

**ANNEX 11**

**PUBLIC TENDER No. MTIC-LP-01-2019**

**REPÚBLICA DE COLOMBIA**

**MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y LAS TELECOMUNICACIONES**

**CONTRACT FOR THE OPERATION OF THE REGISTER OF THE INTERNET DOMAIN OF COLOMBIA (ccTLD .CO**

**TECHNICAL APPENDIX 1**

Bogota D.C. November 2019

**TABLE OF CONTENT**

[CAPÍTULO I GENERAL ASPECTS OF TECHNICAL SPECIFICATIONS 4](#_Toc24706629)

[1.1 Definitions 4](#_Toc24706630)

[1.2 Introduction 4](#_Toc24706631)

[1.3 International Standards and Rules 5](#_Toc24706632)

[CAPÍTULO II AUTHORITATIVE NAME SERVER - DNS 6](#_Toc24706633)

[2.1 General Specifications of the System 6](#_Toc24706634)

[2.2 DNS services 6](#_Toc24706635)

[2.3 Authoritative Name Servers 7](#_Toc24706636)

[2.4 Domain Name System Security Extensions ("DNSSEC") 8](#_Toc24706637)

[CAPÍTULO III REGISTRANT DATA DIRECTORY SERVICES (RDDS) 9](#_Toc24706638)

[3.1 General Specifications of the System 9](#_Toc24706639)

[3.2 Technical features 9](#_Toc24706640)

[CAPÍTULO IV REGISTRY ACCESS PROTOCOL THROUGH EXTENSIBLE PROVISIONING (EPP) 10](#_Toc24706641)

[4.1 Shared Registry System 10](#_Toc24706642)

[4.2 Registry Access Protocol - RAP 10](#_Toc24706643)

[4.3 Application for Registrars 11](#_Toc24706644)

[4.4 Transport and Security of the EPP protocol 12](#_Toc24706645)

[4.5 Reseller ID support 13](#_Toc24706646)

[4.6 EPP software development toolkit 13](#_Toc24706647)

[CAPÍTULO V FACILITIES AND SYSTEMS 13](#_Toc24706648)

[5.1 Description of facilities and systems 13](#_Toc24706649)

[5.2 Physical security and risk mitigation. 14](#_Toc24706650)

[CAPÍTULO VI SYSTEM SECURITY AND RELIABILITY 14](#_Toc24706651)

[6.1 General System Security Obligations 14](#_Toc24706652)

[6.2 Disaster Recovery Procedures 15](#_Toc24706653)

[6.3 Requirements of Security 15](#_Toc24706654)

[6.4 Risk and Abuse Mitigation Plan 15](#_Toc24706655)

[CAPÍTULO VII CONTINUITY OF SERVICE 17](#_Toc24706656)

[7.1 Contingency Plan 17](#_Toc24706657)

[7.2 General Aspects of the Contingency Plan 17](#_Toc24706658)

[7.3 Contents of the Contingency Plan 17](#_Toc24706659)

[CAPÍTULO VIII EMERGENCY TRANSITION PLAN 20](#_Toc24706660)

[8.1 Emergency Transition Plan 20](#_Toc24706661)

[8.2 Preparation of the Emergency Transition Plan 20](#_Toc24706662)

[CAPÍTULO IX FINAL TRANSITION PLAN 22](#_Toc24706663)

[9.1 Description 22](#_Toc24706664)

[9.2 General activities 22](#_Toc24706665)

[9.3 Detailed Activities 22](#_Toc24706666)

[CAPÍTULO X GENERAL REQUIREMENTS FOR SUPERVISION, CONTROL AND REPORTS 25](#_Toc24706667)

[10.1 Right of supervision, inspection and periodic audit of MINTIC 25](#_Toc24706668)

[10.2 Control dashboard, Reports and Billing 25](#_Toc24706669)

[10.3 Reports 26](#_Toc24706670)

[10.4 Annual Activity Planning Report 27](#_Toc24706671)

[10.5 Monthly Operation Report - Periodicity 28](#_Toc24706672)

[10.6 Final report 29](#_Toc24706673)

[10.7 Specific Reports 29](#_Toc24706674)

[10.8 Follow-up meetings 29](#_Toc24706675)

[10.9 Documentary information 30](#_Toc24706676)

# GENERAL ASPECTS OF TECHNICAL SPECIFICATIONS

## Definitions

* + - 1. In addition to the definitions contained in Chapter II of the Contract, the following definitions will apply for the purposes of interpreting this Appendix:
				1. Internet Engineering Task Force (“IETF”): Refers to the international non-governmental entity, responsible for developing open standards for Internet architecture.
				2. NRO: Refers to the new registry operator that will succeed the Registry Operator upon termination of this Agreement.
				3. Registry Access Protocol (RAP)
				4. RFC: Refers to the denomination of Internet standards developed by IETF.
				5. THICK: It is a service model that must be implemented by the Registry Operator in which all the information associated with domains, both technical and domain contacts is stored and maintained by the Domain Operator.

## Introduction

* + - 1. In accordance with the provisions of Section 2.8 of the Contract, this Appendix establishes the minimum technical conditions to be met by the Registry Operator in the provision of the Registry Services and other activities under its charge related to the Contract.
			2. The content of this Appendix shall be applied in accordance with the hierarchy that among the Contract documents is established in Section 1.2 (d).
			3. The aspects described below do not correspond to an exhaustive list of the requirements (software and hardware infrastructure) that the Registry Operator of the ccTLD.CO must have, but rather to some minimum components that the Registry Operator must meet to efficiently manage the .CO domain.
			4. The Registry Operator can innovate and propose different hardware and software configurations to meet or exceed the standards required in this Appendix, provided it meets the Service Levels requested in Appendix 2: Service Levels.
			5. The Registry Operator must comply with the Applicable Law, particularly with those related to security, protection of personal data and accreditation of Registrars.

## International Standards and Rules

* + - 1. The Registry Operator must comply with the international standards set forth in this Appendix, applicable to the Registry Services and other obligations set forth in the Contract, specifically those issued by:
				1. Internet Engineering Task Force (“IETF”).
				2. ICANN
				3. Internet Architecture Board (“IAB”)
				4. Security and Stability Advisory Committee (“SSAC”)
			2. In any case, the Registry Operator must provide the Registry Services and comply with other obligations set forth in the Contract under the standard of international best practices.

# AUTHORITATIVE NAME SERVER - DNS

## General Specifications of the System

* + - 1. The Registry Operator must comply with the relevant and existing RFCs for the operation and administration of the domain name registry and those published in the future by the IETF, including all successive regulations, modifications or additions related to the DNS and the operations of the name server, in accordance, but not limited to RFCs 1034, 1035, 1123, 1982, 2181, 3226, 3596, 3597, 4343, 5966 y 6891.
			2. The Registry Operator will sign the zone files of the Colombian ccTLD implementing DNSSEC. To do this, it will comply with RFC 4033, 4034, 4035, 4509 and its successors, and will follow the best practices described in RFC 6781 and its successors.
			3. The Registry Operator will comply with internationalized domain names ("IDN"), for which it will comply with RFCs 5890, 5891, 5892, 5893 and their successors.
			4. The system provided by the Registry Operator will support IPv6 connectivity to the registry and for DNS resolution. It should be able to accept IPv6 addresses as queue records in the Registry and publish them in the DNS. The recommendations and considerations described in RFC 4472 should be followed. Public transport of IPv6 for its SRS must be offered to any Registrar.
			5. DNS infrastructure must locate a minimum of two (2) resolution servers within the geographic boundaries of Colombia with diverse accessibility to ensure continuity / redundancy, which must be in data center facilities in different geographic locations, meeting at least the conditions specified in the ANSI/TIA-942 standard for a Tier III Data Center.

## DNS services

* + - 1. The provision of DNS services will have the following characteristics:
				1. Resolution of the .CO domain ensuring the availability of Authoritative Nameservers for the ccTLD .CO and the accuracy of data resolution of the .CO zone.
				2. The diversity of DNS resolution and the infrastructure that the Registry Operator must operate, must be compatible with the diversity of resolution software and the diversity in all the hardware used.
				3. DNS servers geographically distributed to meet the Service Levels and be connected to the Internet in different locations and networks to ensure its operation in case of temporary damage to any of the servers.
				4. The DNS infrastructure must locate a minimum of two (2) resolution servers within the geographical boundaries of Colombia, with diverse accessibility to ensure demand, continuity and redundancy.
				5. DNS servers must be connected to the internet through the world's high-speed rings, using anycast broadcast technology.
				6. The Resolution System must be scalable to handle the existing number of names and projected growth, loads of existing DNS queries, including normal peaks and projected growth, attacks and traffic generated by viruses, worms and spam, simultaneous attacks on the network (geographically dispersed), etc.
				7. This system must be secure with Distributed denial-of-service (“DdoS”) mitigation capability and must be compatible with “DNSSEC” (Domain Name System Security Extensions), Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6) and Internationalized Domain Names ("IDNs").
				8. Continuous registration of near-real-time DNS updates to the distributed network of DNS servers.
			2. The Registry Operator must:
				1. Operate and maintain the primary server of ccTLD .CO;
				2. Operate and maintain secondary services of ccTLD .CO;
				3. Compile, generate and propagate zone files from ccTLD .CO;
				4. Operate the ccTLD. CO under a THICK domain registrar support

## Authoritative Name Servers

* + - 1. The Registry Operator must provide Authoritative Name Servers both at First Level Domain and Second Level Domains.
			2. The Registry Operator shall comply with the relevant existing RFCs and those published in the future by the IETF, including all subsequent standards, modifications or additions thereto related to DNS and name server operations, which include, among others:
				1. RFC 1034 - Domain names - concepts and installations (part of STD 13)
				2. RFC 1035 - Domain names - implementation and specification (part of STD 13)
				3. RFC 1123 - Internet Host Requirements - Application and Support (part of STD 3)
				4. RFC 1982 - Serial number arithmetic
				5. RFC 2181 - Clarifications to the DNS specification
				6. RFC 2182 - Selection and operation of secondary DNS servers (BCP 16)
				7. RFC 3226: A6-compliant DNSSEC and IPv6 server/solver message size requirements
				8. RFC 3596: DNS extensions to support IP version 6 (STD 88)
				9. RFC 3597: Handling of unknown DNS resource records (RR) types
				10. RFC 4343 - Clarification of case insensitivity to Domain Name System (DNS)
				11. RFC 5966 - DNS Transport over TCP - Implementation Requirements
				12. RFC 6891 - Extension mechanisms for DNS (EDNS (0)) - STD 75
			3. The Registry Operator must follow the Operating Guidelines for IPv6 transport of DNS BCP 91 (RFC 3901) (https://www.rfc-editor.org/rfc/rfc3901.txt) and the recommendations described in RFC 4472 - Considerations and operational problems with IPv6 DNS.

## Domain Name System Security Extensions ("DNSSEC")

* + - 1. The Registry Operator must sign its zone files by implementing DNSSEC. In particular, the Registry Operator will sign the .CO zone file and the second level name spaces managed by the registry and the zone files for the DNS servers.
			2. The Registry Operator must comply with the following RFCs and their subsequent modifications:
				1. RFC 4033 - Introduction and DNS safety requirements
				2. RFC 4034 - Resource records for DNS security extensions
				3. RFC 4035: Protocol modifications for DNS security extensions
				4. RFC 4509: Use of SHA-256 in the resource records (RR) of the DNSSEC (DS) delegation signer and follow the best practices described in:
				5. RFC 6781 - DNSSEC Operational Practices, Version 2
			3. Any change in host names or IP addresses of any of the authoritative name servers must be subject to prior notification to IANNA by the Registry Operator in its capacity as technical contact.

# REGISTRANT DATA DIRECTORY SERVICES (RDDS)

## General Specifications of the System

1. The Registry Operator must guarantee public, reliable and updated access to the domain name base in the ccTLD.CO. Initially this service must be provided by the WHOIS protocol as defined by RFC 3912. However, before the expiration of the third (3rd) year of the Operation Stage, the Registry Operator must provide access to this data through the Registration Data Access Protocol (RDAP), which will replace the WHOIS protocol.

1. The Registry Operator must define a migration plan to make the transition between Whois and RDAP following the guidelines established by ICANN, detailed in <https://www.icann.org/gtld-rdap-profile>.
2. The delivery of the migration plan to make the transition between Whois and RDAP must be made before the thirtieth (30th) month of the Operation Stage, and will be subject to the abbreviated review procedure provided for in Section 9.2 of the Contract.

## Technical features

* + - 1. The RDDS/Whois service and RDAP must provide configurable results options including, but not limited to:
				1. RDDS / WHOIS /RDAP based in the web;
				2. WHOIS Hardware and software in EPP standard format;
				3. RDDS / WHOIS / RDAP searching capabilities able to support exact match, partial match and Boolean search;
				4. Configurable delivery of RDDS / WHOIS / RDAP data;
				5. Support for multilingual contact information in local language, and
				6. There should be an adequate security mechanism to prevent the abuse of data mining.

# REGISTRY ACCESS PROTOCOL THROUGH EXTENSIBLE PROVISIONING (EPP)

## Shared Registry System

The Registry Operator must provide services related to the provision and maintenance of the Shared Registry System, through the Registry Access Protocol under the Extensible Provisioning Protocol (EPP) that includes, but it’s not limited to:

* + - * 1. Have infrastructure for a stable registration system and access support equivalent to SRS for all Registrars. Load balancing in all registration operations: gateway, SRS, WHOIS / RDDS, DNS, RDAP, etc.
				2. Scalable and reliable registration system that includes hardware, equipment and software solutions.
				3. Systems architecture, services provided and maintenance methodologies to meet the Service Levels.
				4. Prepare and manage operational tests and evaluation ("OT&E") to registrars, as they prepare and validate their systems;
				5. Registration block that allows the registrant to block the domain name for security reasons at the registration level;
				6. Include domain synchronization feature that allows applicants to synchronize their domain name portfolio with a common renewal date;
				7. SRS branching from WHOIS / RDS services;
				8. Replication with a mirror database located in Colombia with a maximum delay of one day

## Registry Access Protocol - RAP

* + - 1. The purpose of the Registry Access Protocol is to allow registrars to perform various operations that are necessary when creating, renewing, transferring, modifying and deleting domain name registrations. The RAP provides a remote interface in the Registry Database.
			2. The Registry Access Protocol (RAP) must be the Extensible Provisioning Protocol (EPP) and the associated data objects that the IETF has developed. The Registry Operator must comply with the Internet standard IETF STD 69 (<https://tools.ietf.org/html/std69>).
			3. The Registry Operator must comply with the following technical standards issued by IETF and must follow the notices of any additional update to the EPP standards during the development of the contract.
				1. RFC5730 - Extensible Provisioning Protocol (EPP)
				2. RFC5731 - Domain Name of the Extensible Provisioning Protocol (EPP)
				3. Mapping
				4. RFC5732 - Host Assignment of the Extensible Provisioning Protocol (EPP)
				5. RFC5733 - Contact assignment of Extensible Provisioning Protocol (EPP)
				6. RFC5734 - Transport of Extensible Provisioning Protocol (EPP) over TCP
				7. RFC3735 - Guidelines for extending the Extensible Provisioning Protocol (EPP) - Informational RFC
				8. RFC3915 - Mapping the grace period of the domain registration for the Extensible Provisioning Protocol (EPP)
				9. RFC5910 - Assigning Domain Name System (DNS) security extensions for the Extensible Provisioning Protocol - Proposed Standard
			4. All EPP functionality outside the base EPP RFCs must be documented in Internet-draft format following the guidelines described in RFC 3735 and published on the Registry Operator's website. The Registry Operator will provide and update the relevant documentation of all EPP objects and extensions prior to implementation and publish such documentation on a public website.
			5. The Registry Operator will provide and update the relevant documentation of all EPP objects and extensions supported by ICANN prior to deployment.
			6. The Registry Operator is required to operate the .CO implementation of the EPP.
			7. Centralized support by the registrar of the domain "THICK" as well as other contacts in the registry using the standard extensible provision protocol - "EPP".

## Application for Registrars

* + - 1. The Registry Operator must provide an HTTPS-based website for Registrars to manage the objects they promote or offer within the Registry. This web-based interface must support all functionalities supported within the EPP protocol, using HTML interfaces that meet standards that are accessible and functional from a variety of browsers (such as Internet Explorer, Firefox, Google Chrome or Safari), as it would be the case of the HTML 5.1 standard, among others.
			2. The web-based interface must support multi-factor authentication for Registrar access with multiple authentication factors
			3. The Registry Operator must also provide an HTTPS-based website that provides Registrars with additional services that include:
				1. Domain lists: Registrars must be able to access and download a list of all domains and their details currently promoted or offered within the registration system;
				2. Contact lists: Registrars must be able to access and download a list of all contacts and their details currently promoted or offered within the Registration System;
				3. Host lists: Registrars should be able to access and download a list of all hosts and their details, currently sponsored within the Registration System;
				4. Accounting reports: this tool allows Registrars to cross-reference their registration invoices;
				5. Search capability: ability of a Registrar to search all domain names under his administration that match a keyword, search for all domain names under its administration associated with a particular contact name, postal address, telephone number or email address, search for all domain names under its administration associated with a name server in particular, look for all the name servers under its administration associated with ranges of IP addresses.
			4. All lists, data extracts, etc., must be available as minimum in CSV and XML format (with a defined scheme) enabling automated data processing by registrars. Data can also be provided in other formats.

## Transport and Security of the EPP protocol

* + - 1. The EPP implementation must use the EPP transport mechanism over TCP (see RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP), using the Transport Layer Security (TLS) v1.2 encryption protocol (RFC 5246), see also RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0).
			2. TLS should be used to ensure the secure and authenticated exchange of messages. Encryption (cryptographic algorithms) and authentication must be used properly.
			3. The main mechanism for registrar authentication must use the EPP <login> as described in the corresponding RFC. Initial passwords must be assigned by the Registry Operator and delivered through a secure out-of-band or out of the usual communication channels. This in addition to any authentication provided in the transport layer.
			4. Other features of EPP should be:
				1. The languages supported by the EPP implementation must include at least English and Spanish;
				2. Standard RAP operations ( <create>, <delete>, etc.) must be identical for all domains and for all Registrars. In addition, the data collection policy with respect to registration data must be identical for all Registrars;
				3. The details of the transaction must be recorded keeping a record of the number and type of query commands by the Registrar;
				4. EPP requires that each domain and contact object also have a unique object identifier deposit (ROID) globally,
				5. Instead of ROID, in EPP requests and responses, each domain and contact object are referred to by its local name (also called as object identifier):
			5. Any future implementation of the registration software should ensure compatibility with previous versions of the registrars whenever possible.

## Reseller ID support

* + - 1. The Registry Operator must implement support for a reseller ID which is provided for the purpose of associating the reseller ID with the domain names under administration, to include them in the WHOIS registry. For these purposes, the reseller is a company that offers domain name registration services through a Registrar.
			2. Once the reseller has provided the reseller ID to the Registrar, the Registrar must associate the Reseller ID with any newly created domain name in the reseller's management.

## EPP software development toolkit

* + - 1. Provision of a registration toolkit (Registrar Toolkit - RTK) where the Registry Operator must provide all Registrars with a registration software toolkit with sufficient technical specifications and documentation to support EPP protocol access to the Database Registry and interfaces of the Registrar's software system.

# FACILITIES AND SYSTEMS

## Description of facilities and systems

* + - 1. Before the expiration of the third month of the Transition Stage, the Registry Operator must submit for information a description of the facilities and systems that will host the Registry, as well as the NOC (Network Operations Center) monitoring platform. This description should provide diagrams of all the systems operating in each location, and include information on physical facilities, hardware and equipment, software, redundant power connections and internet connectivity, environmental equipment, redundancy systems and fault tolerance.
			2. The data centers where the support technology platform is hosted must have a minimum design and operation certification TIER-IV, or similar.

## Physical security and risk mitigation.

* + - 1. Data centers must have the capacity, interoperability and availability required to ensure compliance with Service Levels. Load balancing capabilities to avoid security breaches, system attacks and system overload problems.
			2. The Registry Operator shall implement the required hardware and software and carry out the administration of the facilities and systems, including but not limited to:
				1. Connectivity between design facilities that comply with the proposed operation and the Service Levels required and the connectivity that supports the fulfilment of the objectives proposed in the BCP.
				2. DDoS facilities (Distributed denial-of-service) reinforced with capabilities to handle bursts of up to 10 Gbps (Gigabit per second) capacity;
				3. The Registry Operator must separate the resources of OT&E (Operational Test and Evaluation) for on-board registration regardless of production facilities;
				4. Filtering for network entry;
				5. IPv6 support

# SYSTEM SECURITY AND RELIABILITY

## General System Security Obligations

* + - 1. All important information assets (such as databases, including the Registration Database, or data files, system documentation and user manuals, training material, operational and support procedures, continuity plans, non-disclosure and stored information agreements) must be tracked and have an assigned head of the management team.
			2. Software assets, such as application and system software, development tools, as well as physical assets, including equipment and parts, must be tracked to ensure control.
			3. The Registry Operator must be responsible for providing and executing the processes and methodologies of operational stability, reliability and safety, including, but not limited to:
				1. 24x7x365 monitoring of the Registration and Network System by a Network Operations Center (“NOC”) with monitoring tools to generate alerts for any problem with the registration system and its network;
				2. Protection against malicious software, DDoS attacks, intrusions, data manipulation and other interruptions in operations;
				3. Implement information security management systems;
				4. The adequate periodical backup of the information and data supporting the system;
				5. Network security to prevent unauthorized access or improper use;
				6. Redundant security systems;
				7. Establish backup copies for ccTLD .CO zone files and the information registered for the domain name;
				8. Have personnel with technical capacity and experience to operate the Registry under the Service Levels provided and
				9. Establish detailed review processes for the integration of current best practices and future technical standards, as well as monitoring of subsequent compliance and periodic review.

## Disaster Recovery Procedures

* + - 1. The registry operator must provide services for disaster recovery, data backup and system recovery procedures, including but not limited to:
				1. Complete disaster recovery procedures;
				2. Backup and registry replicas;
				3. Redundant systems;
				4. Backup availability for the operating system/ software/ hardware;
				5. Mitigations of technical risk;
				6. Procedures for operation restoration systems in the event of service outages, and
				7. Procedures for planned and preventive maintenance.

## Requirements of Security

* + - 1. The Registry will always comply with the following security standards:
				1. ISO / IEC 27001: 2013 Information technology - Security techniques - Information security management systems -
				2. ISO / CEI 27002: 2013 Information technology - Security techniques - Code of practices for information security controls.

## Risk and Abuse Mitigation Plan

* + - 1. The Registry Operator must adopt a risk management approach and develop a Risk and Abuse Mitigation Plan that aligns the information security practice with broader risk management practices.
			2. Information security risk management should be implemented through identification, analysis, evaluation and, where appropriate, the treatment of security risks for information and systems.
			3. The Registry Operator must prepare the Risk and Abuse Mitigation Plan, which must be submitted within the deadlines established in the Contract and submitted to the General Review Procedure for verification.
			4. The Registry Operator must carry out periodical safety and audit evaluations of the Risk and Abuse Mitigation Plan.
			5. The Risk and Abuse Mitigation Plan will be updated at least annually.
			6. The Risk and Abuse Mitigation Plan will have the following elements:
				1. Information Security Policy
				2. Security Risk Management Plan
				3. System Security plan (software, databases accesses, etc.)
				4. Physical security elements
				5. Standard operation procedures
				6. Incident response plan
				7. Emergency procedures
				8. Business continuity and disaster recovery plans
			7. The objectives of the Risk and Abuse Mitigation Plan will be the following:
				1. Ensure that an appropriate level of security is applied to the Registration System by adopting an appropriate certification framework;
				2. Implement appropriate vulnerability management practices;
				3. Measure and evaluate the impact and time needed to resolve cybersecurity incidents by implementing procedures and technical measures properly configured;

# CONTINUITY OF SERVICE

## Contingency Plan

* + - 1. The Registry Operator must prepare a Contingency Plan for the Registration System, which must be submitted within the deadlines established in the Contract and submitted to a General Review Procedure for its verification.
			2. The Contingency Plan will detail the processes that will be carried out to ensure the continuous operation of the registry in the event of a disaster.
			3. Once the documentary verification has been completed, the Registry Operator must implement the necessary systems and infrastructure to ensure that the Contingency Plan is executed successfully.

## General Aspects of the Contingency Plan

* + - 1. The Contingency Plan should aim to ensure that, in the event of a contingency, it is possible to restore the operation at primary or production level of the Registry by the end of the following Day.
			2. According to the Contingency Plan, in the event of the occurrence of a contingency the Registry must be fully operational within three (3) business days.
			3. The Contingency Plan must establish mechanisms enabling continuity in the provision of the service in situations of:
				1. loss of information,
				2. loss of access or
				3. loss of personnel

## Contents of the Contingency Plan

* + - 1. Analysis of the impact on the business: Analysis of all aspects of the Registry, generating a report that should include:
				1. An audit of sites where the business, personnel, equipment in each place is developed and the impact of the loss of personnel and equipment.
				2. A survey of computers and communications equipment of the organization that includes:

physical security, including access control

tasks performed by the staff

operating procedures

backup and recovery procedures

system development and maintenance

database security

personal computers

* + - * 1. An audit of possible disaster situations that may affect the registration system, in particular

power loss (for example, failure or extended blow)

loss of environmental controls (e.g. air conditioning)

security breaches (for example, physical, electronic, virus or hacking)

loss of internal / external communications

system failure (for example, computer malfunctions or parts thereof)

Internet connection failure or interruption

File loss or destruction

* + - 1. Business continuity plan: The business continuity plan is an extension of the impact analysis and effectively documents the procedures to follow to recover from a disaster situation. Copies of documents must be kept off-site with appropriate backup copies and software files in case the main site is destroyed. The business continuity plan must be written to allow an external organization or a qualified individual to perform the recovery process. The main components of the business continuity plan will be as follows:
				1. Organization details: location of other offices, contact details of trained personnel for recovery processes;
				2. Disaster reporting procedures for operations: list of organizations and individuals to be notified;
				3. Procedures for activating alternative workplaces;
				4. Procedures to recover vital data and files that must be in a different place as part of the recovery process;
				5. Definition of equipment and recovery responsibilities: provide a list of the people assigned to the recovery team and the tasks to be performed by those teams. This documentation should take the form of a "flow chart" for recovery in any situation. Arrangements with external organizations or qualified individuals may be included to be used as alternatives to internal personnel in the event of a disaster. External personnel must be trained in recovery procedures;
				6. Recovery procedures: defines the steps involved in the recovery process. The steps should be clearly defined and reviewed during staff training and testing. This is the key area of the continuity plan;
				7. Relocation Procedures: This section relates to the relocation of the registration system, either temporarily or permanently as a result of a disaster situation;
				8. Resource and procurement requirements: Provide a list of vendors and suppliers who may be asked to provide equipment and/or services to help with the recovery process. The section must also document any agreement or contract with suppliers to supply short-term equipment, for example. immediate supply of a replacement computer;
				9. Staff training;
				10. Business continuity plan tests;
				11. Effectiveness in the evaluation and monitoring of the service, carried out on a full annual basis, which must be conducted by a senior manager.

# EMERGENCY TRANSITION PLAN

## Emergency Transition Plan

* + - 1. The Registry Operator must prepare an Emergency Transition Plan, which must be submitted within the deadlines established in the Contract and submitted to a General Review Procedure for its verification.
			2. The Emergency Transition will cover situations in which the Registry Operator cannot execute the Contingency Plan, the plan fails, or an Early Termination of the Contract occurs.
			3. The Emergency Transition Plan must be oriented to transfer the Critical Registry Services to EBERO, seeking continuity of service.
			4. The Transition Plan will also refer to the use of the Mirror Database in those events in which the Registration Database cannot be used.
			5. In the event that it is necessary for the EBERO to enter into operation, this one must ensure continuity in the provision of the services until the moment in which the Registry Operator demonstrates to the satisfaction of the MinTIC that it can resume with the execution of the Contract without recurrence of the problem. After such demonstration, the Registry Operator may resume operation in accordance with the procedures established in the registration transition process.
			6. If the EBERO must enter into operation for reasons attributable to the Registry Operator, he will pay the MinTIC the costs associated with the operation of the Registration System by the EBERO. These values may be deducted from any amount owed by the Registry Operator to the MinTIC or may be considered as damages to be charged against the Single Compliance Guarantee.

## Preparation of the Emergency Transition Plan

* + - 1. For the preparation of the Emergency Transition Plan, the Registry Operator will take into account the provisions of ICANN in the document that is available at: <https://www.icann.org/resources/pages/transition-processes-2013-04-22-en>
			2. The Registry Operator must provide the MinTIC and/or the EBERO with all the data regarding the registry operations for the Colombian ccTLD necessary to maintain the registration operations and functions that MinTIC and/or the EBERO may request.
			3. The Registry Operator expressly accepts that MinTIC may request changes deemed as necessary in the IANA database for DNS and WHOIS registrations with respect to the Colombian ccTLD if in accordance with the provisions of the Contract it is necessary to proceed with an Emergency Transition.
			4. Registry Operator and MinTIC will develop an annual test of the Emergency Transition Plan to ensure that all software and data are available to temporarily resume service.

# FINAL TRANSITION PLAN

## Description

In accordance with the provisions of Section 5.9 (a) of the Contract, the Registry Operator shall submit, within the first sixty (60) Days of the Transition Stage, a Final Transition Plan that includes the delivery of all data regarding the TLD operations necessary to maintain the Registration Services by the new operator, enabling service continuity, without interruption or trauma, with security and stability in a set time.

## General activities

The general activities are mainly associated with the transfer of databases hosted in the Registry Operator platform to the operational platform of a new service operator. Specifically, the data migration of the SRS (Shared Registration System) and the Establishment of Services Associated with the Domain Name System-DNS and the Domain Registration Data Directory- (RDDS/WHOIS-RDAP) required by the new registry operator (NRO).

The Transition Plan must have a maximum timeline of four (4) months, which includes three migration tests with planned interruptions to address data inconsistencies and ensure a smooth cut.

At the end of the transition, the NRO must meet at least the registration performance specifications indicated by ICANN in:

<https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-es.pdf>

In particular, the NRO must fulfil the following functions, essential for the operation of a ccTLD registry that operates as gTLD as is the case of the .CO domain

1. DNS resolution;
2. DNSSEC zone duly signed (if the registry offers DNSSEC);
3. Shared Registration System (SRS), usually through the Extensible Provisioning Protocol (EEP);
4. Domain Name Registration Data Directory Services (RDDS) under WHOIS/RDAP protocols
5. Registry data escrow.

Additionally, as part of the Final Transition Plan, the request to ICANN to modify the technical contact of the ccTLD .co must be included.

## Detailed Activities

The following is the framework of the activities that must be organized and detailed in time and responsible within the Transition Plan to be presented to the MinTic:

FIRST MONTH

1. ICANN

Authorization submission for the necessary changes in the DNS of the root zone

1. DNS and DNSSEC transition
* Coordination of database and debugging transfer formats.
* Ensure that firewalls and other security components allow communication with NRO
* Configuration of monitoring systems to verify that all zones are updated and loaded correctly. Transference of signed versions of all second, third and any lower level zones.
* DNSSEC key accumulation suspension
* Suspension of changes in TTL
1. WHOIS service
	* Coordination of database and debugging transfer formats.
	* Provide complete extract of registration data to NRO
2. REGISTRARS
	* Inform to all registrars who will be the new domain operator

SECOND AND THIRD MONTH

Perform between two and three scheduled tests during planned interruptions where registrars will be informed that records cannot be created, renewed or updated for a period of a few hours. The tests must be performed on the night from Saturday to Sunday.

1. DNS and DNSSEC transition
* Receipt of DNS and DNSKEY from NRO to include them in the zone apices for the second, third and any lower level zone.
* Proof of the transition process in aspects such as the time required to create the data extraction during the closure of records.
1. WHOIS service
	* Provide two complete extracts of registry data to NRO to verify data integrity.
2. REGISTRARS

Report scheduled test dates for few hours

MONTH BEFORE THE TRANSITION (MAY BE THE THIRD OR FOURTH MONTH)

1. IANA

Request addition of DS records to the root zone

Request changes to TLDs in the root zone

1. DNS and DNSSEC transition
* Aggregation of NRO name servers to the vertex for the second, third and any lower level zone, so that NRO name servers are publicly visible
* Aggregation of the necessary records to ensure that NRO name servers are publicly visible in the DNS zone files for. ccTLD
* Reduce TTLs, to ensure that any changes can be quickly spread.
1. WHOIS/RDAP service
	* Provide a complete extract of registry data to NRO to verify data integrity (this would be number 3)
2. REGISTRARS

Report the exact date for the transition to ensure that any changes to the domain are made before the transition

A WEEK BEFORE THE TRANSITION

1. IANA

Request to remove the name servers of the Operator Registry from the reference of the root zone

1. Remove the name servers from the vertex of the .ccTLD zone so that they are no longer visible and the NRO name servers continue to receive the file from the ERO zone

ONE DAY BEFORE THE TRANSITION

1. DNS and DNSSEC transition
	* Closing the registration, sending the final registration and zone data. Although the DNS service will continue to work, it cannot create new names, nor renew or update.
	* Stop all transferences from ERO zone to additional NRO
2. WHOIS/RDAP service
	* Provide final extract of full registration data to NRO

TRANSITION DAY

1. IANA

Report the removal of DS records from the root zone

1. DNS and DNSSEC transition
	* Remove DS records from zone parent references
	* Close name servers for all zones. They should not be visible to the public.
2. WHOIS/RDAP service
	* Stop operating the WHOIS(RDAP) server

AFTER THE TRANSITION

1. DNSEEC key deletion
2. Final copy of domain log and transactionality (historical movements and prices)

# GENERAL REQUIREMENTS FOR SUPERVISION, CONTROL AND REPORTS

## Right of supervision, inspection and periodic audit of MINTIC

* + - 1. MinTIC directly or through a contractor designated to carry out supervisory activities, reserves the right to inspect and monitor, evaluate progress and measure the performance of the Registry Operator, after providing proper notification to the Registry Operator.
			2. The Registry Operator must provide MinTIC with any document, data, material, access to computer systems or any other information it may require, to enable the evaluation of the progress of the project, the Service Levels and the performance of the entire technological infrastructure implemented for the provision of the aforementioned services.
			3. The Registry Operator must always provide to MinTIC, access to the operation sites both national and international.

## Control dashboard, Reports and Billing

* + - 1. The Registry Operator must ensure that the .CO Registry has an automated integrated solution for monitoring and generating reports, on a mirror database platform maximum one day old of the Registry Database and all what is necessary to enable control and verification of the required services, (ERP, NOC, CRM) resident in the Colombian territory. This panel must be integrated with the .CO Registry operation analytic. The system must have a provision of conversion reports, statistics, information in figures and/or tables and/or graphs for easy interpretation. The MIS (Management information system) must also be integrated with the access control panels to access the DASHBOARD, who will be based on roles upon MinTIC requirement.
			2. The Registry Operator is required to deliver a holistic vision of the elements that interact in the structuring of the service, the provision of the service, its implementation, maintenance, support, continuous improvement, optimization, growth, etc; both at the level of commercial strategy and tactical actions, processes, methodologies, best practices, human talent, user experience, architecture of information and communications technologies, allowing to:
				1. Discover relationships between components and models
				2. Correlate events and detect root causes
				3. Collect and analyse performance metrics of all components
				4. Monitor application response time
				5. Monitor the response time of computer services
				6. Monitor the response time of business services
				7. Monitor database performance
				8. Monitor the performance of physical and virtual systems
				9. Automate and coordinate actions
				10. Plan and manage capabilities
				11. Verify in real time the status of the services contracted with third parties
				12. Guarantee the required service levels.
				13. Ensure proactive monitoring of availability and End-to-End performance.
				14. Ensure compliance with the service level agreements of the proposed service.
				15. Provide and develop the strategy and maturation of the user experience management service

## Reports

At least, the following types of reports must be extracted from the control panel, including but not limited to:

* + - 1. Transaction Progress:
				1. Daily / weekly / monthly type for all transactions (Create, Renew, Transfer, Delete, Restore RGP, etc.)
				2. Zone Type (.COM.CO, .CO, etc.)
			2. Financial progress: Reports of daily / monthly / weekly billable transactions in (.xls / .csv / .pdf / .dat) formats, as specified by the MINTIC accounting team.
			3. Performance Reports:
				1. Follow-up reports of a monthly report of compliance of the Service Levels detailing the performance of the registration system and important registration metrics. The report will measure compliance by the Registry Operator of Service Levels.
				2. Registrar's monthly registration card
				3. MINTIC Domain Abuse Weekly Report
				4. Generate reports on MINTIC ad-hoc requests for specific data points
				5. Incident and alerts report from the User Experience Management Center.
				6. Reports of solution activities of the User Experience Management Center
			4. Demand generation reports:
				1. Master demand generation plan, adjusted and updated if appropriate, in each period
				2. Reports of specific actions of demand generation carried out in the respective period and their relationship with the actions executed in previous periods
				3. Report of specific actions to generate demand to be carried out in the next period and its relationship with those executed in the report period
				4. Executive report (including graphic evidence) of the realization and/or participation in face-to-face or virtual events of demand generation at national and international level.
			5. Billing to the Registrars: In accordance with the type and amount of financial transactions made by a Registrar in a given month and the current rates, the Registry Operator will be responsible for generating the corresponding account statement to the Registrars. These statements will be uploaded in the first five (5) days of each month.

.

## Annual Activity Planning Report

* + - 1. The Registry Operator must submit annually (in Months 13, 25, 37, 49 and 60 of the Operation Stage) to MinTIC, a planning report which must include, among other elements:
				1. Analysis and assessment of risks in the administration of ccTLD .CO
				2. Organization of the working team
				3. General working schedule, indicating dates of delivery of the reports.
				4. General description of audit tests, among others
				5. Biannual report on comprehensive audit of proper application of the ccTLD .co policy.
				6. Quarterly compliance report covering at least the following points:

Verification of the financial development of the Contract

Verification of the controls established to detect and report errors.

Execution of tests on controls that guarantee the confidentiality, integrity, availability and traceability of the information managed by the Registry Operator operator of ccTLD.CO and that ensure compliance with the policy of ccTLD.CO (based on processes or systems).

Evaluation of the integrity of the information processing performed by the information system used by the Registry Operator.

* + - * 1. Annual report on security audit
				2. Annual report on continuity audit
				3. Annual report on audit to third parties, including practices on transparency between the Registry Operator and the Registrars vr.gr. Identical sales price management for all registrars.
				4. Final settlement report, which must contain the corresponding Settlement Record.
			1. This report will be the subject of an abbreviated documentary verification process.
			2. Additionally, it must deliver extraordinary reports requested by the MinTIC, or those deemed relevant in order to ensure the correct execution of the activities derived from the Contract.

## Monthly Operation Report - Periodicity

* + - 1. The Registry Operator must submit to MinTIC, the following operations and financial reports.

|  |  |  |
| --- | --- | --- |
| **#** | **General reports** | **Periodicity** |
| 1 | Registration: New registrations, transfers, suspensions, cancellations and changes among others. | Report available no later than the 5th calendar day after the end of the month. |
| 2 | Accredited Registrars. | Report available no later than the 5th calendar day after the end of the month.  |
| 3 | Database support for accumulated behaviour over time. | Report available no later than the 5th calendar day after the end of the month.  |
| 4 | Service Level Behaviour.  | Report available no later than the 10th calendar day after the end of the month.  |
| 5 | Monthly report on the Administrator's transactions, broken down by:* New registrations, transfers, suspensions, cancellations and changes among others.
* Accredited Registrars.
* Other statistics suggested by the Registry Operator or previously agreed upon.
 | Report available no later than the 5th calendar day after the end of the month.  |
| 6 | Period management, including information on the reliability of the data contained in the WHOIS/RDDS.  | Annual report available no later than the 10th calendar day after the final month of the year of operation. |
| 7 | Audit reports on the different components (infrastructure, services, information asset security, physical security, disaster recovery, business continuity plan, among others) | Quarterly report available no later than the 10th calendar day after the final month of the quarter of operation |

|  |  |  |
| --- | --- | --- |
| **#** | **Financial reports** | **Periodicity** |
| 4 | Detailed report of monthly billable transactions: this report includes all domain name registration data (such as: create, renew, delete, transfer, redeem and cancel, and discount program transactions related to automatic renewal) listed by transaction date, registrar, registrant and TLD. | Report available no later than the 5th calendar day after the end of the month.  |
| 5 | Monthly reimbursement report: This report includes all reimbursement data by domain name, promotion program, transaction date, registrar, registrant and TLD. | Report available no later than the 5th calendar day after the end of the month.  |
| 6 | Monthly registrar fees report: This report lists the registrar fees by domain name, transaction date, registrar, registrant.  | Report available no later than the 5th calendar day after the end of the month.  |
| 7 | Monthly registrar billing: Each registrar account receives an invoice and a detailed statement from the previous month. | Invoices are distributed electronically to registrars no later than the 5th calendar day after the end of the month. |

## Final report

* + - 1. In the final stage of the project and not before three hundred and sixty (360) Days, the Registry Operator undertakes to deliver a final report containing detailed information on the execution of the project, including as minimum:
				1. Consolidated information of the main stages of the project,
				2. Historical information on the execution of the project,
				3. The lessons learned,
				4. What worked well? Main success stories that arose during the execution
				5. What failed? how could have been avoided
				6. Main difficulties and risks encountered during project execution and recommendations for their mitigation.
				7. Risks detected and
				8. Documentary record backup.
				9. Proposals for adjustments or updating of the Final Transition Plan, if necessary, including justification.

## Specific Reports

At any time during the execution of the Contract, MinTIC may request specific reports of technical, administrative, legal, financial, economic and other aspects related to the execution of the Contract, which must be delivered within a term not exceeding five (5) Days business or otherwise in the term defined (in no case less than five (5) business days) by MinTIC.

## Follow-up meetings

* + - 1. MinTIC will schedule the respective meetings to which the Registry Operator must attend with the Project Manager. The Project Manager will be the person in charge by the Registry Operator to fully accompany the execution of the project, it will be the main communication channel with MinTIC.
			2. If the Project Manager cannot attend the meetings, for duly justified reasons, the Legal representative of the Registry Operator or whoever acts as such may designate a substitute having broad and enough powers for decision-making in order to monitor the execution of the project. These meetings will be scenarios to socialize the execution and development of the project, the facilities, attend requests, solve problems, among others. Record of these meetings must be kept through a document briefing the Minutes of meetings.
			3. Follow-up meetings will be of the following type:

Operation follow up meeting:

Frequency: Weekly. Its purpose is to follow up the main factors of the service.

Follow-up meeting of tactical actions and activities:

Frequency: Monthly. Its purpose is the analysis and establishment of action plans for activities that require adjustments, modifications, minor changes, major changes; seeking the continuous improvement of the service and revenues collected from the provision of the service.

Strategic Follow up Meeting:

Frequency: Quarterly. Its purpose is the general analysis of the project, decisions of the highest executive level.

## Documentary information

* + - 1. The information generated during the execution of the contract must be structured in a common access repository with tracking schemes and changes in the status of each document and the availability of digital signatures for closing versions.
			2. This is a solution that can be evaluated, aligned with zero paper policy, as an alternative to the reports requested in the previous paragraphs in compliance with legal provisions and documentary retention of MinTIC.