

# Suporte IronFence

## Plataforma de Processamento de Dados e Inteligência

### Definição

A plataforma de processamento de dados e inteligência deve ser uma solução abrangente e altamente especializada para atender às demandas crescentes de correlacionamento, estruturação, processamento e geração de insights em diferentes áreas da administração pública. A plataforma deve combinar tecnologias avançadas de inteligência artificial (IA), big data analytics e machine learning para transformar dados brutos, provenientes de múltiplas fontes heterogêneas, em informações acionáveis que suportam decisões estratégicas e operacionais.

A plataforma deve ser composta por módulos especializados, cada um projetado para executar funções específicas dentro de um ecossistema integrado. Essa modularidade deve permitir que a plataforma seja altamente flexível, escalável e adaptável às necessidades de diferentes áreas da administração pública ou organizações. A interação entre os módulos deve ser coordenada por uma camada central de orquestração, que garanta a comunicação eficiente, o compartilhamento de dados e a execução coordenada das tarefas.

A plataforma deve ser composta, no mínimo, pelos seguintes módulos:

1. Módulo de Inteligência Cibernética - MAP
2. Módulo de Inteligência de Dados - Dataverso Investigação
3. Módulo de Gestão do Conhecimento - Dataverso Gestão
4. Módulo de Inteligência de Controle - Dataverso Controle
5. Módulo de Inteligência de Análise de Cenários de Interesse - ChatGuard
6. Módulo de Inteligência de Ocupação e Presença em Locais de Interesse - Tracker
7. Módulo de Comparação de Faces, Reconhecimento Facial, Reconhecimento Veicular e de Comportamentos - Horus

Cada módulo deve operar como uma unidade funcional autônoma, mas todos devem estar interconectados por meio de APIs (Interfaces de Programação de Aplicativos) padronizadas e protocolos de comunicação seguros. Essa arquitetura modular deve permitir que os módulos sejam ativados, desativados ou atualizados de forma independente, sem comprometer o funcionamento do sistema como um todo.

O sistema deve ser capaz de integrar módulos especializados de forma eficiente, garantindo que tanto os dados de login quanto os dados operacionais fluam de maneira segura, consistente e escalável. A interação entre os módulos deve ser projetada para atender às demandas operacionais e estratégicas da administração pública, com foco em desempenho, segurança e flexibilidade. Estes requisitos técnicos visam garantir que a solução seja robusta, adaptável e capaz de suportar cenários complexos de processamento e análise de dados.

## **CARACTERÍSTICAS DO FUNCIONAMENTO E DA INTERAÇÃO ENTRE OS MÓDULOS**

Os módulos especializados deverão ser projetados para operar de forma integrada e colaborativa, assegurando a execução eficiente de processos complexos. A integração e a comunicação entre os módulos são essenciais para garantir a consistência, segurança e o desempenho do sistema como um todo. As características técnicas relacionadas ao funcionamento e à interação entre módulos são as seguintes:

### **1. Arquitetura Modular Integrada**

O sistema deverá possuir uma arquitetura modular, onde cada módulo opera com autonomia funcional, porém plenamente integrado ao restante do ecossistema. A infraestrutura centralizada garantirá comunicação fluida, segura e padronizada entre módulos, independentemente da função específica de cada um.

### **2. Comunicação Unificada entre Módulos**

Os módulos deverão comunicar-se utilizando interfaces padronizadas, empregando protocolos abertos como RESTful APIs e formatos de troca de dados JSON ou XML, garantindo interoperabilidade, compatibilidade e facilidade de integração.

O sistema deverá suportar comunicação síncrona para processos críticos que exijam respostas imediatas, bem como comunicação assíncrona para cenários onde a latência não comprometa o resultado final.

Dados de autenticação (login) e dados operacionais deverão ser compartilhados com segurança e consistência entre os módulos, evitando redundância ou perda de informações.

### **3. Autenticação e Autorização Centralizada**

Será implementado um mecanismo centralizado de autenticação e autorização baseado em padrões como JWT, OAuth 2.0 e OpenID Connect, permitindo autenticação única (Single Sign-On – SSO). As credenciais de acesso e as permissões serão reconhecidas de forma consistente por todos os módulos, evitando falhas e inconsistências.

O controle de acesso deverá ser granular, permitindo a aplicação de políticas específicas de autorização em função dos perfis dos usuários.

### **4. Orquestração Centralizada**

O sistema deverá possuir uma camada centralizada de orquestração, responsável por coordenar as atividades dos módulos, garantindo execução eficiente e ordenada dos fluxos de trabalho.

Essa camada deverá gerenciar pipelines de processamento, distribuir tarefas entre os módulos e monitorar o status de cada execução.

Deverá ser implementada utilizando tecnologias que permitam escalabilidade horizontal e alta disponibilidade, tais como Kubernetes ou frameworks equivalentes.

### **5. Sincronização e Consistência de Dados**

Os módulos deverão compartilhar dados de forma síncrona ou assíncrona, assegurando consistência, integridade e atualização em tempo real. Um mecanismo robusto de sincronização de dados deverá ser utilizado, incluindo técnicas de controle de transações, bloqueios distribuídos ou filas de processamento em cenários de alta concorrência.

## 6. **Processamento Distribuído**

O sistema deverá ser capaz de distribuir o processamento de dados entre módulos, otimizando recursos computacionais para alto desempenho em cenários de grande demanda.

Deverá suportar processamento paralelo, utilizando frameworks reconhecidos como Apache Spark ou tecnologias equivalentes, abrangendo tanto processamento em lote (*batch processing*) quanto processamento em tempo real (*streaming*).

## 7. **Monitoramento e Autocorreção**

O sistema deverá possuir monitoramento contínuo, capaz de identificar falhas ou gargalos em tempo real. Deverá implementar funcionalidades de autocorreção para ajuste automático em resposta a eventos inesperados, como sobrecarga de processamento ou falha de componentes específicos.

As métricas de desempenho deverão ser registradas e disponibilizadas para análises e otimização contínua.

## 8. **Segurança na Interação**

A comunicação entre módulos deverá ser protegida por criptografia robusta, utilizando protocolos como TLS 1.3 para garantir a confidencialidade e integridade dos dados trocados.

Todas as interações deverão ser registradas em logs detalhados, garantindo capacidade de auditoria e análise forense sempre que necessário.

## 9. **Flexibilidade e Adaptabilidade**

A arquitetura deverá ser suficientemente flexível para permitir reconfiguração dinâmica dos fluxos de trabalho e pipelines de processamento, atendendo necessidades variadas da administração pública.

Cada módulo deverá aceitar múltiplas fontes de entrada e fornecer saídas facilmente consumíveis por outros módulos ou sistemas externos. A plataforma deverá permitir inclusão de novos módulos e funcionalidades sem impactos negativos aos módulos já existentes.

## 10. **Resiliência e Tolerância a Falhas**

O sistema deverá ser resiliente e projetado de forma que falhas em um módulo específico não comprometam a operação global. Deverá possuir mecanismos automáticos de failover e redundância operacional.

Dados processados deverão ser armazenados com replicação ou backups incrementais, garantindo proteção contra perdas e possibilitando recuperação rápida.

## **ESPECIFICAÇÕES GERAIS**

1. A plataforma deverá funcionar como um sistema unificado e integrado, com módulos harmonizados entre si. Será obrigatório um sistema de autenticação e autorização único e centralizado, oferecendo experiência fluida aos usuários ao acessarem diferentes subsistemas. A identidade visual, UX e UI deverão ser consistentes entre todas as

aplicações da plataforma, evitando a percepção de um conjunto de soluções isoladas.

2. Deverá ser possível integrar múltiplas fontes de dados, incluindo bancos governamentais, privados, fontes abertas, bases proprietárias e informações coletadas da deep e dark web, contemplando dados estruturados, semiestruturados e não estruturados, com flexibilidade e amplitude.
3. A plataforma utilizará inteligência artificial em múltiplos níveis, tais como reconhecimento de padrões complexos, transcrição automática de textos provenientes de imagens, áudio e vídeo, enriquecimento automático de entidades (pessoas, locais, organizações e eventos) e processamento avançado de linguagem natural (LLM – Large Language Models). Essas funcionalidades permitirão realizar análises detalhadas, classificações inteligentes, geração de resumos automáticos e respostas contextuais.
4. A solução deverá ser capaz de identificar padrões ocultos nos dados, emitir alertas automatizados em tempo real e gerar relatórios detalhados e customizáveis, facilitando decisões estratégicas e operacionais.
5. Todas as ações realizadas deverão ser registradas e rastreadas com atributos que atendam padrões de prova forense, garantindo total transparência, auditabilidade e confiabilidade dos dados processados. Os relatórios deverão ser exportáveis em formatos padronizados como PDF, CSV ou Excel.
6. A plataforma incluirá ainda módulo específico para gestão de equipes, permitindo cadastro estruturado e definição granular de níveis de acesso e permissões específicas a cada módulo, garantindo controle adequado, segurança e privacidade das informações.

### **TREINAMENTO, SUPORTE TÉCNICO E MANUTENÇÃO EVOLUTIVA**

Além dos requisitos técnicos relacionados ao funcionamento e interação entre os módulos, é essencial que o sistema inclua suporte para capacitação dos usuários, assistência técnica contínua e mecanismos de manutenção evolutiva. Esses elementos são fundamentais para garantir a operacionalidade, sustentabilidade e otimização do sistema ao longo do tempo. Abaixo estão detalhadas as necessidades específicas:

7. Treinamento
  - a. Capacitação dos Usuários: a IronFence oferece treinamento estruturado para todos os usuários finais, desde operadores até gestores responsáveis pela administração do sistema.
  - b. Formato: o treinamento será realizado em formato presencial ou remoto, com materiais didáticos claros e práticos, como apostilas, vídeos tutoriais e laboratórios práticos.
  - c. Conteúdo: o conteúdo do treinamento abrange:
    - i. Operação básica e avançada do sistema, incluindo a utilização de cada módulo e suas funcionalidades específicas.

- ii. Integração e comunicação entre os módulos, com foco em fluxos de trabalho típicos da administração pública.
  - iii. Configuração inicial e personalização de pipelines e workflows.
  - iv. Práticas recomendadas para segurança e gestão de dados.
- d. Duração: o treinamento tem duração suficiente para garantir que os usuários estejam aptos a operar o sistema de forma eficiente, com sessões divididas por níveis de complexidade (básico, intermediário e avançado).
- e. Acompanhamento Pós-Treinamento: após a conclusão do treinamento, a IronFence disponibilizará suporte adicional para esclarecer dúvidas e orientar os usuários durante a fase inicial de uso.

#### 8. Suporte Técnico

- a. Disponibilidade: suporte técnico 24h, todos os dias da semana (24x7), garantindo assistência imediata em caso de falhas críticas ou problemas operacionais.
- b. Canais de Atendimento: disponível por meio de múltiplos canais, como telefone, e-mail, chat online ou portal de atendimento, permitindo que os usuários escolham a forma mais conveniente de contato.
- c. Tempos de Resposta: tempos máximos de resposta para diferentes níveis de severidade, com prioridade para incidentes que impactem diretamente a operação do sistema.
- d. Equipe Especializada: a equipe de suporte é composta por profissionais capacitados, com conhecimento técnico profundo sobre o sistema e suas integrações.
- e. Registro de Incidentes: todos os incidentes são registrados e acompanhados em um sistema de ticketing, permitindo o monitoramento do progresso e a geração de relatórios históricos.

#### 9. Manutenção Evolutiva

- a. Atualizações e Melhorias Contínuas: a IronFence garante que o sistema receba atualizações regulares para incorporar novas funcionalidades, melhorias de desempenho e correções de vulnerabilidades.
- b. Ciclo de Atualizações: as atualizações são planejadas e comunicadas com antecedência, minimizando o impacto nas operações diárias.
- c. Compatibilidade Retroativa: todas as atualizações garantem compatibilidade com versões anteriores do sistema, evitando a necessidade de reconfigurações extensivas ou perda de dados.
- d. Customização: o sistema permite ajustes e personalizações para atender às mudanças nas demandas da administração pública, incluindo a criação de novos módulos ou a adaptação dos existentes.
- e. Monitoramento Proativo: serão implementados mecanismos de monitoramento proativo para identificar possíveis áreas de melhoria no sistema, antecipando necessidades antes que se tornem problemas críticos.

- f. Feedback dos Usuários: será estabelecido um canal formal para coleta de feedback dos usuários, permitindo que sugestões e demandas sejam avaliadas e incorporadas ao processo de manutenção evolutiva.
- g. Garantia de Longevidade: o sistema permanece viável e competitivo ao longo do tempo, alinhando-se às melhores práticas do mercado e às tendências tecnológicas emergentes.

## **ESPECIFICAÇÕES DOS SERVIÇOS DE SUPORTE TÉCNICO**

### DESCRIÇÃO GERAL

- 10. O Serviço de Suporte Técnico da solução adquirida deverá ser provido pela IronFence durante todo o prazo de vigência do contrato.
- 11. O serviço especificado neste documento engloba assistência intelectual para a operação e administração da solução, bem como as manutenções preventiva, corretiva e adaptativa da solução como um todo, englobando seu hardware e software.
- 12. Todas as despesas dos recursos necessários para a execução dos serviços de suporte, tais como deslocamento e hospedagem dos profissionais envolvidos na prestação do serviço, serão custeadas e executadas pela IronFence.
- 13. Caso surjam custos operacionais decorrentes da operação e do funcionamento da solução, ainda que não abrangidos neste documento, serão estes de encargo exclusivo da IronFence devendo ser adimplidos sem a possibilidade do repasse de valores ou cobranças adicionais.
- 14. Dada a volatilidade dos serviços, no caso de indisponibilidade comprovada de algum dos mesmos, a IronFence poderá, a qualquer momento, indicar outro serviço equivalente para substituí-lo, bem como removê-lo caso não haja equivalência.

## **CONDIÇÕES DE EXECUÇÃO E GESTÃO DO SERVIÇO**

### Chamados de Suporte Técnico

- 15. Os chamados de suporte técnico representam a solicitação formal de serviços de suporte à IronFence e devem ser atendidos de acordo com os critérios e parâmetros estabelecidos para execução dos serviços.
- 16. A IronFence deverá prover a manutenção mensal para a solução adquirida pelo CONTRATANTE no prazo de vigência deste contrato, conforme as especificações seguintes:
  - a. retirada de dúvidas quanto à operação e administração da solução;
  - b. resolução de problemas de software e de hardware na ferramenta;
  - c. garantia do correto desempenho das funcionalidades adquiridas da solução;
  - d. correção de falhas de software (bugs), com fornecimento de versões atualizadas;
  - e. atualização de versões de módulos de software (updates) disponibilizados;
  - f. correções de software, aperfeiçoamentos, modificações e atualizações dos artefatos necessários para renovação do conteúdo dos indicadores;

- g. contratação de infraestruturas de serviços e subscrições para consumo de dados, tais como:
  - i. Licenças de software e suas respectivas atualizações;
  - ii. Contratação e manutenção de bases de dados externas;
  - iii. Contratação e gerenciamento de servidores virtuais, VPNs e proxies;
  - iv. Superação de mecanismos de captcha ou filtros de rede;
  - v. Licenças e taxas para consumo de dados via API ou RESTful Web Services;
  - vi. Custos associados ao armazenamento seguro dos dados coletados (nuvem ou data center próprio);
  - vii. Aquisição ou subscrição de ferramentas especializadas para extração de dados (web scraping);
  - viii. Despesas relacionadas à utilização de infraestrutura para monitoramento de fontes abertas, deep e dark web;
  - ix. Custos associados à criptografia e segurança das conexões e das bases de dados utilizadas para armazenamento;
  - x. Contratação de serviços adicionais de inteligência de fontes externas especializadas;
  - xi. Serviços de processamento em tempo real (streaming) e processamento de grandes volumes de dados (big data);
  - xii. Gastos relacionados ao monitoramento contínuo e automação de rotinas de coleta (robôs/crawlers);
  - xiii. Outras despesas provenientes da execução do serviço de coleta
- h. O chamado deve conter uma descrição detalhada do problema, a indicação dos itens de configuração afetados e o nome do contato do CONTRATANTE responsável pelo acompanhamento do serviço.
- i. O CONTRATANTE poderá ainda anexar ao chamado documentos ou imagens que auxiliem na identificação do problema, sugerir o perfil profissional adequado para execução do serviço e, se for o caso, agendar data e hora para o atendimento.

#### Abertura e Acompanhamento dos Chamados

17. Os chamados de Suporte Técnico poderão ser iniciados e acompanhados por meio dos seguintes canais de comunicação:
- a. Portal de Suporte – portal em ambiente web a ser fornecido e mantido pela IronFence;
  - b. Contato telefônico – número de discagem gratuita (0800) ou um número local no Brasil, provido pela IronFence; ou
  - c. E-mail – endereço de e-mail específico para este contrato, provido pela IronFence.
  - d. WhatsApp – atendimento via aplicativo WhatsApp, com número exclusivo fornecido pela IronFence, para abertura, acompanhamento e atualização dos chamados.

- e. Os meios de comunicação descritos neste item deverão ser disponibilizados ao CONTRATANTE em até 15 (quinze) dias após a assinatura do contrato.
- f. A IronFence irá fornecer, com periodicidade mensal, relatórios a respeito das atividades de suporte demandadas, com informações sobre os chamados, SLA (Service Level Agreement) de atendimento e demais dados pertinentes.

#### Disponibilidade e Modelo de Atendimento

- 18. Tendo em vista que a ferramenta irá operar em alta disponibilidade, com provimento contínuo e ininterrupto, o serviço de Suporte também irá operar de forma contínua e ininterrupta, com atendimento 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana.
- 19. O atendimento poderá ser prestado de forma remota ou presencial.
- 20. A IronFence fornecerá um manual em português que detalha a utilização do sistema e seus recursos básicos e avançados, podendo o mesmo ser disponibilizado em formato digital.

#### Classificação de Severidade e Prazos

- 21. Os chamados de suporte técnico serão classificados por severidade, dependendo do impacto que o problema a ser resolvido possa causar ao ambiente computacional do CONTRATANTE, sendo possíveis os seguintes níveis de severidade:
  - a. URGENTE: chamado para restabelecer um serviço que esteja parado. O tempo de resposta por parte da IronFence aos chamados com esse nível de severidade deverá ser, no máximo, de 2 (duas) horas após a abertura do chamado realizado pelo CONTRATANTE, sendo que o prazo de solução desses chamados deverá ser de, no máximo, 3 (três) horas para a resolução do problema.
  - b. ALTA: chamado para restabelecer serviço que não esteja operando corretamente ou que apresente problema de desempenho. O tempo de resposta por parte da IronFence aos chamados com esse nível de severidade deverá ser, no máximo, de 6 (seis) horas após a abertura do chamado realizado pelo CONTRATANTE, e o prazo para sua solução deverá ser de, no máximo, 6 (seis) horas.
  - c. MÉDIA: chamado para resolução de erros que não causem interrupção dos serviços da solução. O tempo de resposta por parte da IronFence aos chamados com esse nível de severidade deverá ser, no máximo, de 24 (vinte e quatro) horas após a abertura do chamado realizado pelo CONTRATANTE, e o prazo para sua solução deverá ser de, no máximo, 12 (doze) horas.
  - d. BAIXA: chamado para esclarecimento de dúvidas referentes a possíveis problemas com a solução, assim como aplicação de melhorias e correções. O tempo de resposta por parte da IronFence aos chamados com esse nível de severidade deverá ser, no máximo, de 48 (quarenta e oito) horas após a sua abertura pelo CONTRATANTE e o prazo para sua solução deverá ser de, no máximo, 24 (vinte e quatro) horas.

22. Caso a IronFence não cumpra com os prazos de resposta aos chamados estipulados neste item, pode sofrer multa de 10% (dez por cento) do valor do serviço contratado, para cada chamado em que o prazo contratual não for cumprido. O valor da multa deverá ser abatido integralmente na mensalidade a ser paga à IronFence no mês posterior ao ocorrido, preferencialmente.
23. O nível de severidade do chamado pode ser posteriormente alterado conforme avaliação da equipe técnica da IronFence, em comum acordo com o CONTRATANTE.
24. O prazo de solução dos chamados poderá ser prorrogado, a critério exclusivo do CONTRATANTE, caso a IronFence apresente, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que fogem ao controle da IronFence e impedem a solução do chamado no tempo estabelecido.
25. Após uma ocorrência de severidade URGENTE, a IronFence deve fornecer relatório a respeito do atendimento e solução empreendidas para o chamado, medidas preventivas para evitar a recorrência do problema e demais dados pertinentes.

## **GLOSSÁRIO**

### **A**

#### **API (Application Programming Interface)**

Interface que permite a comunicação entre diferentes softwares, permitindo o compartilhamento de dados e funcionalidades. Exemplo: RESTful APIs são interfaces baseadas em padrões web que permitem integração entre sistemas.

#### **Autenticação**

Processo de verificar a identidade de um usuário ou sistema antes de conceder acesso a recursos ou informações. Pode envolver login com senha, tokens ou biometria.

#### **Autorização**

Processo de definir e controlar quais ações um usuário autenticado pode realizar dentro de um sistema. Por exemplo, quem pode visualizar relatórios, editar dados ou excluir registros.

### **B**

#### **Batch Processing (Processamento em Lote)**

Método de processamento de grandes volumes de dados coletivamente, em vez de individualmente ou em tempo real. É eficiente para análises históricas ou rotinas noturnas.

#### **Big Data**

Termo usado para descrever conjuntos de dados extremamente grandes e complexos que exigem tecnologias especiais para armazenamento, gerenciamento e análise.

## C

### Deep Web

Parte da internet que não é indexada pelos motores de busca tradicionais (como Google). Inclui páginas protegidas por login, bases de dados privadas e conteúdos dinâmicos.

### Dark Web

Subset da Deep Web acessível apenas por redes anônimas (como Tor) e frequentemente associada ao uso ilegal de serviços e informações.

### Desempenho

Capacidade de um sistema ou componente em operar com eficiência sob carga, medido por métricas como velocidade, tempo de resposta e capacidade de processamento.

### Dados Estruturados

Dados organizados em formato tabular ou predefinido, como planilhas ou bancos de dados relacionais.

### Dados Semi-Estruturados

Dados que possuem alguma estrutura, mas não seguem um esquema rígido, como XML ou JSON.

### Dados Não Estruturados

Dados sem formatação padronizada, como textos livres, imagens, vídeos e áudios.

## E

### Escalabilidade

Capacidade de um sistema de aumentar ou diminuir sua capacidade de processamento conforme necessário, mantendo desempenho adequado.

### Extração de Dados (Data Scraping / Web Scraping)

Técnica automatizada de coleta de informações disponíveis na web, muitas vezes usada para obter dados públicos de sites.

## F

### Failover (Redundância e Recuperação)

Processo automático de alternância para um sistema ou componente reserva quando ocorre uma falha no principal, garantindo continuidade operacional.

## G

### Governança de Dados

Conjunto de políticas, práticas e controles que asseguram o uso correto, seguro e ético dos dados em uma organização.

H

Horizonte Tecnológico

Visão estratégica sobre tendências e inovações tecnológicas emergentes que podem impactar a evolução de um produto ou serviço.

I

Inteligência Artificial (IA)

Tecnologia que permite que máquinas realizem tarefas normalmente associadas à inteligência humana, como reconhecimento de padrões, tomada de decisão e aprendizado.

Integração

Capacidade de conectar e sincronizar diferentes módulos ou sistemas para trabalharem juntos de forma coerente.

Interoperabilidade

Capacidade de diferentes sistemas ou componentes trocarem informações e funcionarem em conjunto, mesmo que sejam de fabricantes distintos.

K

Kubernetes

Plataforma de código aberto usada para automatizar a implantação, escalabilidade e gestão de aplicações em containers (ambientes isolados de execução de software).

L

LLM (Large Language Model)

Modelo avançado de IA capaz de entender e gerar linguagem natural, utilizado em assistentes virtuais, resumos automáticos, traduções e mais.

Licença de Software

Autorização legal concedida pelo desenvolvedor ou fornecedor que permite o uso de um programa de computador sob certas condições.

M

Machine Learning

Subconjunto da inteligência artificial que permite a um sistema aprender com dados e melhorar seu desempenho ao longo do tempo, sem ser explicitamente programado.

### Manutenção Evolutiva

Atualizações e melhorias feitas em um sistema para adaptá-lo a novas necessidades ou incorporar funcionalidades adicionais.

### Monitoramento Proativo

Acompanhamento constante do desempenho e saúde de um sistema com o objetivo de detectar e resolver problemas antes que afetem os usuários.

### O

#### Orquestração

Coordenação automatizada de múltiplos componentes ou serviços para executar fluxos de trabalho complexos de maneira integrada e eficiente.

### OAuth 2.0

Protocolo de autorização usado para permitir que aplicativos acessem recursos em nome de um usuário sem compartilhar credenciais.

### OpenID Connect

Camada de autenticação construída sobre OAuth 2.0, usada para verificar a identidade de usuários em aplicações.

### P

#### Processamento Distribuído

Uso de múltiplos computadores ou servidores para dividir e executar tarefas simultaneamente, aumentando a velocidade e a eficiência.

### Processamento em Tempo Real (Streaming)

Análise ou manipulação de dados assim que eles são gerados, permitindo reações imediatas.

### Prova Forense

Coleção de evidências digitais com validade jurídica, geralmente obtidas com rastros auditáveis e registros detalhados.

### R

#### Reconhecimento Facial

Tecnologia que identifica ou verifica pessoas com base em características faciais captadas em imagens ou vídeos.

### Redundância

Cópia de segurança de dados ou sistemas, criada para garantir disponibilidade em caso de falha.

### Registro de Incidentes

Sistema de controle onde todos os eventos relevantes (falhas, alterações, acessos) são documentados para auditoria e análise.

### Replicação de Dados

Cópia de dados entre diferentes locais ou servidores para garantir consistência, segurança e disponibilidade.

## S

### Segurança da Informação

Práticas e tecnologias destinadas a proteger dados contra acesso não autorizado, perdas ou corrupção.

### SLA (Service Level Agreement)

Acordo contratual entre cliente e fornecedor que define níveis esperados de serviço, como disponibilidade, tempos de resposta e qualidade.

### Streaming

Transmissão contínua de dados ou mídia em tempo real, sem necessidade de download completo antes do uso.

### SSO (Single Sign-On)

Sistema que permite ao usuário acessar múltiplos sistemas com uma única credencial.

### Sincronização de Dados

Processo de manter cópias de dados atualizadas entre diferentes fontes ou dispositivos.

### Sistema Modular

Arquitetura de software composta por partes independentes (módulos), cada uma com funções específicas, mas interligadas.

### Sistema Unificado

Plataforma que opera como uma única solução, embora seja composta por vários módulos integrados.

## T

### TLS (Transport Layer Security)

Protocolo de segurança usado para criptografar comunicações entre dispositivos e servidores, garantindo confidencialidade e integridade.

## Treinamento

Atividade educacional voltada à capacitação de usuários finais para o uso eficaz de ferramentas ou sistemas.

## U

### UX (User Experience)

Experiência geral do usuário ao interagir com um produto ou serviço, incluindo facilidade de uso, satisfação e eficiência.

### UI (User Interface)

Elementos visuais e interativos com os quais o usuário interage em um sistema, como menus, botões e telas.

## W

### Web Scraping

Técnica automatizada de extração de dados de páginas da web, frequentemente utilizada para coletar informações públicas.