Documento de Especificação de Requisitos Funcionais e de Dados

1. Identificação do Projeto

Nome da aplicação/projeto: Sistema de Persistência e Análise de Crimes Cibernéticos (SIPACC)

Equipe responsável: Lucas Antônio Petry, Arthur Virgílio, José Carvalho

Data da elaboração: 29/09/2025

2. Introdução

O avanço das tecnologias digitais trouxe inúmeros benefícios para a sociedade, mas também aumentou a incidência de crimes cibernéticos, como fraudes bancárias, estelionatos virtuais, ataques de phishing, invasões de sistemas e diversas outras ações criminosas dentro do mundo da Internet. Esses crimes apresentam características específicas: ocorrem em meio digital, podem ter múltiplas vítimas espalhadas geograficamente de forma até simultânea e muitas vezes envolvem anonimato dos autores, ao aplicarem técnicas que violem os meios de segurança da informação e tentarem se esconder em ambientes com maior de dificuldade de rastreio.

O SIPACC é um sistema de banco de dados voltado para o registro, consulta e análise de crimes cibernéticos. Permite cadastrar ocorrências, gerenciar informações sobre vítimas, suspeitos, dispositivos e contas envolvidas, além de fornecer relatórios estatísticos e análises de padrões digitais, auxiliando na produção de informações estratégicas para a investigação e contribuir para o desempenho da gestão da informação para a resolução dos casos.

Os objetivos principais do sistema são: Registrar detalhadamente crimes ocorridos em meio digital, centralizar dados de vítimas, suspeitos, contas e dispositivos utilizados, facilitar consultas e recuperação de dados visando a persistência, gerar relatórios estatísticos que apoiem órgãos de investigação e prevenção, construir uma arquitetura que permita ao mesmo tempo centralizar o armazenamento e produzir informações estratégicas consumíveis para auxiliar no combate ao crime dentro dos ambientes digitais.

3. Requisitos Funcionais

ID	Título	Descrição	Prioridade	Entradas	Saídas
RF01	Registro de ocorrência	Permite registrar novas ocorrências	Essencial	ID, data, descrição, tipo, localização, vítimas, suspeitos, logs e modus operandi	Ocorrência cadastrada
RF02	Cadastro de vítima	Permite registrar novas vítimas	Essencial	CPF, RG, Nome, Telefone, Endereço, Idade, Sexo	Lista de vítimas cadastradas
RF03	Cadastro de suspeitos/criminosos	Permite que o suspeito/criminoso possa ser registrado	Essencial	CPF, RG, Nome, Telefone, Endereço, Idade, Sexo	Lista de suspeitos cadastrados e registrados
RF04	Cadastro de dispositivos	Permite que os dispositivos envolvidos na ação possam ser registrados	Essencial	ID, Tipo, Descrição, Endereços MAC	Lista de dispositivos e provas registrados
RF05	Consulta de ocorrências	Permite que os devidos usuários possam consultar e recuperar dados das ocorrências	Essencial	Consulta e filtro da ocorrência	Lista de ocorrências que atendem à busca
RF06	Cadastro de provas e evidências	Permite que outras evidências e provas	Essencial	ID, TIpo, Descrição, conteúdo	Lista de provas e evidência cadastradas

		possam ser registradas e armazenadas no sistema			
RF07	Gerar relatórios e painéis estatísticos	Permite que os dados das ocorrências possam gerar informações estratégicas a partir de visualizações de dados	Importante	Dados referentes às ocorrências e seus relacionados	Dashboard analítico contendo informações de destaque estratégicas
RF08	Cadastro de instituição investigativa	Permite o registro de instituições de natureza policial ou pericial envolvidas nas investigações	Essencial	Nome da instituição, tipo (civil, federal, perícia técnica), endereço, cidade, unidade federativa, contato e responsável principal.	Instituições responsáveis por cada fato cadastradas.
RF09	Cadastro de entidade judicial	Permite registrar as instituições responsáveis pelas etapas processuais e judiciais, como tribunais, promotorias, varas criminais	Essencial	Nome da instituição, tipo (tribunal, promotoria, vara), jurisdição, endereço, contato e responsável jurídico vinculado.	Órgãos públicos e entidades responsáveis pelo acompanhamento jurídico e processual cadastrados

		ou ministérios públicos			
RF10	Cadastro de denúncia	Permite o cadastro de denúncias relacionadas a crimes cibernéticos, enviadas por cidadãos, empresas ou instituições ligadas ao fato	Importante	Descrição detalhada do fato, data, plataforma afetada, opção de anonimato	Formalização do registro da denúncia feita
RF11	Cadastro de agente/autoridade policial responsável	Permite cadastrar agentes, delegados, investigadores e peritos que participam das investigações.	Essencial	Nome completo, cargo, função, identificação funcional, instituição de origem, contato, nível de acesso	Funcionários investigativos cadastrados no banco
RF12	Cadastro de figura judicial responsável	Permite o registro de promotores, juízes ou procuradores associados aos processos judiciais decorrentes das	Essencial	Nome, cargo, instituição judicial, jurisdição, contato e processos vinculados.	Figuras públicas responsáveis pelo andamento processual cadastradas

		ocorrências.			
RF13	Cadastro de contas e perfis digitais	Permite cadastrar contas e perfis utilizados por vítimas ou suspeitos, vinculados às ocorrências.	Importante	Identificador da conta ou perfil, plataforma (rede social, banco digital, e-mail, carteira cripto etc.), tipo de conta (pessoal, comercial, fraudulenta), usuário associado, status (ativa, banida, rastreada)	Contas e perfis, usuários utilizados na ocorrência cadastrados.
RF14	Cadastro de documentos processuais	Permite o armazenamento e vinculação de documentos jurídicos e processuais relacionados às investigações e processos.	Importante	ID do documento, tipo (laudo, sentença, despacho, mandado), data, autor ou responsável pela emissão, descrição, instituição vinculada e arquivo digital anexado	Documentos utilizados e essenciais para o acompanhamento processual cadastrados
RF15	Consulta e Análise Institucional	Permite realizar consultas sobre instituições investigativas e judiciais, agentes envolvidos e perfis	Importante	Consulta e filtros aplicados	Lista de atores e informações relacionadas às instituições e ao processo investigativo

		digitais vinculados, com filtros por tipo, responsável, localidade e ocorrências associadas.			
RF16	Geração de relatórios investigativos e processuais	Permite gerar relatórios consolidados com informações sobre o andamento de investigações e processos.	Importante	Todas as entradas e entidades cadastradas	O sistema retornará relatórios e painéis analíticos sobre quantidade de casos sob responsabilidade de cada instituição, tempo médio de conclusão e colaborações interinstitucionais, alimentando indicadores de desempenho.

4. Requisitos de Dados

Grupo de Dados	Descrição do Grupo	Campos/Dados Principais	Origem/Quem fornece	Uso no Sistema
Ocorrência	Dados gerais da ocorrência criminosa	Entrada RF01	Administrador	Cadastro, consulta e análise
Vítima	Dados das vítimas	Entrada RF02	Próprio objeto	Cadastro e consulta
Suspeito	Dados dos suspeitos	Entrada RF03	Próprio objeto	Cadastro e consulta
Dispositivos	Dados sobre os dispositivos envolvidos no ocorrido	Entrada RF04	Administrador	Cadastro, Consulta e análise
Evidências	Dados e conteúdos das provas e evidências relacionadas com a ocorrência	Entrada RF06	Administrador	Cadastro, Consulta e análise
Instituição Investigativa	Representa órgãos policiais ou periciais que atuam na investigação de crimes cibernéticos.	Entrada RF08	Administrador	Cadastro, vinculação de ocorrências e análise de desempenho institucional

Instituiçã o Judicial	Representa tribunais, promotorias e órgãos do sistema judiciário.	Entrada RF09	Administrador	Registro e acompanhame nto de processos judiciais
Denúncia	Registro de denúncias enviadas por cidadãos ou entidades.	Entrada RF10	Usuário	Cadastro, consulta e triagem das denúncias
Agente/A utoridade policial	Agentes, delegados e peritos que atuam nas investigações.	Entrada RF11	Administrador	Cadastro, controle, histórico e indicadores
Figura Judicial	Promotores, juízes ou procuradores associados a processos judiciais.	Entrada RF12	Administrador	Cadastro, controle, histórico e indicadores
Conta/pe rfil digital	Representa contas e perfis utilizados por	Entrada RF13	Responsável investigativo	Cadastro, consulta, Rastreamento digital e

	vítimas ou criminosos.			vinculação com crimes
Documento processual	Conjunto de documentos oficiais e jurídicos relacionados a investigações e processos.	Entrada RF14	Responsável judicial	Cadastro e consulta documental

5. Critérios de Aceitação

- O sistema deve permitir todas as funcionalidades previstas nos requisitos funcionais.
- Todos os dados essenciais devem ser gerenciados conforme especificado na tabela de requisitos de dados.
- Apenas usuários autorizados poderão registrar, editar ou excluir ocorrências.
- O vínculo entre ocorrência, vítimas, suspeitos e dispositivos deve ser garantido conforme o processo ocorrido na vida real.
- O sistema deve permitir o registro e gerenciamento das instituições, assegurando que sejam devidamente identificadas, documentadas e vinculadas às ocorrências correspondentes.
- Os responsáveis devem estar associados a suas respectivas instituições e às ocorrências sob sua supervisão.
- Todos os documentos associados devem ser armazenados de forma segura e vinculados aos casos, preservando a cadeia de custódia digital e garantindo acesso apenas a usuários autorizados.

6. Texto detalhado

O SIPACC contará com um conjunto de funcionalidades essenciais voltadas ao registro, consulta e análise de crimes cibernéticos.

O sistema permitirá, em primeiro lugar, o registro de ocorrências (RF01), possibilitando que cada crime seja documentado de forma estruturada e consistente. Ao registrar uma ocorrência, serão armazenados dados como o identificador único, a data e hora do ocorrido, a descrição detalhada do evento, o tipo de crime (fraude bancária, phishing, invasão de sistema, entre outros), além da localização associada, seja ela física ou digital, como um endereço de IP ou região aproximada. Também será possível vincular vítimas e suspeitos ao registro, armazenar logs técnicos relevantes e descrever o modus operandi utilizado pelo criminoso.

Além disso, o sistema permitirá o cadastro de vítimas (RF02), no qual poderão ser registrados dados pessoais como CPF, RG, nome completo, telefone, endereço, idade e sexo. Esses dados são fundamentais para associar uma ou mais vítimas a uma ocorrência, garantindo que exista uma identificação adequada e que se possa futuramente analisar padrões relacionados a perfis de vítimas.

De forma semelhante, o SIPACC oferecerá o cadastro de suspeitos ou criminosos (RF03). Para cada suspeito identificado, será possível inserir informações como CPF, RG, nome, possíveis apelidos, idade, sexo, endereço e formas de contato. Esse registro poderá ser vinculado a diversas ocorrências, permitindo a análise de reincidência e identificação de possíveis conexões entre crimes.

Outro recurso relevante é o cadastro de dispositivos (RF04), em que serão armazenados os dados dos equipamentos envolvidos nos crimes, sejam eles utilizados por vítimas ou suspeitos. Esses registros incluirão informações como o identificador do dispositivo, tipo (computador, smartphone, servidor, roteador etc.), uma descrição detalhada de suas características técnicas e os endereços MAC ou outros identificadores únicos. Esse requisito é importante para rastrear os meios pelos quais os crimes foram praticados, permitindo inclusive a associação de um mesmo dispositivo a diferentes ocorrências.

No que se refere à investigação e recuperação de informações, o sistema contará com a funcionalidade de consulta de ocorrências (RF05). Esse recurso permitirá a realização de buscas por meio de filtros como tipo de crime, intervalo de datas, localidade, vítima ou suspeito envolvido, além de dispositivos registrados. Como resultado, o sistema retornará listas de ocorrências que correspondam aos critérios definidos, fornecendo acesso aos detalhes de cada registro.

Complementarmente, o SIPACC possibilitará o cadastro de provas e evidências (RF06), garantindo que conteúdos relacionados aos crimes digitais possam ser armazenados. Entre os tipos de evidências aceitos estão prints de tela, e-mails, mensagens, documentos digitais ou mesmo arquivos de log. Cada evidência contará com um identificador único, uma descrição detalhada, a categorização por tipo e o conteúdo armazenado, que poderá ser em forma de arquivo anexado ou texto. Essa funcionalidade assegura a persistência de informações relevantes para o processo investigativo e judicial.

No que se refere aos requisitos de dados, o sistema organizará suas informações em diferentes grupos de entidades, garantindo a consistência e a rastreabilidade das ocorrências.

O primeiro grupo é o de Ocorrência, que reúne os dados gerais sobre cada crime registrado. Esses dados são provenientes do processo de registro de ocorrência (RF01) e incluem informações como o identificador único, a descrição do crime, o tipo, a data, a hora, a localização, além da vinculação com vítimas, suspeitos e dispositivos. Esse grupo serve como núcleo do sistema, centralizando as informações que serão consultadas e analisadas.

O grupo de Vítima reúne os dados pessoais de cada pessoa envolvida como alvo dos crimes cibernéticos. Os campos principais incluem nome, CPF, RG, endereço, telefone, idade e sexo. Esses dados são informados no momento do cadastro da vítima (RF02) e permitem consultas e análises que identifiquem perfis de maior exposição a determinados crimes.

De forma paralela, o grupo de Suspeito contém as informações relativas às pessoas investigadas ou identificadas como possíveis autores dos crimes. Assim como no caso das vítimas, os dados incluem nome, CPF, RG, telefone, endereço, idade e sexo, registrados no cadastro de suspeitos (RF03). Esse grupo é essencial para a investigação, pois permite correlacionar indivíduos com múltiplas ocorrências.

Outro grupo importante é o de Dispositivos, que armazena dados técnicos sobre os equipamentos relacionados às ocorrências, sejam eles de vítimas ou de suspeitos. Os campos contemplam identificadores do dispositivo, tipo, descrição e endereços MAC, conforme registrado no requisito funcional RF04. Essas informações são fundamentais para a análise técnica e rastreamento digital.

Por fim, há o grupo de Evidências, que compreende os dados associados às provas coletadas durante a investigação. Incluem-se aqui o identificador da evidência, o tipo, a descrição e o conteúdo em si (texto ou arquivo anexado). Esse grupo resulta do cadastro de evidências (RF06) e desempenha papel crucial na preservação da cadeia de custódia e no suporte às etapas investigativas.

Dessa forma, os requisitos funcionais e de dados do SIPACC garantem que o sistema não apenas permita o registro e consulta das ocorrências de crimes cibernéticos, mas também assegure a integridade, a centralização e a análise estruturada de todas as informações necessárias ao combate desse tipo de criminalidade, possibilitando posteriormente análises mais detalhadas e estratégias que venham auxiliar a tomada de decisões dentro dos grupos policiais.

O SIPACC abrange também o registro e gestão de instituições investigativas e judiciais, permitindo que cada ocorrência seja vinculada a uma organização responsável, seja ela policial, pericial ou jurídica. Essa integração institucional viabiliza uma visão completa do ciclo do crime cibernético, desde o momento da denúncia até o julgamento final, fortalecendo a transparência e a rastreabilidade das ações realizadas.

O módulo de denúncias permitirá que cidadãos, empresas ou organizações relatem crimes cibernéticos de forma estruturada, podendo optar por preservar sua identidade. As denúncias armazenadas servirão como fonte primária de dados para a geração de novas ocorrências e contribuirão para o monitoramento preventivo de atividades suspeitas.

O cadastro de agentes e autoridades policiais responsáveis assegura o controle das investigações, vinculando cada ocorrência a um ou mais profissionais designados. Essa associação possibilita mensurar a carga de trabalho, acompanhar o progresso de casos específicos e garantir que cada etapa da investigação tenha um responsável devidamente identificado.

Da mesma forma, o registro de figuras judiciais responsáveis, como juízes, promotores e procuradores, permitirá mapear os atores jurídicos envolvidos em cada processo e seus desdobramentos. Essa rastreabilidade viabiliza análises sobre a tramitação e o tempo médio de resposta judicial em casos de crimes cibernéticos.

O sistema também incorporará o gerenciamento de contas e perfis digitais relacionados às ocorrências, permitindo identificar e associar perfis fraudulentos, contas bancárias, e-mails e perfis em redes sociais utilizados em práticas criminosas. Essa camada de informação enriquece o potencial de análise e correlação entre diferentes casos e criminosos, além de contribuir com o rastreamento técnico das atividades ilícitas.

Por fim, o SIPACC incluirá o cadastro e controle de documentos processuais e jurídicos, assegurando que laudos periciais, mandados, despachos, sentenças e relatórios técnicos sejam armazenados com segurança e vinculados às investigações ou processos correspondentes. Essa funcionalidade garante a preservação da cadeia de custódia digital, fundamental para a integridade das provas e a legitimidade das decisões judiciais.

Essas novas entidades e requisitos fortalecem o papel do SIPACC como um sistema de gestão e inteligência integrada voltado para o combate à criminalidade digital, ampliando sua aplicabilidade prática e tornando-o uma plataforma completa para investigação, análise e acompanhamento processual de crimes cibernéticos.

Volume de trabalho

Ação	Tipo	Informação Manipulada	Frequência Estimada	Prioridade
Registrar uma nova ocorrência	Escrita	ID, descrição, data, tipo, localização, vítimas, suspeitos, modus operandi	50 por dia	Alto
Consultar ocorrências registradas	Leitura	ID da ocorrência, descrição, vítimas, suspeitos, dispositivos, provas	1.000 por dia	Alto
Cadastrar nova vítima	Escrita	Nome, CPF, endereço, idade, sexo, contato	100 por dia	Médio

Cadastrar novo suspeito	Escrita	Nome, CPF, endereço, sexo, idade, telefone	80 por dia	Médio
Registrar dispositivos vinculados	Escrita	Tipo, identificador, descrição técnica, endereço MAC	150 por dia	Médio
Inserir provas e evidências digitais	Escrita	Tipo, descrição, conteúdo, arquivo	200 por dia	Alto
Consultar provas e evidências	Leitura	ID, tipo, conteúdo, ocorrência associada	500 por dia	Médio
Gerar relatórios e dashboards analíticos	Leitura	Ocorrências, dispositivos, vítimas, suspeitos, padrões	20 por hora	Alto
Registrar nova instituição investigativa	Escrita	Nome, tipo, cidade, contato, responsável	5 por dia	Médio
Registrar instituição judicial	Escrita	Nome, tipo, jurisdição, endereço, contato	3 por dia	Médio
Registrar nova denúncia	Escrita	Descrição, data, tipo de crime, anonimato, anexos	80 por dia	Alto
Triar e converter denúncias em ocorrências	Leitura/Escrita	ID da denúncia, status, ocorrência gerada	40 por dia	Alto

Cadastrar agente/autoridade policial	Escrita	Nome, cargo, identificação funcional, instituição	10 por dia	Médio
Cadastrar figura judicial responsável	Escrita	Nome, cargo, instituição, jurisdição, processos	5 por dia	Médio
Registrar contas e perfis digitais	Escrita	Identificador, plataforma, tipo, status, vínculo	100 por dia	Alto
Consultar contas e perfis digitais	Leitura	ID, plataforma, tipo, ocorrência vinculada	400 por dia	Médio
Registrar documentos processuais	Escrita	Tipo, descrição, data, autor, arquivo digital	30 por dia	Alto
Consultar documentos processuais	Leitura	Tipo, data, descrição, instituição vinculada	200 por dia	Médio
Consultar e analisar instituições e responsáveis	Leitura	Instituições, agentes, ocorrências vinculadas	100 por dia	Médio
Gerar relatórios investigativos e processuais	Leitura	Ocorrências, instituições, tempo de resposta, responsáveis	10 por hora	Alto

Mapeamento dos relacionamentos