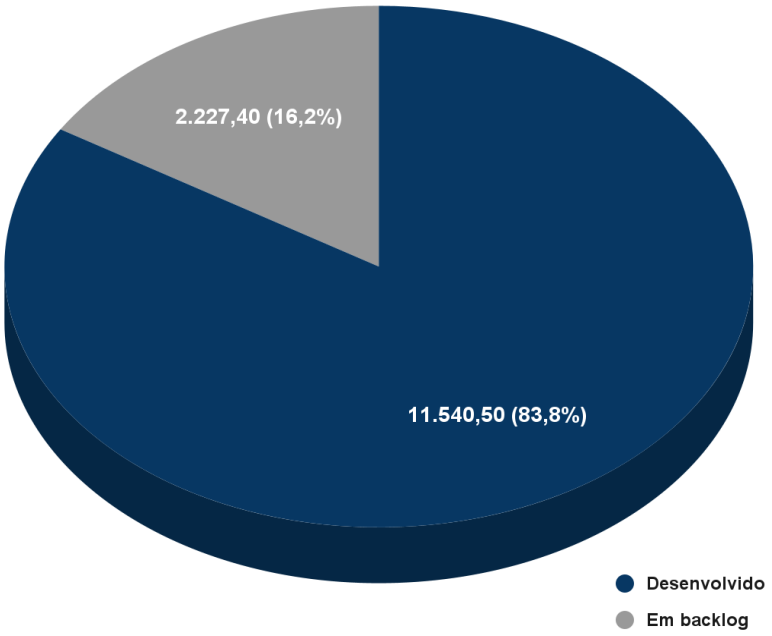
Tipo	Macro Dimensionamento (MPs)		
	Simples	Média	Complexa
Estória do Usuário	1	3	5
Melhoria	0,2	0,6	1

A tabela e o gráfico abaixo representam a situação atual do desenvolvimento, detalhando as funcionalidades do AGHUse já desenvolvidas e em backlog aguardando priorização:

Funcionalidade	Desenvolvido	Em backlog
Ambulatório	482,2	34,4
Anamnese e Evolução	486,6	0,4
Beira do Leito	187	75
Certificação Digital	14,8	0,8
Cirurgias	190	45,6
Comissões e Avaliadores	87,6	5,2
Compras	557,2	46,4
Contabilidade	105,8	44,4
Contas a Pagar	58,6	9,2
Contas a Receber	2	1,8
Controle de Infecção	219	17
Controles do Paciente	32,6	22,2
Custos	533,4	60,8
Emergência	397	13,4
Engenharia	116,6	3,8
Escalas de Enfermagem	97,6	40,8
Escalas Profissionais	102,8	0
Estoque	753,6	106,6

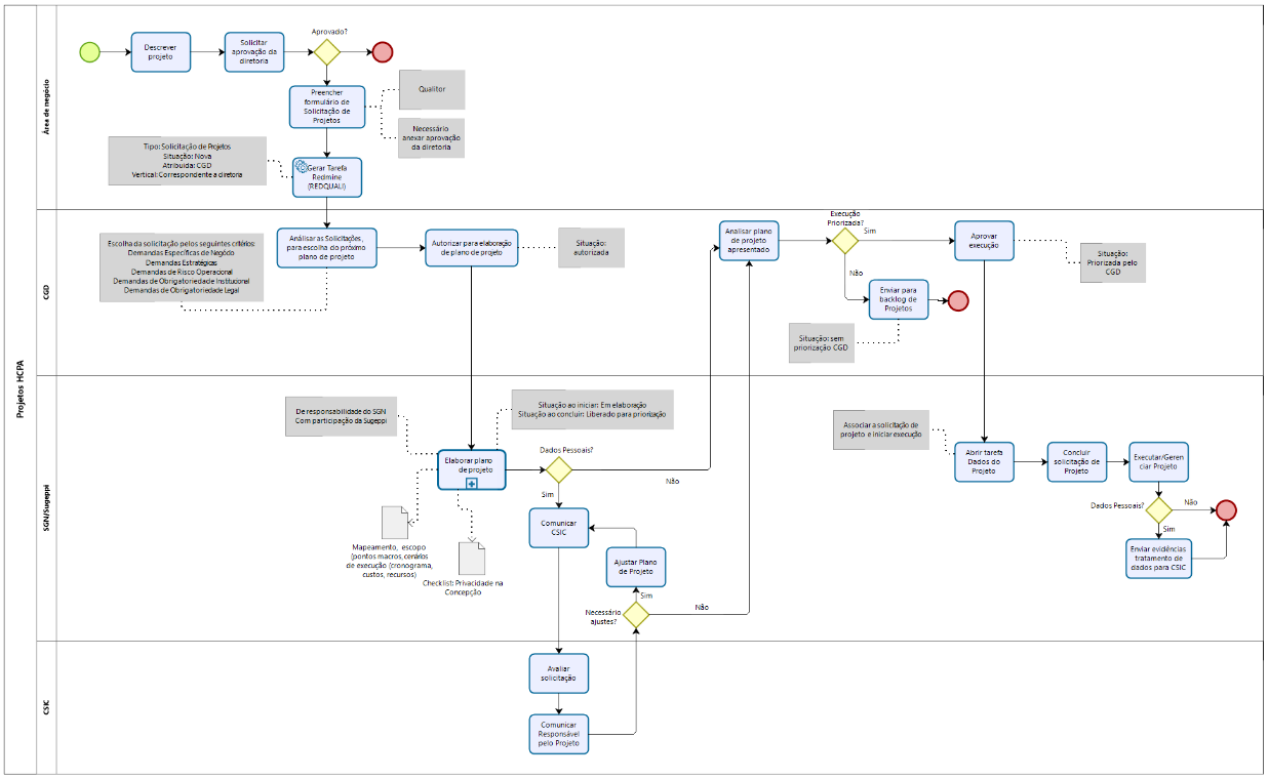
Exames	632,6	48
Farmácia	211,2	138,6
Faturamento Ambulatório	223,6	81,2
Faturamento Convênios	525,2	50,6
Faturamento Internação SUS	253,2	153
Financeiro	101,8	6,2
Geral	260,6	101,2
Informações ao Público	25,4	1
Internação	236	57,8
Investimentos	87,8	18,8
Meu Clínicas	161,5	8,8
Nutrição	293,6	9,8
Ordens de Manutenção	103,2	0
Orçamento	233,6	198,8
Pacientes	108,8	6,2
Patrimônio	458	309
Perinatologia	298	7,6
Plano de Contingência		110
Prescrição Médica	792,2	111,6
Prescrição de Enfermagem	116,4	19,4
Projetos de Pesquisa	432,8	48,2
Prontuário OnLine	75,6	8,4
Registro do Colaborador	56,4	4
Segurança	144	31,8
Sessões Terapêuticas	1004	164,8
Transplantes	280,6	4,8
Total	**11.540,5**	**2.227,4**

Situação atual em Macropontos



5.1.5. Processo de priorização e gestão de demandas de sistemas

No HCPA, tendo em vista seu tamanho e complexidade, é grande a busca pela otimização dos processos de trabalho à procura de maior agilidade, praticidade e eficiência, o que vem exigindo cada vez um maior envolvimento da TIC. A quantidade de solicitações por melhorias e novas funcionalidades do sistema AGHUse, além de outros serviços, afeta significativamente o fluxo de demandas de TIC, tornando a seleção e priorização extremamente importantes para que a qualidade dos serviços prestados às áreas de negócio seja mantida. O Comitê de Governança Digital (CGD) elaborou um processo de priorização e gestão de demandas de TIC considerando critérios de classificação e priorização claros, como tempo de esforço, custo envolvido, relação com metas estratégicas e quantidade de recursos críticos, cujo mapeamento encontra-se abaixo:



Como se pode observar, o mapeamento descreve o passo a passo do processo de priorização e gestão de demandas de TIC conforme detalhamento abaixo:

Projeto: Para solicitar um projeto de TIC, a área de negócios precisa anexar a autorização da Diretoria da vertical de negócios atendida, bem como documentar e detalhar o pedido.

Destaque da solicitação de projeto pela Diretoria: os representantes de cada diretoria sinalizam ao CGD as solicitações mais importantes/estratégicas para subsidiar o processo de priorização.

Autorização para detalhamento pelo CGD: o CGD avalia a necessidade e viabilidade da solicitação de projeto e encaminha para detalhamento, denominada Plano de Projeto.

Elaboração do Plano do projeto pelo Chefe de Seção: a solicitação de projeto, após autorização pelo CGD é encaminhada para o Serviço de Gestão de Negócio quando trata-se de projeto de Negócio ou para o Serviço de Gestão de Tecnologia quando trata-se de projeto de Tecnologia, para que o Chefe de Seção correspondente, juntamente com a SuGePPI possa realizar o Plano de Projeto com a definição do escopo, alocação dos recursos necessários e tempo previsto para execução do projeto. Após a elaboração do Plano de Projeto, é novamente encaminhado para o CGD que deliberará por sua priorização ou aguardo de recursos para desenvolvimento.

Priorização CGD: o CGD recebe o Plano de Projeto e define dentro da disponibilidade de recursos para desenvolvimento se o projeto deve ser priorizado. Caso o projeto não seja priorizado, permanece no backlog de projetos (portfólio) para priorização em momento posterior.

Para projetos priorizados, caso definida alocação de time dedicado ou de infraestrutura, a execução do projeto deve ser realizada com o acompanhamento e gestão do projeto (integral ou parcial), conforme planejamento aprovado até o encerramento do projeto.

A priorização dos projetos leva em conta as definições abaixo, sendo que a de maior valor corresponde à mais crítica e prioritária:

1. **Demandas Específicas de Negócio:** demandas solicitadas pelas áreas de negócios;
2. **Demandas Estratégicas:** demandas identificadas como estratégicas para o HCPA;
3. **Demandas de Risco Operacional:** demandas que representem impacto nas atividades do HCPA;

4. **Demandas de Obrigatoriedade Institucional:** demandas de auditoria, regulação ou solicitadas pela Diretoria Executiva (DE) do HCPA com data prevista de entrega;
5. **Demandas de Obrigatoriedade Legal:** demandas com data prevista de entrega em função de obrigatoriedades para cumprimento legal.

Solicitação pela área de negócio de demandas de incidentes, melhorias ou serviços:

É feita pelo Portal de Chamados de TIC ou através de ligações telefônicas (pelo ramal 8565 na opção 1 – atendimento aos sistemas corporativos). Ao receber esse chamado, é feita a triagem pela Central de Relacionamento CGTIC (primeiro nível de atendimento). Nessa triagem para cada solicitação são seguidos os seguintes procedimentos:

Incidente: entrar em contato com o solicitante para:

- Incluir evidências: vídeo ou captura da tela com o erro relatado;
- Capturar e anexar ao chamado o log de erro, incluindo o número do ticket na descrição;
- Revisar e categorizar o chamado conforme o tipo de serviço;
- Revisar e categorizar o chamado conforme a prioridade;
- Direcionar a solicitação para a equipe correta em segundo nível de atendimento;
  Se erro de ticket para Desenvolvimento, senão para o segundo nível de atendimento.

Melhoria:

- Verificar se o usuário que abriu a melhoria tem permissão para tal (Chefias de Serviço, Coordenadores e Assessores);

- Ler e entender a solicitação, se não estiver clara, entrar em contato com o solicitante e solicitar mais detalhes;
- Revisar e categorizar o chamado conforme o tipo de serviço;
- Revisar e categorizar o chamado conforme a prioridade;
- Direcionar a solicitação para a equipe correta em segundo nível de atendimento.

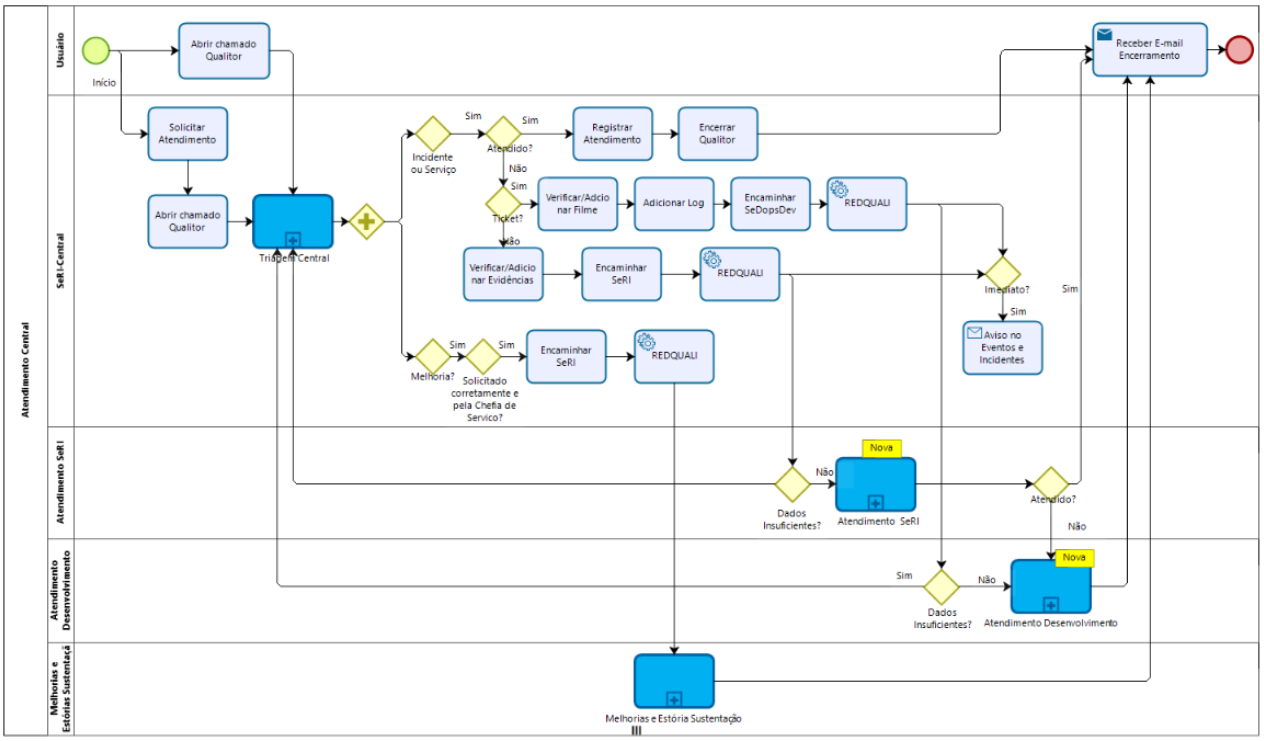
Serviço:

- Ler e entender a solicitação, se não estiver clara, entrar em contato com o solicitante e solicitar mais detalhes;
- Revisar e categorizar o chamado conforme o tipo de serviço;
- Revisar e categorizar o chamado conforme a prioridade;
- Direcionar a solicitação para a equipe correta em segundo nível de atendimento.

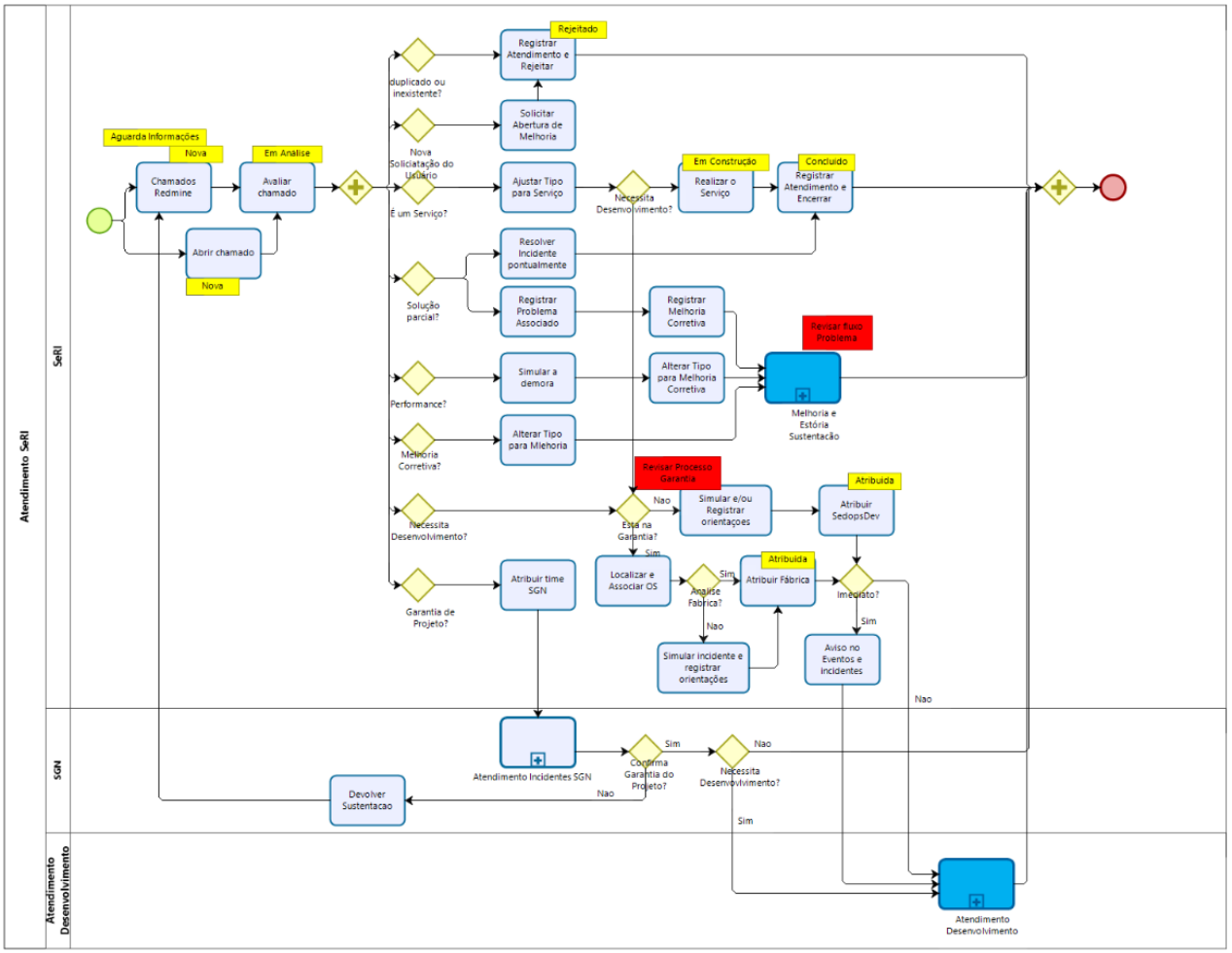
A priorização de **incidentes** e **serviços** deve considerar a definição abaixo onde a de maior valor corresponde à mais crítica e prioritária:

1. **Normal:** demandas necessárias somente em uma situação ou funcionalidade específica do sistema;
2. **Alta:** demandas específicas com pouco impacto no uso do sistema;
3. **Imediata:** demandas impeditivas para o funcionamento de um processo crítico de negócio ou do sistema como um todo.

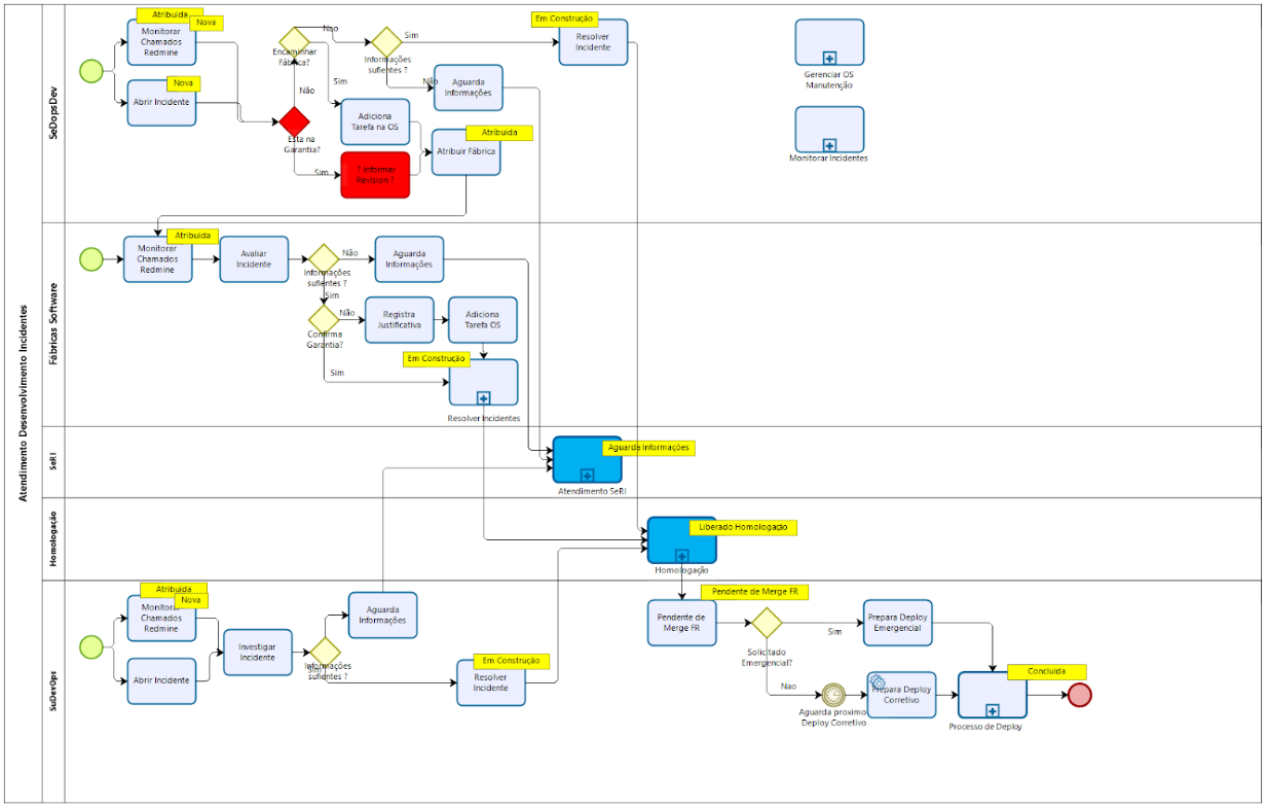
A imagem abaixo representa o fluxo do primeiro nível de atendimento(N1):



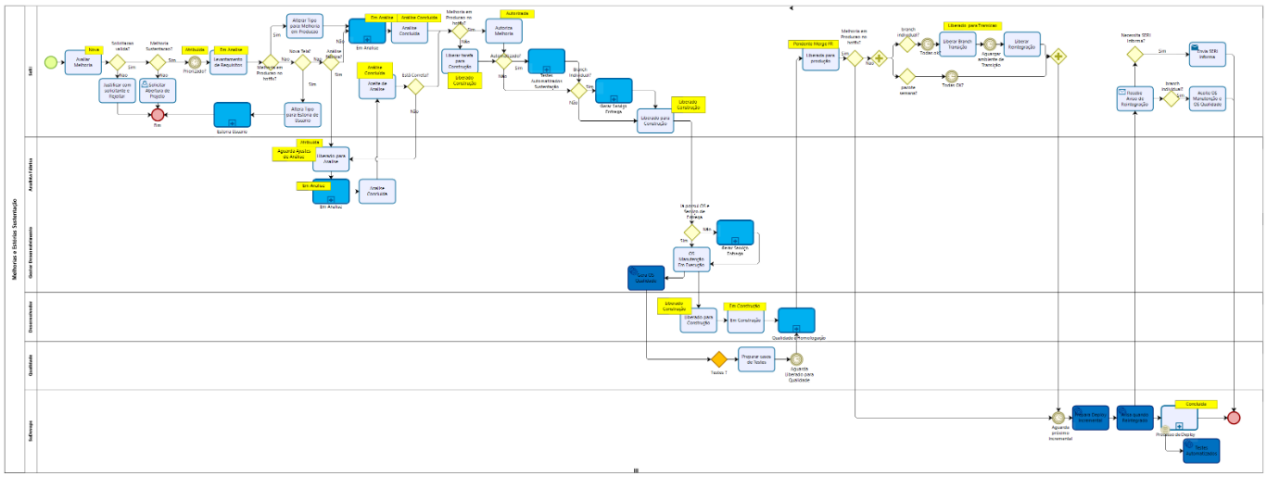
A imagem abaixo representa o fluxo do segundo nível de atendimento (N2):



A imagem abaixo representa o fluxo do atendimento de incidentes:



A imagem abaixo representa o fluxo do atendimento de melhorias na sustentação:



5.2. INFRAESTRUTURA

5.2.1. Centro Integrado de Tecnologia da Informação (CITI)

Implantação do prédio do Centro Integrado de Tecnologia da Informação (CITI), onde será instalado datacenter unificando e qualificando as infraestruturas de Tecnologia da Informação e Comunicação (TIC) do HCPA e da Universidade Federal do Rio Grande do Sul (UFRGS), otimizando o uso de recursos públicos, garantindo segurança da informação e alta disponibilidade com a qualificação nos serviços prestados à comunidade.

Realizado edital de concessão onerosa de uso parcial do datacenter no primeiro semestre de 2022 com empresa vencedora em processo de homologação.

O CITI possuirá o seguinte escopo / abrangência:

- HCPA
    - Biobanco
    - Coordenadoria de Gestão de Tecnologia da Informação e Comunicação (CGTIC)
    - Núcleo de Inovação e Transferência de Tecnologia (NITT)
- UFRGS
    - Centro de Processamento de Dados (CPD)
        - Ponto de Presença (PoP-RS)
    - Centro Nacional de Supercomputação (CESUP)
    - Ponto de Troca de Tráfego (PTT) de Internet Região Sul - IX.br
- Datacenter Parceiro Privado

6. IDENTIFICAÇÃO DAS NECESSIDADES ATUAIS

Durante as atividades de diagnóstico do ambiente de TIC, foram identificadas as necessidades de projetos, conforme seguem:

6.1. Necessidades de Desenvolvimento de Sistemas

Tarefa	Descrição
Administrativos	
87473	Órtese e Prótese - desenvolver a gestão das solicitações de materiais consignados ao fornecedor
87530	Supply Chain - Portal do Fornecedor
91683	Disponibilizar versão mobile (tablet ou celular) com a Requisição de Materiais do AGHUse
92219	Alterar o sumário de alta para Informar ao paciente o uso de dispositivos implantáveis (Órteses)
98637	Migração Faturamento Ambulatorial SUS
99947	Nova portaria para apac de otorrino - implantação habilitação 03.05 - atenção especializada às pessoas com deficiência auditiva
103058	Aba aguardando atualização automática AGHUse na sala de estar médico do CO
105507	Integração dos exames de cardiotocografia ao prontuário
122318	[BI] Indicador Experiência do Paciente (atual Pesquisa de Satisfação do Paciente Internado)
123931	Dispensação de MMh por prescrição
124590	[BI] - Cubo Nutrição: Assistencial, Estatística e Níveis Assistenciais (novo cubo)
130583	[Migração] Módulo de Segurança do AGHWeb para o AGHUse - Fase 5 (Unificar módulo de segurança e refatorar AGHUse)
131327	[BI] Criação de novos cubos - Indicadores de planejamento de suprimento

133672	[Migração] Faturamento Convênios - Migração regras de banco de dados
137242	Projeto - Atualização do Sistema dos Dispensários Eletrônicos
143093	[BI] Projeto BASE - Dashboard Internação
144020	Projeto - Redimensionamento da movimentação de Empréstimos
144774	Projeto - Terceirização da Digitalização de Prontuários X Adequação a nova legislação
145974	Projeto - Projeto de melhoria Kardex® E Pyxis®
149498	Projeto - Integração AGHUse - GERCON
149626	Integração do AGHUse com o Sistema e-SUS AB
149634	Solicitação de botão de notificação na tela de Gestão de Interconsulta
149642	Incluir campo Turno na tela Grades de agendamento
150994	Projeto - Registro assistencial e faturamento de doenças raras
151321	[BI] Projeto BASE - Produção de cirurgias por profissional
152104	Projeto - Registros de dados prescrição dietética
153379	Projeto - Integração Supply RFID
156609	[BI] Reorganização das UFs do Centro de Tratamento Intensivo e Emergência
170968	Projeto - Infraestrutura para adequação do Sistema de Contas a Receber
174848	Projeto - Inteligência Artificial para Farmácia Clínica
176140	Projeto - UPGRADE PACS: Modernização da Solução de Imagens Médicas para o HCPA - Infraestrutura
	Assistenciais
87572	[Migração] Sistema de Contingência - Tecnologia e Infraestrutura
87581	Prescrição de enfermagem do paciente ambulatorial
88982	Relatório de preenchimento Folha de Parada Pediátrica
110789	[BI] Integração GEO da Pesquisa de Satisfação de Usuários - Internação

114902	Projeto de melhorias para o sistema manchester de classificação de risco no serviço de emergência
120319	[Sessões terapêuticas] Implantação / Estabilização integração prescrição - dispensação medicamentos
127962	Projeto de informatização para melhorias na identificação da sepse e manejo precoce
132591	[BI] BASE (cubo novo): CCIH - dias de dispositivos invasivos entre infecções
137473	Projeto - Aprazamento e Checagem de Dieta
149570	Projeto - Relatório de fim de radioterapia
150525	Projeto - Listas de espera pacientes - Gestão dos Leitos
152666	Prescrição de Solução Padrão
153416	Projeto - Identificação pacientes UBS Santa Cecília no AGHUse
155701	Projeto - Registro e auditoria de acessos à informações de pacientes
158318	[BI] Criar CUBO para Escala DINI
163907	[BI] Projeto BASE - Cubo escala Martins
163908	[BI] Projeto BASE - CUBO escala SiCAD
168268	Projeto - Integração Banco de Sangue - HIMSS
171476	Projeto - Melhorias no AGHUse para solicitação e coleta de sangue para dosagem de nível sérico de drogas terapêuticas
Presidência	
142447	Gerenciador de escalas
166114	Projeto - Gestão do Núcleo de Inovação e Transferência de Tecnologia
Relacionamento	
102452	Revisão dos cadastros do AGHUse
121657	Migração do Sistema Operacional das estações do HCPA para Windows 10
Tecnologia	
114366	Sistema de monitoramento de EEG para pacientes com risco de crises convulsivas

117131	Ajustes na Gestão de Permissões e Perfils do AGHUse / Segurança para funcionamento na Comunidade AGHUse
131355	Melhoria Rede sem fio wi-fi médica corporativa
151293	Projeto - Reparo do servidor da Unidade de Fisiologia Pulmonar (UFP)

6.2. Necessidades de aporte de recursos em Infraestrutura de TIC

A Coordenadoria de Gestão de Tecnologia da Informação e Comunicação (CGTIC) está representada na Comissão de Investimentos do HCPA por seu coordenador, visando encaminhar as demandas de infraestrutura e atualização tecnológica de TIC, assim como, garantir a interface e impactos gerados por solicitações de investimentos de outras áreas.

A tabela abaixo apresenta as necessidades atuais de investimentos de recursos em infraestrutura de TIC:

Item	Valor estimado	Detalhamento da necessidade
Modernização da Rede Wi-Fi	**R$ 808.800,00**	Maior área de cobertura (3X), maior velocidade de comunicação na rede (8X), estabilidade, confiabilidade e segurança do tráfego e satisfação dos usuários.
Atualização da Rede	**R$ 1.159.320,00**	Manutenção e reposição dos Switches do HCPA. Aumento de velocidade com a comunicação com a internet (10X)
Storage All Flash (armazenamento)	**R$ 4.000.000,00**	Aquisição de novo equipamento de storage em substituição aos contratos de manutenção dos equipamentos antigos já obsoletos. Maior segurança e performance dos sistemas corporativos.
Oracle GEN2	**R$ 359.872,14**	Atualização tecnológica do ambiente de Produção e DR
Computadores com monitor	**R$ 1.704.000,00**	Atualização do parque de equipamentos e atendimento a necessidades de expansão
Notebooks	**R$ 202.240,00**	Projeto Beira-Leito

Servidores Blade / Computação Hiperconvergente	**R$ 1.258.800,00**	Atualização de equipamentos do datacenter (servidores) adequando o poder computacional para rodar as aplicações, com velocidade e segurança.
Microcomputador tipo Mini-PC	**R$ 429.000,00**	Reposição do parque do hospital em manutenção
Microcomputador CPU (sem monitor) para aplicações especiais	**R$ 125.840,00**	Substituição de estações de trabalho dos desenvolvedores, para ganhar produtividade na programação do AGHUse
Monitor padrão HCPA	**R$ 96.600,00**	Reposição do parque do hospital em caso de manutenção/desfazimento de monitor avariado

6.3. Projetos em andamento, priorizados pelo Comitê de Governança Digital

Conforme demonstrado no capítulo 5, a priorização dos projetos é realizada pelo Comitê de Governança Digital, seguindo processo previamente definido.

A tabela abaixo apresenta os projetos priorizados e em andamento, com seu respectivo dimensionamento em macropontos e as datas de início e conclusão previstas:

Projeto	Macropontos Aprovados	Início	Fim Previsto
Administrativos			
Empenhos Fase 2: Geração/envio (origem movimentos e inclusão manual)	45	14/02/2022	24/08/2022
Migração etiquetas para o padrão Datamatrix /GS1	41,1	17/01/2022	15/07/2022
Ateste de NF´s	42,2	14/04/2022	18/11/2022
GERPAC - Terapia Renal Substitutiva	44,6	30/05/2022	12/01/2023
Assistenciais			
Beira do Leito - Checagem Dose Unitária Fase 2	37,8	03/03/2022	15/09/2022

Descrição de Procedimentos à Beira Leito	44,7	02/05/2022	09/12/2022
Sessões Terapêuticas - Quimioterapia Internação	40,0	23/05/2022	06/01/2023
Escores Assistenciais	43,3	23/05/2022	27/01/2023
Tecnologia			
Atualização do Backend do BI	58,0	01/11/2021	25/03/2022
Projetos de Melhoria			
Origem dos medicamentos/ Contabilizar custo	10,6	25/10/2021	24/06/2022
Banco de sangue - integração Realblood com exames AGHUse	10,6	09/05/2022	23/09/2022
Sistema de Contingência - Arquitetura e Infra	37,0	27/06/2022	14/01/2023

7. SEGURANÇA DAS INFORMAÇÕES E INSTALAÇÕES

A criticidade do negócio e a sensibilidade das informações presentes na infraestrutura e nos bancos de dados corporativos do HCPA exigem processos e procedimentos avançados de segurança das informações e instalações. Abaixo estão apresentados alguns dos principais itens de segurança adotados pelo HCPA.

- **Política de Segurança da Informação e Comunicações:** A Política de Segurança da Informação e Comunicações está formalizada e publicada no repositório de documentos institucionais sob número POL-0061 e possui como integrantes os documentos: Plano de Segurança da Informação (PLA-0139), Plano de Segurança da Tecnologia da Informação e Comunicações (PLA-0140), Plano de Segurança Cibernética (PLA-0141), respectivamente (anexos 3 a 6).
- **Confidencialidade dos dados:** o HCPA possui uma sistemática de gestão de perfis de acesso aos sistemas corporativos e de terceiros.

- **Comissão de Segurança da Informação e Comunicações (CSIC):** Instituída oficialmente no HCPA em 30/11/2017 através do Ato 322/2017.

- **Renovação periódica de senhas:** em alinhamento com as boas práticas de segurança da informação, a cada 6 meses, é obrigatória a renovação da senha do usuário. A cada troca de senha, são apresentadas as normas de segurança, exigindo que os usuários dêem o aceite eletrônico para prosseguimento da troca de senha e reativação dos acessos.

- **Termos de responsabilidade / confidencialidade:** Em casos específicos são assinados termos de responsabilidade/confidencialidade, como por exemplo: na criação de usuários administradores da rede, que executam tarefas com maiores privilégios, é emitido um termo específico. Quando da não existência de norma de confidencialidade de dados na licitação/contratação de softwares de terceiros, é emitido termo específico para disponibilização de acessos à infraestrutura.

- **Criação de usuários / contas de acesso:** A criação é feita pela Coordenadoria de Gestão de Pessoas e pela Central de Identificação, como parte do processo de admissão do funcionário ou início de contrato de prestação de serviços. As contas de usuários para administração de serviços são criadas exclusivamente pela CGTIC. A inativação de uma conta de usuário (no banco de dados e no AD) acontece de forma automatizada quando do término do vínculo do colaborador com o HCPA. Caso haja seguidas (10) tentativas de acesso às aplicações com senha errada, ocorre o bloqueio da conta do usuário (no AD e no banco de dados).

- **Controles de acesso à rede e bancos de dados:** Tentativas de acesso não autorizado por usuários/equipamentos/aplicativos são controlados por um mecanismos de Intrusion Prevention System (IPS), Firewalls, Web Filtering e Appliances de VPN. Quando da tentativa de acesso não autorizado, os administradores recebem notificações para atuarem no problema. Usuários com contas bloqueadas/expiradas ou com dificuldade de acesso fazem contato com a Central de Relacionamento AGHUse através da abertura prévia de chamado ou por

contato telefônico. São mantidos logs detalhados com informações de acessos à rede, servidores, aplicativos, bancos de dados etc. Existem também tabelas *de auditoria* que guardam histórico de interações dos usuários nas principais tabelas negociais do sistema AGHUse.

- **Acessos à Internet:** São controlados através de solução integrada ao *Firewall* que contém categorização de destinos proibidos. Caso o usuário tente fazer acesso a algum conteúdo proibido, é apresentada mensagem de bloqueio e é armazenado o registro da tentativa indevida.

- **Controle de acesso físico:** O acesso aos ambientes de servidores (datacenter) é controlado por vários itens de segurança, tais como: monitoramento por vídeo, barreira humana (profissional operador de datacenter em regime 24 x 7 x 365) e sistema de controle de acesso.

- **Sala Cofre:** Os equipamentos centrais (servidores principais, ativos *core* de rede, storages etc.) estão alocados no datacenter em uma Sala Cofre Certificada, protegida contra arrombamentos, fogo, água, projéteis etc.

- **Procedimento Operacional Padrão de Salvaguarda e Recuperação de Informações:** Tem por objetivo definir os procedimentos necessários para a execução de backup (salvaguarda e recuperação) de informações custodiadas pela CGTIC.

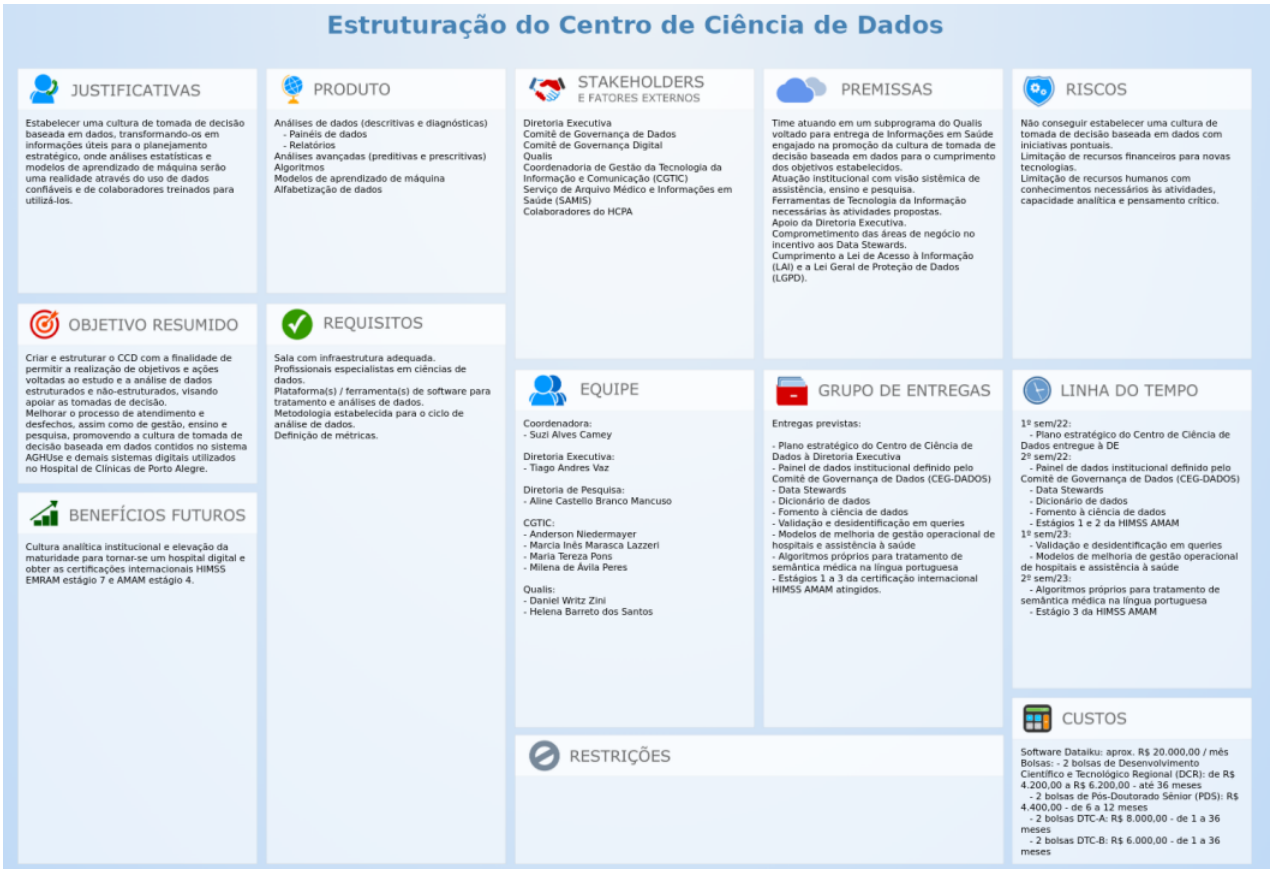
- **Plano de Continuidade dos Serviços de TIC:** Descreve recursos, acordos, critérios e responsabilidades ao restabelecimento dos serviços de tecnologia da informação e comunicações em situações críticas, assegurando a continuidade dos serviços de TIC prestados. Está formalizado e publicado no repositório de documentos institucionais sob número PLA-0481 (anexo 7).

- **Plano Institucional de Gerenciamento de Sistema de Comunicação e Dados:** Estabelece o conjunto de procedimentos de gestão, planejados e implementados a partir de bases técnicas, normativas e legais, abrangendo cada etapa do gerenciamento dos sistemas de Comunicação e Dados do HCPA sob

responsabilidade da CGTIC. Está formalizado e publicado no repositório de documentos institucionais sob número PLA-0737 (anexo 8).

8. ANEXOS

8.1. ANEXO 1 – CANVAS DE ESTRUTURAÇÃO DO CENTRO DE CIÊNCIAS DE DADOS



8.2. ANEXO 2 - MATRIZ DE RISCOS DE TIC

A Matriz de Riscos de TIC é uma ferramenta de gerenciamento de riscos que permite de forma visual identificar quais são os riscos que devem receber mais atenção. Consiste em uma matriz orientada por duas dimensões: probabilidade e impacto. Por meio dessas duas dimensões, é possível calcular e visualizar o nível de risco, que consiste na avaliação do impacto versus a probabilidade.

Probabilidade de ocorrência do evento relacionado ao risco:

Probabilidade	Descrição
Improvável	Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
Rara	De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
Possível	De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
Provável	De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
Praticamente certa	De forma inequívoca, o evento ocorrerá, às circunstâncias indicam claramente essa possibilidade.

Impacto na atividade e/ou volume financeiro envolvido ao risco:

Impacto	Descrição
Mínimo	Causa morosidade no processo e/ou envolve valores de até R$ 200.000,00.
Mínimo / Médio	Fragiliza as informações geradas e/ou envolve valores entre R$ 200.000,01 e R$ 300.000,00.
Médio	Causa morosidade no processo e fragiliza as informações geradas e/ou envolve valores entre R$ 300.000,01 e R$ 400.000,00.

Médio / Alto	Resulta na interrupção parcial do fornecimento dos serviços do setor / entidade e/ou envolvem valores entre R$ 400.000,01 a R$ 500.000,00.
Alto	Resulta na interrupção total do fornecimento dos serviços do setor / entidade e/ou envolve valores acima de R$ 500.000,00.

Critérios para aceite de riscos:

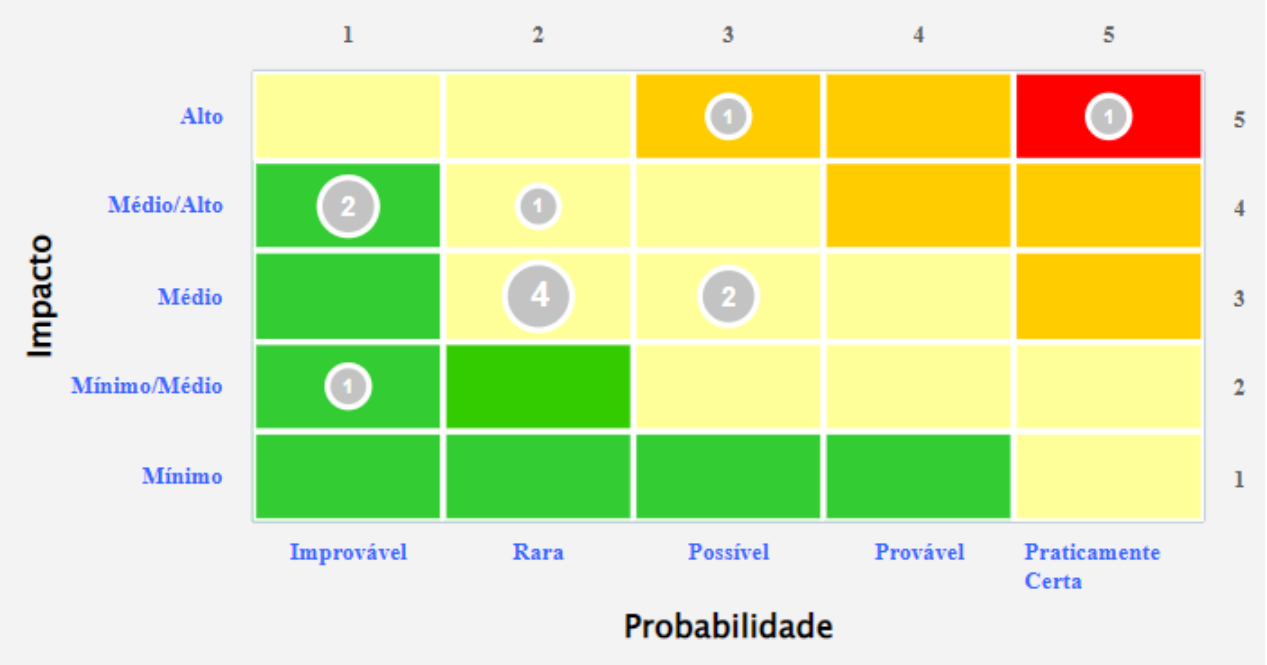
Nível de Risco	Valor Inicial	Valor Final	Ação
Muito Baixo	0,01	1,99	Aceitar
Baixo	2,00	3,99	Aceitar
Médio	4,00	9,99	Mitigar
Alto	10,00	19,99	Mitigar
Muito Alto	20,00	25,00	Mitigar

Tabela de riscos:

Código	Risco	Nível de Risco	Probabilidade	Impacto
R.01	Comprometimento da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade)	Muito Alto (25)	Praticamente Certa	Alto
R.02	Indisponibilidade de recursos orçamentários para aplicação em TIC	Alto (15)	Possível	Alto
R.03	Entrega de um Serviço de TIC que gere impacto negativo ao negócio	Médio (9)	Possível	Médio
R.04	Obsolescência intelectual em TIC	Médio (9)	Possível	Médio
R.05	Indisponibilidades dos sistemas de rede	Médio (8)	Rara	Médio / Alto

R.06	Descumprimento das demandas de regulamentação de TIC (Compliance)	Médio (6)	Rara	Médio
R.07	Indisponibilidade dos sistemas corporativos	Médio (6)	Rara	Médio
R.08	Obsolescência do parque tecnológico de TIC	Médio (6)	Rara	Médio
R.09	Obsolescência dos sistemas corporativos	Médio (6)	Rara	Médio
R.10	Impacto à imagem do HCPA pela uso inadequado do AGHUse pela comunidade AGHUse	Médio (4)	Improvável	Médio / Alto
R.11	Indisponibilidade do datacenter central do HCPA	Médio (4)	Improvável	Médio / Alto
R.12	Interrupção de serviços críticos de TIC providos por terceiros	Baixo (2)	Improvável	Mínimo / Médio

Matriz de riscos:



8.3. ANEXO 3 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – POL-0061

HOSPITAL DE CLÍNICAS PORTO ALEGRE RS	**Política de Segurança da Informação e Comunicações**	Página 1/2
		POL-0061

Definição

O Hospital de Clínicas de Porto Alegre (HCPA) desenvolve ações sistemáticas para viabilizar e assegurar a disponibilidade, integridade, confidencialidade, legalidade e autenticidade das informações produzidas ou custodiadas pela instituição, a fim de garantir a continuidade do negócio, minimizar os riscos e maximizar a efetividade da missão institucional.

Tais ações perpassam a elaboração, manuseio, disponibilização, armazenamento, transporte e descarte de informações. Sua execução é regida por planos específicos nas áreas de segurança da informação, segurança da tecnologia da informação e comunicações e segurança cibernética, os quais são analisados criticamente em intervalos planejados.

Os procedimentos de segurança previstos devem ser observados pelas comunidades interna (dirigentes, conselheiros, lideranças, funcionários, professores, pesquisadores, residentes, alunos, estagiários, prestadores de serviços e jovens aprendizes) e externa (pacientes, acompanhantes, fornecedores, visitantes e outros públicos relacionados com a instituição).

Elaborado por: **Diretoria Executiva**

8.4. ANEXO 4 - PLANO DE SEGURANÇA DA INFORMAÇÃO - PLA-0139

HOSPITAL DE CLÍNICAS PORTO ALEGRE RS	Plano de Segurança da Informação	Página 1/5
		PLA-0139

Definição

Este plano estabelece normas gerais e específicas de proteção das informações, independente do formato (físico ou digital), produzidas e/ou custodiadas pelo Hospital de Clínicas de Porto Alegre (HCPA), abrangendo pessoas e processos de negócio.

Objetivos

Definir normas e instrumentos de controle para assegurar a salvaguarda dos ativos de informação e dos recursos de processamento da informação, a fim de garantir o nível adequado de proteção, conforme os requisitos estabelecidos na gestão de riscos, bem como as obrigações legais, regulamentares, contratuais ou de requisitos do negócio relacionadas à Segurança da Informação.

Indicação

Este plano é aplicável a toda instituição, ou seja, abrange a comunidade interna (grupo formado por professores, pesquisadores, funcionários, estudantes, residentes, estagiários e jovens aprendizes) e externa (pacientes, acompanhantes, fornecedores, visitantes e órgãos reguladores) e está condicionado ao ciclo de vida dos ativos e recursos de processamento da informação.

Instruções específicas

Definem-se:

- Ativos de Informação: meios de armazenamento, transmissão e processamento de informações, locais onde se encontram estes meios, sistemas de informação, pessoas que a eles têm acesso, imagem institucional, serviços e tudo aquilo que tem valor para o HCPA e que esteja relacionado com informação e comunicações.
- Incidentes de Segurança da Informação: qualquer evento que tenha probabilidade de comprometer as operações do negócio.

A aplicação deste plano pressupõe o desdobramento de ações com os seguintes objetivos:

1. Assegurar que a comunidade interna e externa estejam conscientes, entendam e cumpram as suas responsabilidades e estejam em conformidade com seus

respectivos papéis.

2. Proteger os interesses da instituição como parte do processo de mudança de atribuições ou encerramento de vínculo com a instituição.
3. Gerenciar a implementação e operação da Segurança da Informação na instituição.
4. Assegurar que a informação receba adequada proteção, sendo classificada de acordo com o seu nível de sigilo e a sua importância para a instituição.
5. Estabelecer diretrizes de controle de acesso à informação e aos recursos de processamento da informação.
6. Prevenir o acesso físico não autorizado aos recursos de processamento das informações, danos e furtos, evitando o comprometimento de ativos e a interrupção dos processos de negócio da instituição.
7. Estabelecer e gerenciar um nível acordado de segurança da informação e de entrega de serviços baseados em acordos com os fornecedores, prestadores de serviços e parceiros.
8. Gerenciar os incidentes de segurança da informação.
9. Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança institucional.
10. Promover anualmente a análise crítica da implementação e operação deste Plano.

Competências e Fluxos

1. Cabe aos gestores do HCPA: conscientizar colaboradores sob sua supervisão em relação aos conceitos, às práticas e à cultura em segurança da informação; incorporar aos processos de trabalho da área práticas inerentes à segurança da informação; tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação, estabelecendo a devida comunicação.
2. Cabe a todos os integrantes das comunidades interna e externa do HCPA zelar

pelas informações e recursos aos quais têm acesso; observar princípios éticos e direitos autorais; comunicar atitudes ou situações suspeitas; observar normas e procedimentos internos a fim de assegurar que requisitos estatutários, legais e contratuais sejam atendidos.

3. Cabe à Comissão de Segurança da Informação e Comunicações as seguintes atribuições:

   a) definir a estratégia de segurança e garantir alinhamento estratégico;

   b) assessorar e promover a implementação das ações de segurança da informação e comunicações no HCPA;

   c) propor a constituição de grupos de trabalho para tratar de temas e soluções específicas sobre segurança da informação e comunicações;

   d) manter a atualização da Política de Segurança da Informação e Comunicações (POSIC) conforme mudanças nos processos institucionais e garantir conformidade com as disposições constitucionais, legais e regimentais vigentes;

   e) aprovar e acompanhar planos de ação e procedimentos operacionais padrão para aplicação da POSIC, avaliando os resultados e propondo melhorias;

   f) promover a cultura em segurança da informação e comunicações;

   g) solicitar apuração quando da suspeita de ocorrências de transgressão da POSIC;

   h) esclarecer eventuais dúvidas e deliberar sobre assuntos relativos à POSIC.

4. Cabe à chefia imediata tratar a omissão ou conivência que implique desobediência ou inobservância das disposições deste Plano, após devidamente apuradas e se comprovadas, providenciando, conforme o caso e de acordo com o Regulamento da Instituição, advertência, suspensão, demissão sem ou por justa causa e/ou comunicação às autoridades competentes.

Registro

A melhoria contínua deste Plano ocorre de forma sistemática com base nos registros de auditorias, incidentes de segurança da informação, retorno dos usuários e análise da eficácia dos controles.

A eficácia deste Plano será avaliada através de apontamentos de eventos não contemplados pelo mesmo.

Referências

O gerenciamento de Segurança da Informação segue os preceitos estabelecidos na Norma ABNT NBR ISO/IEC 27001 (Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos) e na Norma complementar 03/IN01/DSIC/GSIPR (Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal).

Elaborado por: **Grupo de Trabalho Atualização das Diretrizes Relacionadas à Segurança da Informação e Comunicações - Ato 192/2016**

8.5. ANEXO 5 – PLANO DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES – PLA-0140

HOSPITAL DE CLÍNICAS PORTO ALEGRE RS	Plano de Segurança da Tecnologia da Informação e Comunicações	Página 1/6
		PLA-0140

Definição

Este plano estabelece normas gerais e específicas de proteção às tecnologias da informação e de comunicações utilizadas pelo Hospital de Clínicas de Porto Alegre (HCPA), abrangendo todos os recursos tecnológicos que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e a comunicação dos processos de negócios.

Objetivos

Definir normas e instrumentos de controle para assegurar a proteção das informações contidas nas tecnologias que interferem e medeiam os processos informacionais e comunicativos, a fim de garantir integridade, confidencialidade e disponibilidade.

Assegurar o atendimento às obrigações legais, regulamentares, contratuais ou de requisitos do negócio relacionadas à Segurança da Informação.

Indicação

Este plano é aplicável em todas as áreas que respondem por recursos de armazenamento e transmissão de informações, envolvendo equipamentos, aplicativos, arquivos de dados, identificação do usuário e senha.

Instruções específicas

Definem-se:

- Integridade: princípio que garante a não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital.
- Confidencialidade: princípio que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal.
- Disponibilidade: princípio que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido.
- Ativos de Tecnologia da Informação (TI): recursos de informática, tais como equipamentos, aplicativos, arquivos de dados, identificação do usuário e senha.

A aplicação deste plano pressupõe o desdobramento de ações com os seguintes objetivos:

1. Assegurar a proteção das informações em rede e dos recursos de

processamento das informações.

2. Garantir a segurança no ciclo de vida dos equipamentos e sistemas de informação desenvolvidos, mantidos, descartados, doados e/ou removidos do HCPA.
3. Estabelecer requisitos de segurança na elaboração de projetos e na aquisição de soluções que envolvam Tecnologia da Informação e Comunicações (TIC).
4. Proteger contra a perda de dados vitais para os processos de negócio da instituição.
5. Gerenciar o acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de gestão, aplicações corporativas e serviços de Tecnologia da Informação e Comunicações (TIC).
6. Gerenciar a proteção dos ativos de informação da instituição ou em uso na mesma e que são acessados pelos fornecedores, prestadores de serviços e parceiros.
7. Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança institucional.
8. Garantir a operação segura e correta dos recursos de processamento da informação.
9. Assegurar a proteção das informações em rede e dos recursos de processamento da informação que as apoiam. Os equipamentos de informática ligados à rede corporativa devem ser de propriedade do HCPA ou estar em regime de cessão de uso a título gratuito ou oneroso.
10. Promover anualmente a análise crítica da implementação e operação deste Plano.

Competências e Fluxos

1. Cabe à Coordenadoria de Gestão de Tecnologia da Informação e Comunicação (CGTIC):
    a. Realizar auditorias periódicas, através de funcionários capacitados e

autorizados para tal, e, sempre que houver necessidade, visando ao cumprimento deste Plano, verificar o conteúdo das informações que trafegam na rede ou que estejam armazenadas em equipamentos instalados no HCPA.

b. Regrar as conexões para manutenção local ou remota dos servidores instalados no Datacenter.

c. Autorizar toda e qualquer conexão ou desconexão da rede corporativa de qualquer equipamento de informática.

2. Cabem à Equipe de Tratamento de Incidentes de Redes e Sistemas (ETIR) atuarem na prevenção, detecção, análise, tratamento e respostas aos incidentes de rede, sistemas e segurança da informação, tanto no ambiente técnico-computacional como na segurança da informação corporativa e técnica.
3. Cabe aos gestores do HCPA:
    a. Conscientizar colaboradores sob sua supervisão em relação aos conceitos, às práticas e à cultura em segurança da informação; incorporar aos processos de trabalho da área práticas inerentes à segurança da informação.
    b. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação, estabelecendo a devida comunicação.
    c. Submeter projetos que envolvam aquisições de soluções de Tecnologia da Informação e Comunicações (TIC), tanto previamente quanto durante o ciclo de vida do projeto, à Coordenadoria de Gestão da Tecnologia da Informação e Comunicação (CGTIC) e/ou à Coordenadoria de Engenharia e Manutenção, para as análises de conformidade técnica e de segurança da informação.
4. Cabe a todos os integrantes das comunidades interna e externa do HCPA zelar pelas informações e recursos aos quais têm acesso; observar princípios éticos e direitos autorais; comunicar atitudes ou situações suspeitas; observar normas e procedimentos internos, a fim de assegurar que requisitos estatutários, legais e contratuais sejam atendidos.

5. Cabe a todos os integrantes da comunidade interna:
    a. Manter cópia de segurança dos arquivos armazenados na respectiva estação de trabalho.
    b. Proteger a sua senha e observar que não é permitido o uso da identificação e senha de outra pessoa.
    c. Acessar de forma intransferível qualquer ativo de TI, sendo estes destinados ao desenvolvimento das atividades inerentes à Missão da Instituição.
    d. Observar os princípios éticos, os direitos autorais, os acordos de licenciamentos obrigatórios para a instalação e uso de programas e o cumprimento da legislação pertinente.
    e. Observar que não é permitida a instalação de dispositivos para acesso remoto em equipamentos ligados à rede corporativa.
    f. Observar que não é permitida a facilitação do acesso a terceiros, não autorizados, aos ativos de TI do HCPA, incluindo equipamentos médicos.
    g. Observar que não é permitido o fornecimento a outrem e/ou a retenção para uso próprio de cópia(s) de programa(s) protegido(s) por copyright ou licenciamento, mesmo que o(s) programa(s) seja(m) sem custo e/ou para uma finalidade educacional, a menos que haja cláusula expressa no contrato de licenciamento que o permita.
6. Cabem à Comissão de Segurança da Informação e Comunicações as seguintes atribuições: a) definir a estratégia de segurança e garantir alinhamento estratégico; b) assessorar e promover a implementação das ações de segurança da informação e comunicações no HCPA; c) propor a constituição de grupos de trabalho para tratar de temas e soluções específicas sobre segurança da informação e comunicações; d) manter a atualização da Política de Segurança da Informação e Comunicações (POSIC) conforme mudanças nos processos institucionais e garantir conformidade com as disposições constitucionais, legais e regimentais vigentes; e) aprovar e

acompanhar planos de ação e procedimentos operacionais padrão para aplicação da POSIC, avaliando os resultados e propondo melhorias; f) promover a cultura em segurança da informação e comunicações; g) solicitar apuração quando da suspeita de ocorrências de transgressão da POSIC; h) esclarecer eventuais dúvidas e deliberar sobre assuntos relativos à POSIC.

7. Cabe à chefia imediata tratar a omissão ou conivência que implique desobediência ou inobservância das disposições deste Plano, após devidamente apuradas e se comprovadas, providenciando, conforme o caso e de acordo com o Regulamento da Instituição, a advertência, suspensão, demissão sem ou por justa causa e/ou comunicação às autoridades competentes.

Registro

A melhoria contínua deste Plano ocorre de forma sistemática, com base nos registros de auditorias, incidentes de segurança da informação, retorno dos usuários e análise da eficácia dos controles.

A eficácia deste Plano será avaliada através de apontamentos de eventos não contemplados pelo mesmo.

Referências

O gerenciamento de Segurança da Informação segue os preceitos estabelecidos na Norma ABNT NBR ISO/IEC 27001 (Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos) e na Norma complementar 03/IN01/DSIC/GSIPR (Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal).

Elaborado por: **Grupo de Trabalho Atualização das Diretrizes Relacionadas à Segurança da Informação e Comunicações - Ato 192/2016**

8.6. ANEXO 6 – PLANO DE SEGURANÇA CIBERNÉTICA – PLA-0141

HOSPITAL DE CLÍNICAS PORTO ALEGRE RS	Plano de Segurança Cibernética	Página 1/7
		PLA-0141

Definição

Este plano estabelece normas gerais e específicas de proteção das informações produzidas e/ou custodiadas pelo Hospital de Clínicas de Porto Alegre (HCPA), abrangendo o controle das ameaças existentes e inerentes aos meios tecnológicos interligados em redes e serviços de abrangência global, promovidas pelas explorações dos agentes usuários.

Objetivos

Definir normas e instrumentos de monitoramento das informações disponibilizadas no espaço cibernético, a fim de promover orientações das melhores práticas comportamentais neste contexto.

Assegurar o atendimento às obrigações legais, regulamentares, contratuais ou de requisitos do negócio relacionadas à Segurança da Informação.

Indicação

Este plano é aplicável a toda comunidade interna (grupo formado por professores, pesquisadores, funcionários, estudantes, residentes, estagiários e jovens aprendizes) e externa (pacientes, acompanhantes, fornecedores e visitantes).

Instruções específicas

Definem-se:

- Mídias Sociais: ferramentas digitais que possibilitam a interação social a partir do compartilhamento e da criação colaborativa de informação nos mais diversos formatos. São exemplos: Facebook, WhatsApp, Twitter, YouTube, Wikipedia, Google+, LinkedIn, Instagram, Picasa e blogs, entre outros.
- Ferramentas Colaborativas: conjunto de ferramentas disponibilizadas pela instituição para compartilhamento de mensagens (e-mails, hangout, chats) e

documentos (arquivos, sites, formulários), assim como interação de membros de grupos (listas e fóruns de discussão).

- Espaço Cibernético ou Ciberespaço: espaço virtual para a comunicação que surge da interconexão das redes de dispositivos digitais interligados no planeta, incluindo seus documentos, programas e dados. A Internet é considerada o principal ambiente do ciberespaço.
- Rede Corporativa ou Rede com Fio: ambiente de equipamentos e serviços interligados, dotado de recursos de segurança para proteção dos Bancos de Dados e demais informações institucionais.
- Rede Visitantes ou Rede sem Fio: segmento de rede com ou sem fio, logicamente isolado da rede corporativa, para uso de pacientes, fornecedores, professores, pesquisadores, alunos e funcionários com equipamentos próprios.

A aplicação deste Plano pressupõe o uso preferencial de sistemas e ferramentas disponibilizados pela instituição, tais como e-mail do domínio @hcpa, plataforma de comunicação Hangout, solução de videoconferência Meet. Além disso, este Plano tem o desdobramento de ações com os seguintes objetivos:

1. Estabelecer as seguintes práticas para o uso seguro das mídias sociais na instituição:
    a. Na rede corporativa do HCPA (com fio), o amplo acesso às mídias sociais nos equipamentos do HCPA é permitido exclusivamente para fins institucionais e em locais específicos, tais como Coordenadoria de Comunicação (CCom), auditórios, anfiteatro, salas de aula e salas de recreação para pacientes.
    b. É permitido acesso às mídias sociais à comunidade interna, assim como pacientes, familiares, fornecedores e visitantes, por meio da rede interna wireless (sem fio), seja utilizando equipamentos próprios ou equipamentos do HCPA. Neste caso, para a comunidade interna, é determinado o uso preferencialmente institucional ou relacionado às atividades desenvolvidas na instituição.

2. Estabelecer as seguintes práticas para o uso seguro das ferramentas colaborativas na instituição:
    a. Na utilização dos aplicativos que o HCPA disponibiliza para a construção colaborativa e o uso compartilhado de mensagens e documentos, estes podem ser gerados por qualquer usuário de domínio do HCPA (@hcpa) e visualizados e/ou editados por outras pessoas, independente de estarem ou não dentro deste domínio, desde que prevaleça a finalidade institucional de uso dos recursos.
    b. É permitida a criação de sites com o uso de ferramentas colaborativas institucionais, para acesso de uma determinada área, grupo, programa ou comissão do hospital, a fim de compartilhar documentos, informações e normas de interesse restrito, de forma a apoiar a realização de seu trabalho. O compartilhamento deve ser restrito.
    c. A responsabilidade pela criação ou autorização de sites fora do domínio HCPA, se necessário, que envolvam divulgação de atividades de áreas, grupos, programas ou comissões, é exclusiva da CCom, de acordo com o Plano de Comunicação Institucional.
    d. É permitida a criação de grupos (listas eletrônicas e fóruns de discussão) para acesso interno e externo, voltados a assuntos de interesse institucional de uma determinada área, grupo, programa ou comissão.
    e. O gerenciamento dos documentos e aplicativos desenvolvidos na plataforma colaborativa, em especial as permissões de acesso para compartilhamento, é de responsabilidade dos respectivos proprietários e editores, aos quais cabe resguardar a segurança das informações institucionais.
    f. As ferramentas colaborativas oferecidas pela instituição à comunidade interna são destinadas ao uso durante os horários regulamentares de trabalho ou de desenvolvimento de atividades acadêmicas ou de pesquisa.

3. Monitorar as marcas de propriedade do HCPA nos espaços de convívio e cibernético.
4. Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança institucional.
5. Promover anualmente a análise crítica da implementação e operação deste Plano.

Competências e Fluxos

1. Cabe à Coordenadoria de Comunicação (CCom):
    a. Atuar como Administradora dos Perfis Institucionais nas Mídias Sociais, respondendo pela criação, manutenção e gestão dos conteúdos disponibilizados nesses meios.
    b. Divulgar informações sobre o HCPA nas mídias sociais, observando que o nome e/ou da marca da instituição estejam alinhados à Missão, ao Propósito, aos Valores e às demais definições estratégicas da instituição, bem como aos preceitos éticos e legais e respeitando estritamente o sigilo e a privacidade de dados de pacientes.
2. Cabe à Coordenadoria de Gestão de Tecnologia da Informação e Comunicação (CGTIC) a gestão da segurança das informações que trafegam na rede corporativa ou que estejam armazenadas em equipamentos instalados no HCPA e, consequentemente, a identificação de usos inadequados e o encaminhamento para a aplicação das medidas cabíveis, segundo normas institucionais vigentes.
3. Cabe aos Integrantes da comunidade interna:
    a. Ao reproduzirem, em seus perfis privados nas mídias sociais, o nome, a logomarca, informações e/ou imagens do HCPA, respeitar os preceitos éticos e as normas de sigilo e privacidade que regem sua atuação na instituição, bem como seguir conduta compatível com a boa imagem

pública do hospital.

b. Observar que a utilização das ferramentas colaborativas oferecidas pelo HCPA fora dos horários regulamentares de trabalho ou de desenvolvimento de atividades acadêmicas ou de pesquisa não representa tempo à disposição do HCPA, salvo exceções, sendo a utilização, neste caso, de responsabilidade exclusiva do usuário.

4. Cabem à Comissão de Segurança da Informação e Comunicações as seguintes atribuições: a) definir a estratégia de segurança e garantir alinhamento estratégico; b) assessorar e promover a implementação das ações de segurança da informação e comunicações no HCPA; c) propor a constituição de grupos de trabalho para tratar de temas e soluções específicas sobre segurança da informação e comunicações; d) manter a atualização da Política de Segurança da Informação e Comunicações (POSIC) conforme mudanças nos processos institucionais e garantir conformidade com as disposições constitucionais, legais e regimentais vigentes; e) aprovar e acompanhar planos de ação e procedimentos operacionais padrão para aplicação da POSIC, avaliando os resultados e propondo melhorias; f) promover a cultura em segurança da informação e comunicações; g) solicitar apuração quando da suspeita de ocorrências de transgressão da POSIC; h) esclarecer eventuais dúvidas e deliberar sobre assuntos relativos à POSIC.
5. Cabe à chefia imediata tratar a omissão ou conivência que implique desobediência ou inobservância das disposições deste plano, após devidamente apuradas e se comprovadas, providenciando, conforme o caso e de acordo com o Regulamento da Instituição, a advertência, suspensão, demissão sem ou por justa causa e/ou comunicação às autoridades competentes.

Registro

A melhoria contínua desse plano ocorre de forma sistemática com base nos registros

de auditorias, incidentes de segurança da informação, retorno dos usuários e análise da eficácia dos controles.

A eficácia deste Plano será avaliada através de apontamentos de eventos não contemplados pelo mesmo.

Referências

1. O gerenciamento de Segurança da Informação segue os preceitos estabelecidos na Norma ABNT NBR ISO/IEC 27001 (Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos) e na Norma complementar 03/IN01/DSIC/GSIPR (Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal).
2. O uso das mídias sociais pelo HCPA segue os preceitos estabelecidos na Portaria n. 38 da Secretaria Executiva do Conselho de Defesa Nacional, de 11 de junho de 2012, a qual homologou a Norma Complementar n. 15/IN01/DSIC/GSIPR, de 11 de junho de 2012, que estabelece diretrizes para o uso seguro das redes sociais na Administração Pública Federal.
3. Ato 008/2016, em que resolvido que todos os usuários do HCPA, no exercício de suas funções, deverão utilizar apenas o e-mail corporativo do Hospital ___@hcpa.edu.br.

Elaborado por: **Grupo de Trabalho Atualização das Diretrizes Relacionadas à Segurança da Informação e Comunicações - Ato 192/2016**

8.7. ANEXO 7 - PLANO DE CONTINUIDADE DOS SERVIÇOS DE TIC (PLA-0481)

HOSPITAL DE CLÍNICAS PORTO ALEGRE RS	Plano de Continuidade dos Serviços de TIC	Página 1/6
		PLA-0481

Definição

O Plano de Continuidade dos serviços de Tecnologia da Informação e Comunicações (TIC) consiste no documento que estabelece acordos operacionais de provimento de serviços de TIC para os momentos críticos que impeçam a operação destes serviços à plena capacidade, assegurando a operação nestes níveis dos principais processos de negócio do Hospital, no que dependem de TIC.

Objetivos

Estabelecer os recursos necessários e disponíveis que deverão ser utilizados em resposta a incidentes que impactam severamente as infraestruturas, dentre os quais os ativos críticos de TIC, tais como as salvaguardas disponíveis, os responsáveis e respectivos papéis, os escopos de cobertura, expectativas mínimas a serem atendidas nestas situações e atendimento às políticas Institucionais e governamentais no provimento de segurança da informação e comunicações.

Além disso, o Plano de Continuidade dos Serviços de TIC relaciona um conjunto de orientações que devem ser seguidas no caso de indisponibilidade na prestação dos principais serviços de Tecnologia da Informação e Comunicação (TIC) providos pela Coordenadoria de Gestão da Tecnologia da Informação e Comunicação (CGTIC), considerando o foco no restabelecimento dos principais serviços Institucionais prestados pelo Hospital de Clínicas de Porto Alegre (HCPA), dependentes dos ativos críticos de TIC localizados em seus Centros de Dados, para manter – em caráter de contingência – a integridade, confiabilidade, disponibilidade e autenticidade dos ativos de informação do HCPA diante de situações e impactos de extrema severidade, referenciados a partir de agora, como DESASTRES.

Indicação

O plano será utilizado quando da indisponibilidade de um ou mais serviços providos pelos Centros de Dados e manter a infraestrutura ativa no site backup, atualmente no

Bloco B, para garantir a disponibilidade, integridade, confidencialidade e autenticidade dos principais serviços de TIC utilizados no HCPA.

O principal serviço ao negócio é o sistema Aplicativos para Gestão Hospitalar (AGHUse). Os serviços técnicos providos pelo núcleo do ambiente computacional, fundamentais ao provimento do AGHUse são: Serviços Técnicos de Comunicação por Redes de Computadores; Serviços Técnicos de Banco de Dados e Serviços Técnicos de Computação nas camadas Servidoras. Não faz parte do escopo deste plano, impacto nas estações de trabalho e/ou dispositivos clientes, exceto se impactados por comprometimentos do núcleo.

O Plano de Continuidade dos Serviços de TIC será aplicado no ambiente de tecnologia da informação do HCPA, focado em grupos de recursos bem definidos: o das infraestruturas críticas de TIC de núcleo e de acesso, por parte do negócio a estes recursos, assegurando o provimento de serviços mínimos de TIC ao negócio, assegurando a operação mínima necessária, ainda que com parâmetros de qualidade de serviço reduzido e os de negócio, localizados junto às diversas áreas operacionais do Hospital.

Componentes do núcleo:

- Rotinas especiais que, baseadas nos fluxos de dados geram arquivos com informações estáticas, os quais são propagadas a todos os computadores assistenciais da rede, para armazenamento local, para acesso pelas rotinas de negócio;
- Os equipamentos de comunicação de rede com fonte redundante e alimentação suplementar (Nobreak);
- Enlaces físicos de redes redundantes, dispositivos por caminhos distintos, em todas as áreas de provimento de serviços de comunicação de redes;
- Ativos críticos armazenados em sala cofre certificada ABNT NBR 15.247;
- Data center redundante e interligados por enlaces redundantes, dispostos em caminhos distintos;
- Ativos críticos redundantes dispostos em locais físicos distintos, de forma a assegurar a o reinício das atividades, a pleno, tão logo o regime de contingenciamento seja encerrado;

Componentes das Áreas Operacionais:

- Impressoras para uso em modo de contingência;
- Servidor departamental instalado junto a área de negócio Emergência para operar em modo de contingência, assegurando a propagação de arquivos estáticos com as informações mais recentes, para aquela área;
- Garantia de propagação das informações para uso em situações de contingência.

Operação da Contingência:

- Revisão contínua do processo;
- Monitoramento contínuo da geração e da propagação das informações estáticas para uso em regime de contingência;
- Capacitação contínua para a operação em regime de contingência;
- Realização de testes periódicos com vistas a assegurar a capacidade de operação quando em regime de contingência.

Instruções específicas

O plano exige a realização de, no mínimo, 3 testes de recuperação de desastres anuais, durante os quais é realizado o chaveamento dos bancos de dados e aplicações para o datacenter de contingência no Bloco B, mantendo por alguns dias a operação do HCPA em regime de contingência. Estes testes são dirigidos pelos documentos técnicos:

- PDR DATABASES ORACLE PRODUÇÃO - procedimentos técnicos para os ambientes de banco de dados de produção;
- PDR AGHUse - procedimentos técnicos para o Aplicativo de Gestão Hospitalar (AGHUse), principal sistema de TIC para serviços de TI ao Hospital;
- PDR AGHWeb - procedimentos técnicos para o Aplicativo de Gestão Hospitalar (AGHUse) em interface Web, um dos principais sistema de TIC para serviços de TI ao Hospital, pois assegura a execução da porção legada do AGHUse;

Cada teste exige que estes documentos sejam reavaliados e ajustados, se necessário, conforme as intercorrências identificadas e contornadas durante os ensaios, contemplando assim qualquer nova mudança no ambiente técnico e/ou de novas práticas de operação de TIC (lições aprendidas);

Durante os testes o ambiente deve operar nas infraestruturas redundantes de recuperação de desastres por um período de aproximadamente 5 dias.

Competências e Fluxos

É de responsabilidade da CGTIC ativar o plano de continuidade conforme análise de impactos, situação operacional, disponibilidade de recursos envolvidos, disparando ações diversas, conforme os seguintes planos de contingência:

- **Plano de Contingência da Emergência por Indisponibilidade do Sistema Informatizado**

  O plano de contingência da emergência é constituído de uma composição de documentos que são gerados no momento em que são feitos registros no prontuário eletrônico do paciente da Emergência. Cada registro é atualizado de forma on-line no documento, e é feita uma atualização dos exames em uma periodicidade pré-determinada, de poucos minutos. Os documentos são gravados em um servidor que fica fisicamente na Emergência, dedicado para este fim. Além da consulta, se a rede principal de computadores do HCPA estiver operando normalmente, o plano de contingência permite o registro da evolução do atendimento. Eventuais registros feitos durante a utilização do plano de contingência são posteriormente carregados para o prontuário eletrônico do paciente, no momento que o AGHUse voltar a operar na sua normalidade. Se apenas a rede local estiver funcionando é possível apenas a consulta das informações. Para profissionais habilitados ao registro e assinatura do atendimento é permitida a consulta aos documentos e registro da evolução. Para os profissionais que podem consultar o atendimento é permitida apenas a consulta dos documentos. Os demais profissionais não possuem acesso aos documentos.

- **Plano de Contingência da Internação por Indisponibilidade do Sistema Informatizado**

  O plano de contingência da internação consiste de único documento chamado Sumário de Parada que é gerado em 2 momentos: é feita uma geração diária para todos os pacientes internados em um horário pré-determinado do dia, e atualizações on-line a cada novo registro de anamnese/evolução. Fazem parte do documento: informações do paciente, da internação, exames, prescrições, cirurgias etc. Os documentos são distribuídos nos computadores da unidade de internação e podem ser consultados apenas se o plano de contingência for ativado. Além da consulta, se a rede de computadores estiver operando normalmente, o plano de contingência permite o registro da evolução do atendimento e permite a impressão do documento. Estes registros são

posteriormente importados para o prontuário eletrônico do paciente, no momento em que o AGHUse voltar a operar na sua normalidade. Para profissionais habilitados ao registro e assinatura do atendimento é permitida a consulta aos documentos e registro da evolução. Para os profissionais que somente consultam os registros de anamnese/evolução é permitida somente a consulta. Aos demais profissionais não é liberado o acesso aos documentos. Os usuários que tiverem um perfil específico poderão imprimir estes documentos.

- **Plano de Contingência do Ambulatório por Indisponibilidade do Sistema Informatizado**

  O plano de contingência do ambulatório é constituído de uma composição de documentos extraídos no dia anterior à consulta do paciente no ambulatório. Fazem parte deste conjunto de documentos: sumário de exames, sumário de alta da internação, histórico do paciente (internações, consultas, cirurgias, diagnósticos e procedimentos) além do registro das anamneses e evoluções ambulatoriais.
  Os documentos são distribuídos nos computadores do ambulatório conforme local de realização da consulta e podem ser consultados somente quando o plano de contingência for ativado. Além da consulta, se a rede de computadores estiver operando normalmente, o plano de contingência permite o registro da evolução do atendimento. Estes registros são posteriormente importados para o prontuário eletrônico do paciente, no momento que o AGHUse voltar a operar na sua normalidade.
  Somente aos profissionais habilitados ao atendimento ambulatorial é liberado o acesso ao plano de contingência. Para profissionais habilitados ao registro e assinatura do atendimento é permitida a consulta aos documentos e registro da evolução. Para os profissionais habilitados somente para a consulta do atendimento é permitida somente a consulta. Os demais profissionais não possuem acesso aos documentos.

Registro
Não aplicável

Referências
Não aplicável

Elaborado por: **Seção de Infraestrutura e Segurança de TIC - Coordenadoria de Gestão da Tecnologia da Informação e Comunicação**

8.8. ANEXO 8 – PLANO INSTITUCIONAL DE GERENCIAMENTO DE SISTEMA DE COMUNICAÇÃO E DADOS

HOSPITAL DE CLÍNICAS PORTO ALEGRE RS	Plano Institucional Gerenciamento de Sistema de Comunicação e Dados	Página 1/10
		PLA-0737

Definição

Este documento estabelece o conjunto de procedimentos de gestão, planejados e implementados a partir de bases técnicas, normativas e legais, abrangendo cada etapa do gerenciamento dos sistemas de Comunicação e Dados do HCPA sob responsabilidade da Coordenadoria de Gestão da Tecnologia da Informação e Comunicação (CGTIC).

Objetivos

Garantir a integridade, confidencialidade e a alta disponibilidade, qualidade e segurança no suprimento dos sistemas de dados, visando à manutenção preventivas e corretivas das condições necessárias à promoção da saúde pública.

Indicação

O Plano se aplica aos sistemas de Comunicação e Dados, rede de Telecomunicações (Rede física e Rede lógica), banco de dados, servidores de aplicações, conectividade externa, Datacenters, computadores centrais (Servidores físicos) e backups.

Instruções específicas

1. Rede de Telecomunicações

1.1. Rede física

A rede física do HCPA é composta por links de fibra óptica que interligam o datacenter aos armários de borda. Cada armário de borda possui uma fibra óptica principal e uma secundária, sendo que a secundária interliga a outro armário próximo. Por exemplo, o armário 13S (13° andar Sul), possui interligação horizontal com o armário 13N (13° andar Norte) e cada um desses possui ligação principal com o datacenter, através de caminhos diferentes. Os armários de borda são alimentados por nobreak específico que garantem continuidade de funcionamento em situações de falta de energia. Os computadores, impressoras e demais equipamentos são ligados aos armários através de cabeamento horizontal metálico.

Com a redundância de fibras ópticas descrita acima, garante-se a continuidade do funcionamento da rede física mesmo em caso de rompimento do caminho principal.

1.2. Rede lógica

No datacenter principal do HCPA estão instalados dois switches de grande porte (A e B), configurados de forma redundante. As fibras ópticas que chegam dos armários de borda são ligadas aos switches de forma organizada, garantindo plena continuidade de conexão. Continuando com o exemplo dado anteriormente, a fibra que chega do armário 13N é ligada ao switch A, enquanto a fibra que chega do armário 13S é ligada ao switch B. Dessa forma, mesmo que ocorra falha de funcionamento de um dos switches, não há descontinuidade de conexão pois o tráfego de dados tem continuidade normal pelo outro lado.

2. Bancos de Dados

Adotamos no HCPA como tecnologia de bancos de dados as soluções providas pela fabricante Oracle Corporation. Trata-se de uma solução consolidada globalmente e utilizada por grandes corporações em todo o mundo por prover recursos de alta tecnologia, segurança e confiabilidade.

Os bancos de dados centrais estão configurados em Oracle Real Application Cluster (Oracle RAC), instalado em equipamento Oracle Exadata Database Machine. Essa configuração provê a instalação simultânea em dois servidores físicos ligados diretamente a área de armazenamento específica e espelhada, provendo altíssima disponibilidade.

Além da configuração acima, possuímos um segundo equipamento Oracle Exadata Database Machine, instalado em datacenter secundário, para onde todas as informações gravadas no banco de dados principal são replicadas em tempo real. Com isso, mesmo que ocorra um evento grave que indisponibilize completamente o datacenter principal, os dados corporativos são plenamente preservados.

Os servidores de banco de dados estão protegidos em uma rede dedicada, onde toda a comunicação de rede é inspecionada, além de forte

mecanismo de controle contra código malicioso. Apenas origens autorizadas podem realizar a comunicação de rede neste ambiente.

3. Servidores de Aplicação

O sistema AGHUse, aplicação corporativa principal do HCPA, é executado a partir de um *pool* (conjunto) de servidores de aplicação, que executam simultaneamente o sistema e recebem as conexões dos usuários de forma balanceada. Atualmente o pool é formado por 9 servidores de produção e possuímos um sistema de balanceamento de carga que distribui automaticamente as conexões, ou seja, cada vez que um usuário faz novo acesso ao sistema, o balanceador intercepta e identifica qual dos servidores está menos sobrecarregado, fazendo o direcionamento. Caso qualquer um desses servidores apresente problemas, essa situação é notificada ao balanceador que automaticamente passa a direcionar as conexões para os demais servidores, garantindo que não ocorra indisponibilidade do sistema.

Possuímos ainda um segundo pool de servidores de aplicação que é utilizado para realizar os chaveamentos de entrada de novas funcionalidades do sistema em produção. Esse processo de chaveamento ocorre em média uma vez por dia, de forma transparente para os usuários, funcionando da seguinte forma:

Sempre que existem novas funcionalidades do AGHUse para entrarem em produção, ocorre um procedimento denominado deploy. Nossos robôs de automação identificam qual o pool de servidores está em produção (Ex: pool A) e então realiza o deploy no outro pool (Ex: pool B). Após o deploy executado no pool B, vai uma notificação para o balanceador que passa a direcionar as conexões dos usuários para o pool B, conforme forem fazendo novo login, sem gerar interrupção do sistema. Após o direcionamento de todos os usuários para o novo pool, fica o pool anterior novamente disponível para realização de outro deploy e assim consecutivamente.

Os servidores de aplicação do AGHUse estão protegidos em uma rede dedicada, onde toda a comunicação de rede é inspecionada, além de forte mecanismo de controle contra código malicioso. Apenas origens autorizadas podem realizar a comunicação de rede neste ambiente.

Adicionalmente, possuímos no datacenter secundário um terceiro pool de servidores que fica em standby (em espera), para utilização em situações de exceção.

Com as tecnologias e implementações acima, fica garantida a plena operacionalidade do sistema AGHUse para funcionamento 24/7 non stop.

4. Conectividade externa

A conectividade à internet (e a integração aos serviços externos) se dá através de um link com fibras ópticas próprias do HCPA interligadas ao Ponto de Presença RS da Rede Nacional de Pesquisa (RNP). Adicionalmente, possuímos contrato com link de fibra óptica comercial a qual entra em operação no caso de falhas do link principal. Regularmente são realizados chaveamentos entre os dois links para testes e garantia de funcionamento.

Toda comunicação de rede do HCPA para a internet ou da internet para o HCPA é inspecionada em camadas de segurança, mitigando ataques cibernéticos.

5. Datacenters

O datacenter principal do HCPA é composto de uma sala cofre certificada ABNT NBR 15247, certificação essa que garante ter passado por ensaios de resistência contra incêndios, umidade, impactos mecânicos etc.. A sala cofre é alimentada por sistemas redundantes de energia instalados em locais diferentes e com caminhos distantes entre si. Da mesma forma, o sistema de climatização é composto por um pool de máquinas de ar condicionado, operando na configuração N+1, o que garante sempre um aparelho de ar condicionado inativo para entrada em operação imediata em caso de falha.

A Sala Cofre possui sistema duplo de detecção de incêndio, sendo que o primeiro deles funciona através da detecção precoce de partículas no ar, monitorado permanentemente, e o segundo através de sensores de teto. O combate a um eventual princípio de incêndio se dá através de sistema automatizado de aspersão de gás FM200.

O acesso físico à sala cofre é controlado através de autenticação por crachá e leitura biométrica e é restrito aos funcionários da CGTIC treinados na operação do sistema de monitoração.

O datacenter secundário não possui sala cofre, porém é instalado com características técnicas semelhantes a de uma sala segura (redundância elétrica (nobreak e gerador) e de climatização, além de monitoramento remoto por CFTV), atendendo as recomendações para sala de servidores. Possui sistema de climatização e detecção de incêndio, com acesso via fechadura eletrônica e chave, e restrição aos funcionários da CGTIC habilitados para sua operação.

6. Computadores centrais (Servidores físicos)

Os computadores centrais que rodam os sistemas corporativos possuem características de alta disponibilidade, contando com placas de rede e fontes elétricas redundantes. As placas de rede são ligadas cada uma a um Switch Core diferente assim como as fontes elétricas são ligadas a diferentes circuitos de alimentação.

7. Backups

Além da replicação dos dados e servidores já descritos nos itens anteriores, são realizadas rotinas diárias de backup, com armazenamento inicial em disco e replicação para unidades de fita LTO, armazenadas em local separado do datacenter.

São realizados periodicamente e documentados, testes do processo de restauração de backup para garantia de funcionamento em caso de necessidade.

8. Monitoramento

Para fins de acompanhar a situação da rede, equipamentos e sistemas em tempo real, a CGTIC dispõe de um painel de monitoramento baseado em ferramenta padrão de mercado, denominada ZABBIX, além disso,

monitoramos toda a rede via o sistema IMC HP. Nessa ferramenta são configurados itens de monitoração que são executados permanentemente fazendo acesso aos diferentes serviços. Como exemplo, temos itens de monitoração que ficam conectados sequencialmente nos servidores e verificando se estão plenamente operacionais. Caso seja detectada qualquer anomalia, é disparado um alarme identificando o problema. Importante destacar que na maioria dos casos, o alarme é disparado preventivamente, ou seja, antes de haver uma indisponibilidade. Detalhando o exemplo anterior, ao conectar em um servidor se for detectado um aumento de uso de memória, processador, disco etc., acima dos valores médios, já é disparado um alarme de advertência, permitindo que a equipe técnica avalie a situação e tome providências antes que se torne crítica.

9. Equipe técnica

Dispomos de uma equipe técnica denominada SuDat (Supervisão de Datacenter), devidamente treinada na operação dos principais ativos de TI localizados no datacenter principal e secundário, além da rede física e lógica do hospital.

Essa equipe possui regime de trabalho 24x7x365, fazendo a operação plena dos sistemas e das rotinas de retaguarda. Nos horários não comerciais a equipe SuDat também realiza o atendimento telefônico da central de relacionamento, dando orientações aos usuários e acionando os plantões de sobreaviso especializados, em caso de incidentes com os sistemas corporativos ou infraestrutura.

10. Planos de contingência

Plano de Continuidade dos Serviços de TIC - PLA-0481.
POP de Salvaguarda e Recuperação de Informações - POP-0138.
Sistema informatizado de contingência para os sistemas críticos.

Competências e Fluxos

Os procedimentos relacionados ao Plano têm suas competências assim distribuídas entre as áreas envolvidas:

1. Comissão de Investimentos

Planejar a destinação de recursos do Hospital determinando as prioridades de aquisição com base em uma avaliação com critérios técnicos (realizada pelo setor competente, conforme definido na sequência).

2. Coordenadoria de Gestão da Tecnologia da Informação e Comunicação - CGTIC

A CGTIC tem como objetivo prover os serviços de Tecnologia da Informação e Comunicação (TIC) às áreas do HCPA, para potencialização das atividades de assistência, ensino e pesquisa, em consonância com o PETIC e o PNGE. Compete à CGTIC: Garantir o alinhamento de Tecnologia da Informação e Comunicação (TIC) com o negócio do Hospital; Conceber, especificar, desenvolver, integrar e aperfeiçoar as soluções de TIC; Gerenciar e executar projetos de TIC; Projetar, implantar e prestar suporte técnico à infraestrutura de TIC; Gerenciar os contratos com empresas prestadoras de serviços em TIC e fornecedoras de hardwares e softwares; Propor e gerir normas para segurança da informação e utilização dos ativos de TIC; Gerenciar o parque de ativos de TIC; Garantir agilidade, confidencialidade, integridade e disponibilidade dos aplicativos, dos serviços e das informações institucionais armazenadas no âmbito da TIC do HCPA; Fomentar iniciativas de Inovação e acompanhar as tendências do mercado de TIC; Apoiar as áreas clientes, na definição dos recursos de TIC, no uso dos aplicativos (softwares) e no gerenciamento de projetos; Elaborar memoriais descritivos, pareceres, aceites e outros documentos técnicos da área de TIC; Preservar a integridade técnica dos equipamentos de TIC; Representar institucionalmente o HCPA em atividades relacionadas a TIC.

2.1. Serviço de Gestão de Tecnologia

Compete ao Serviço de Gestão de Tecnologia realizar as atividades técnicas e desenvolvimento de aplicativos, a operação e o monitoramento dos serviços e TIC, a administração de banco de dados, a atualização e a manutenção da infraestrutura de TIC, bem como a gestão de datacenter e da segurança da informação;

2.2. Seção de Infraestrutura e Segurança

Compete à Seção de Infraestrutura e Segurança projetar, implementar e entregar soluções de infraestrutura de TIC, através do provimento de recursos e serviços com agilidade, segurança, estabilidade e escalabilidade, cultivando a colaboração entre equipes e as melhores práticas de segurança da informação nos processos e tecnologias do ecossistema computacional.

2.3. Supervisão de Gestão de Datacenter

Compete à Supervisão de Gestão de Datacenter a monitoração da disponibilidade dos serviços de TI em regime de 24x7x365, a execução de rotinas operacionais, a responsabilidade pela segurança física do datacenter e da CGTIC e pela integridade e manutenção da rede física de TIC.

2.4. Seção de Desenvolvimento e Operações

Compete à Seção de Desenvolvimento e Operações o desenvolvimento e a manutenção dos sistemas corporativos por meio da atuação integrada de sua equipe técnica multidisciplinar (desenvolvedores, analista de qualidade, arquiteto de software, analista de infraestrutura e administrador de dados), primando pelas boas práticas, padrões e metodologia com foco na entrega de resultados com qualidade e agilidade.

2.5. Supervisão de Monitoramento e Controle

Compete à Supervisão de Monitoramento e Controle as atividades multidisciplinares de monitoramento e atualização dos sistemas de TIC na Instituição. Buscando a automatização e otimização dos processos de atualização de software, gerência de configuração e garantia da qualidade do produto (Quality Assurance).

Registro

- Registro do boletim - A SuDat elabora dois documentos diários com registros de todos os eventos referentes a alertas de monitoramentos, rotinas diárias, avisos de manutenções programadas, acionamentos de plantonistas e atendimentos aos usuários em horários específicos. Os documentos são denominados “Boletim Diurno”, que abrange o período das 07hs às 19hs, e “Boletim Noturno”, das 19hs às 07hs. São compartilhados ao término do período com uma lista de e-mails própria e ficam armazenados no Drive para consultas futuras.

- Como descrito acima, usamos o sistema de monitoramento Zabbix, nele temos registrado todos os eventos no nosso sistema de comunicação de dados, sendo possível criar indicadores e buscas inteligentes no histórico.

- Todas as atividades são registradas nos sistemas de gestão de chamados, tanto no Qualitor como no Redmine. Qualitor usado principalmente pelo time da SuDat contém os chamados dos usuários, incidentes ou novos pedidos e todo o fluxo de atendimento e registro de atuação ficam registrados. O Redmine usado pelas demais equipes são para atividades internas, sejam elas projetos ou ações mais especializadas.

- Construção de pareceres sobre situações, riscos e pontos de melhorias necessários, notificando os responsáveis.

Referências

Elaborado por: **Renato Falsarella Martins Malvezzi rmalvezzi**

8.9. ANEXO 9 – MATRIZ DE CAPACITAÇÃO DA CGTIC

A matriz de capacitação da CGTIC tem o objetivo de definir as capacitações necessárias para buscar o desenvolvimento constante das competências dos colaboradores da CGTIC, com as qualificações e conhecimentos necessários para execução do PDTIC em consonância com os objetivos estratégicos institucionais, assim como, para motivar e incentivar os colaboradores à excelência das suas atividades e ao aprendizado contínuo para fazer frente às mudanças exponenciais na qual estamos inseridos.

Matriz de Capacitação Setorial			
Área de Interesse	**Capacitação**	**Periodicidade**	**Área**
Ciência de Dados	Analista de Dados de Negócios	Anual	CGTIC
	Introdução à Ciência de Dados		
Congressos	Agile Brazil	Anual	CGTIC
	Congresso Brasileiro de Gestão, Projetos e Liderança (PMI)	Anual	SGN / SSR / SuGePPI
	Congresso Brasileiro de Informática em Saúde (CBIS)	Bienal	CGTIC
	South Summit Brasil	Anual	CGTIC
	The Developers Conference (TDC)		
Contratos	Administração de Serviços na Nuvem de Governo	Anual	CGTIC
	Análise de Riscos para Contratações de TIC		
	Fiscalização e Gestão dos Contratos de TIC		

	Fundamentos de Gestão de Contratos		
	Planejamento da Contratação de Soluções de TIC		
	Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME	Anual	SuCon
Infraestrutura	Administração de Sistemas Linux	Anual	SGT
	BGP Avançado		
	Cloud Essentials		
	IPv6 Básico		
	Planejamento e Projeto de Infraestrutura para Datacenter		
	Instalações e Manutenções de Fibras Óticas		
	Protocolos de Roteamento IP		
	Virtualização de Servidores		
Institucionais	Conduta e Integridade	Anual	CGTIC
	Direitos e Deveres do Paciente		
	Gestão por Competência		
	Incêndio e Outras Emergências		
	Lei Geral de Proteção de Dados (LGPD)		
	Metas Internacionais de Segurança dos Pacientes		
	Segurança da Informação e Comunicações		
	SEI! Sistema Eletrônico de Informações		

	Sustentabilidade nas Práticas Hospitalares		
Governança e Gestão de TIC	Criatividade e Novas Tecnologias no Serviço Público	Anual	CGTIC
	Desenvolvendo Times de Alta Performance		
	Elaboração de PDTI		
	Fundamentos do COBIT	Anual	SSR
	Fundamentos de Governança de TIC	Anual	CGTIC
	Gerenciamento de Serviços de TIC	Anual	SGT / SSR
	Gestão de Conflitos e Negociação	Anual	CGTIC
	Gestão de Continuidade de Negócios	Anual	SGT / SSR
	Gestão de Equipes em Trabalho Remoto	Anual	CGTIC
	Gestão de Projetos de Teste de Software	Anual	SGT / SuGePPI
	Governança de TIC no Contexto da Transformação Digital	Anual	CGTIC
	Inteligência Emocional		
	ITIL 4 Foundation	Anual	SSR
	Lei Geral de Proteção de Dados (LGPD)	Anual	CGTIC
	Planejamento e Gestão Estratégica de TIC		
	Planejamento Estratégico para Organizações Públicas		
	Proteção de Dados Pessoais no Setor Público		
	Sistema de Gestão da Integridade – Compliance		

	& Antissuborno		
Inovação e Métodos Ágeis	Ágil no Contexto do Serviço Público	Anual	CGTIC
	Design Thinking		
	Gestão Ágil de Projetos		
	Gestão de Containers com Docker	Anual	SGT
	Princípios do Design Thinking e Inovação em Governo	Anual	CGTIC
	Scrum no Contexto do Serviço Público		
Segurança da Informação	Cibersegurança	Anual	SGT
	Correlacionamento de eventos com Graylog		
	Fundamentos de Segurança da Informação	Anual	CGTIC
	Gestão da Segurança da Informação e Privacidade		
	Gestão de Riscos de Segurança da Informação e Privacidade		
	Hardening em Linux	Anual	SGT
	PenTest		
	Segurança de Redes e Sistemas		
	Teste de Invasão de Aplicações Web		
	Tratamento de Incidentes de Segurança		