**Convergence**
Services

What does **Convergence do** for your company or institucion?

Advise, train, structure, and implement IT matters with functional and secure processes, seeking to ensure that the technological area is led by trained personnel, **aligned with international standards; ISO 27001 for information security and ISO 22301 for business continuity**
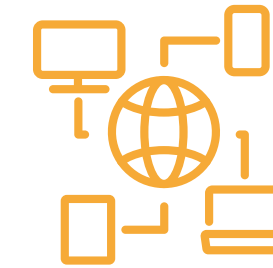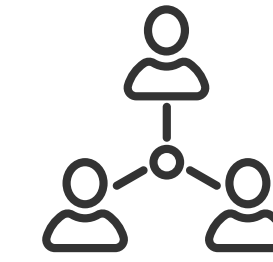
Convergence
SERVICES

Our general services are:
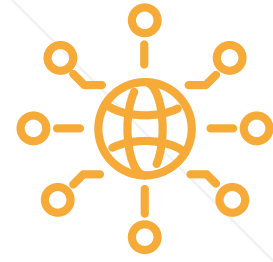
Management services of wired and wireless networks
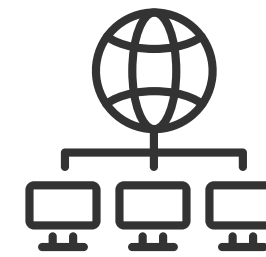
Server Management (Windows and Linux)

computer equipment management

First and second line technical support

National and international supplier management

Service Management

Cloud Services (AWS)

we offer **key services** such as:

- **Certifications** Consulting
- **Certificators**
- **Strengthening** of ISO information security a

Convergence
SERVICES

We start the process with meticulous planning and needs assessment to **identify demands such as:**

- ○ Consultancy
- ○ Development of documentation and processes **for a proper operation**
- ○ Design and implementation of **HA (High Availability)**
- ○ Design and implementation of **DRP (Disaster Recovery Plan)**
- ○ Identification of compliance with ISOS and other certifications, and review of information for accreditation **with direct contact with the certifying houses.**
- ○ Identification of additional development needs

Convergence
SERVICES

How do we do it?

initial phase

As an initial phase, a **period of three months of operation is crucial to understand the client's operation and identify areas of opportunity where more attention needs to be paid.**
Afterwards, a report of results and findings identified at the conclusion of this phase will be presented in order to implement improvements, processes, technological recommendations, and remediations that contribute to the correct structure.
Examples:

- ↻ Systems and safety analysis
- ↻ Establishment of a security zone for sensitive information
- ↻ Network analysis and troubleshooting
- ↻ Resolution of security observations
- ↻ Asset monitoring
- ↻ Introduction of operational procedures

implementation phase

The findings of the initial phase will be resolved.

Action Plan

In accordance with the defined objectives, we propose the work plan designed in the following phases.

Follow-up phase

- Adaptation of operational procedures by the entire team.
- Delivery of the first monthly performance-based reports
- Complete alignment between operational processes and information security procedures.

Fase de mejoras

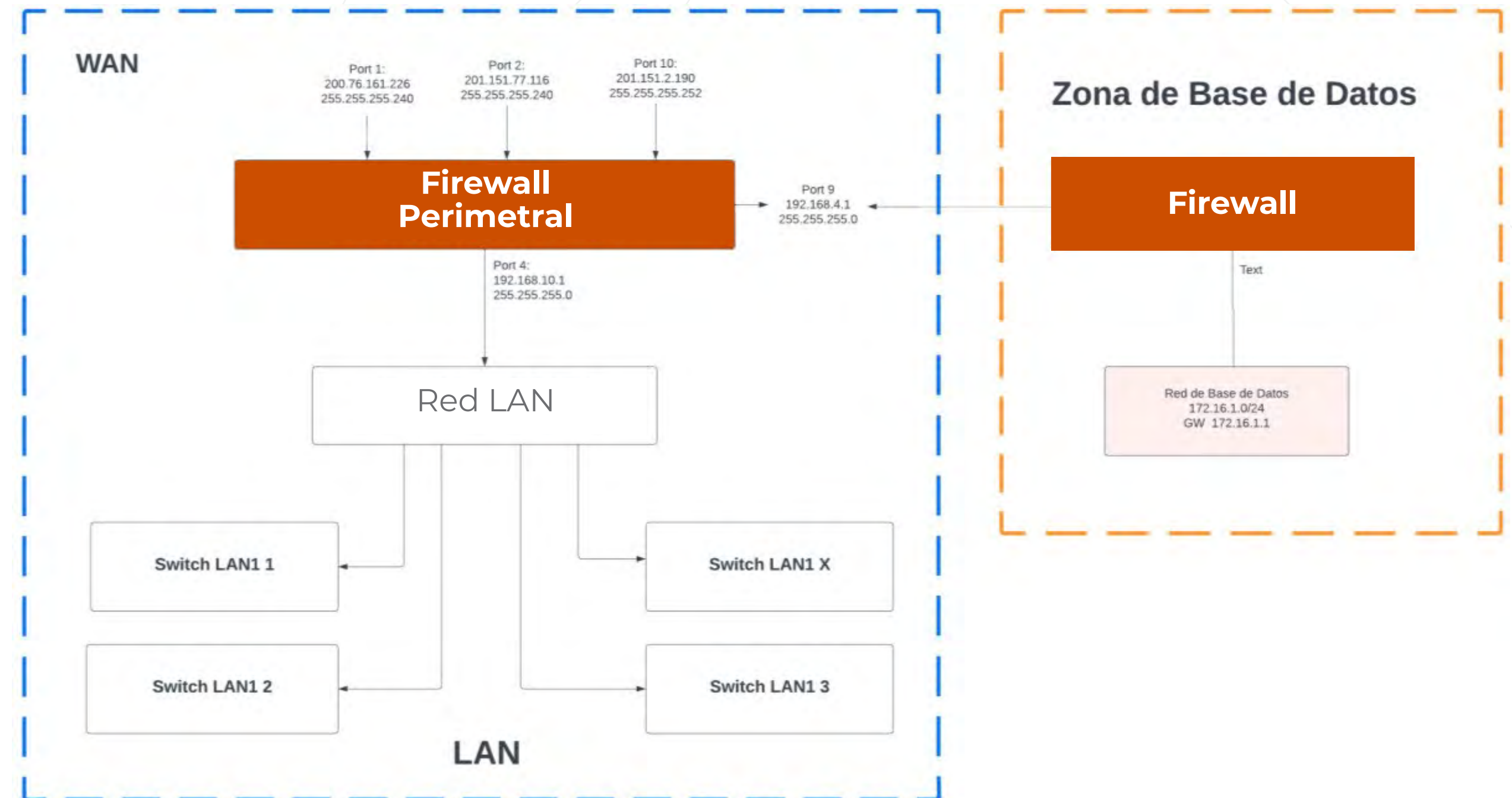Adaptation based on the needs of the operation, considering the scope of the proposal.

Convergence
SERVICES

04

Initial phases

Identification of Security zones (physical and logical)

The main assets and resources that belong to the secure zone will be identified, generating a section of critical assets.
Critical assets will be identified in the analysis phase, based on the results of the analysis in the initial stage, the configuration of the Firewall Swiches security equipment that can be optimally managed will be determined. During the second quarter the activity is to evaluate whether the configuration is optimized.

Convergence
SERVICES

Networks

An analysis of the network will be carried out, **it is possible to find multiple risks, which will be solved by following the next actions:**

○ A single network segmented as **wired or wireless according to needs**

○ Traffic control, for which **navigation profiles associated with each network will be created,** thus providing granular control of navigation permissions.

○ Network access control, whereby **access control is implemented through the physical address of the devices.**

Convergence
SERVICES

Guidelines of ISOs 27001 and 22301

Our strength in consulting services is our experience in compliance and alignment with the requirements of **ISO 27001 for information security and ISO 22301 for business continuity**, the most significant actions to be considered are the following:

- ↻ Comprehensive business continuity strategy

- ↻ Periodic risk analysis

- ↻ Installation of DRP architecture

- ↻ Implementation of ticketing tool for complete traceability of events.

- ↻ Installation of antivirus

Convergence
SERVICES

Pro Active monitoring

Monitoring of physical and logical equipment that is running or working, the most critical assets will be registered in the monitoring system, which are categorized into: Switches, Firewalls, Access Points, Servers and Printers. The use of 1,000 sensors will be evaluated.

It will be covered by the monitoring system
Finally, while it is true that the implementation of a monitoring tool can be completed 100%, it is important to mention that during the next phase, the monitoring strategy will be optimized..
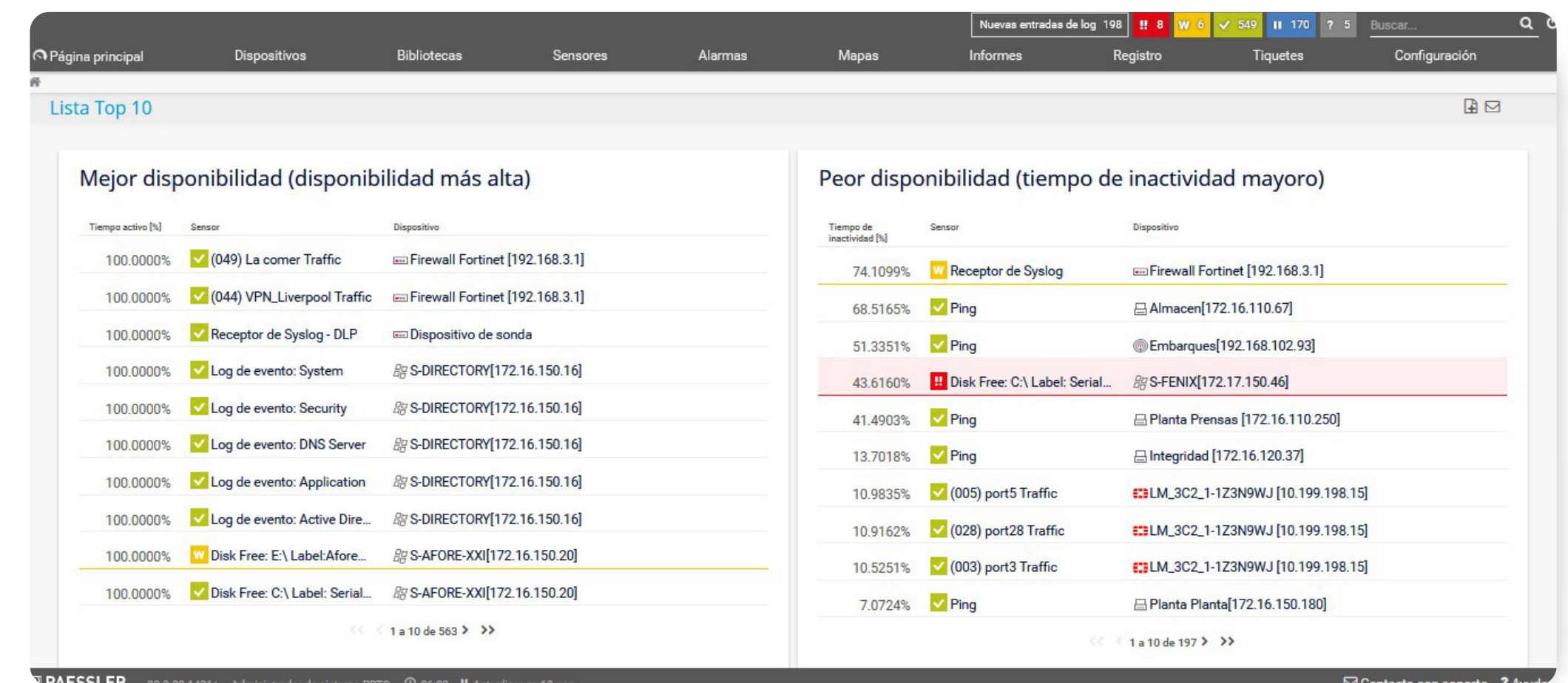
Licencias se venden por separado*
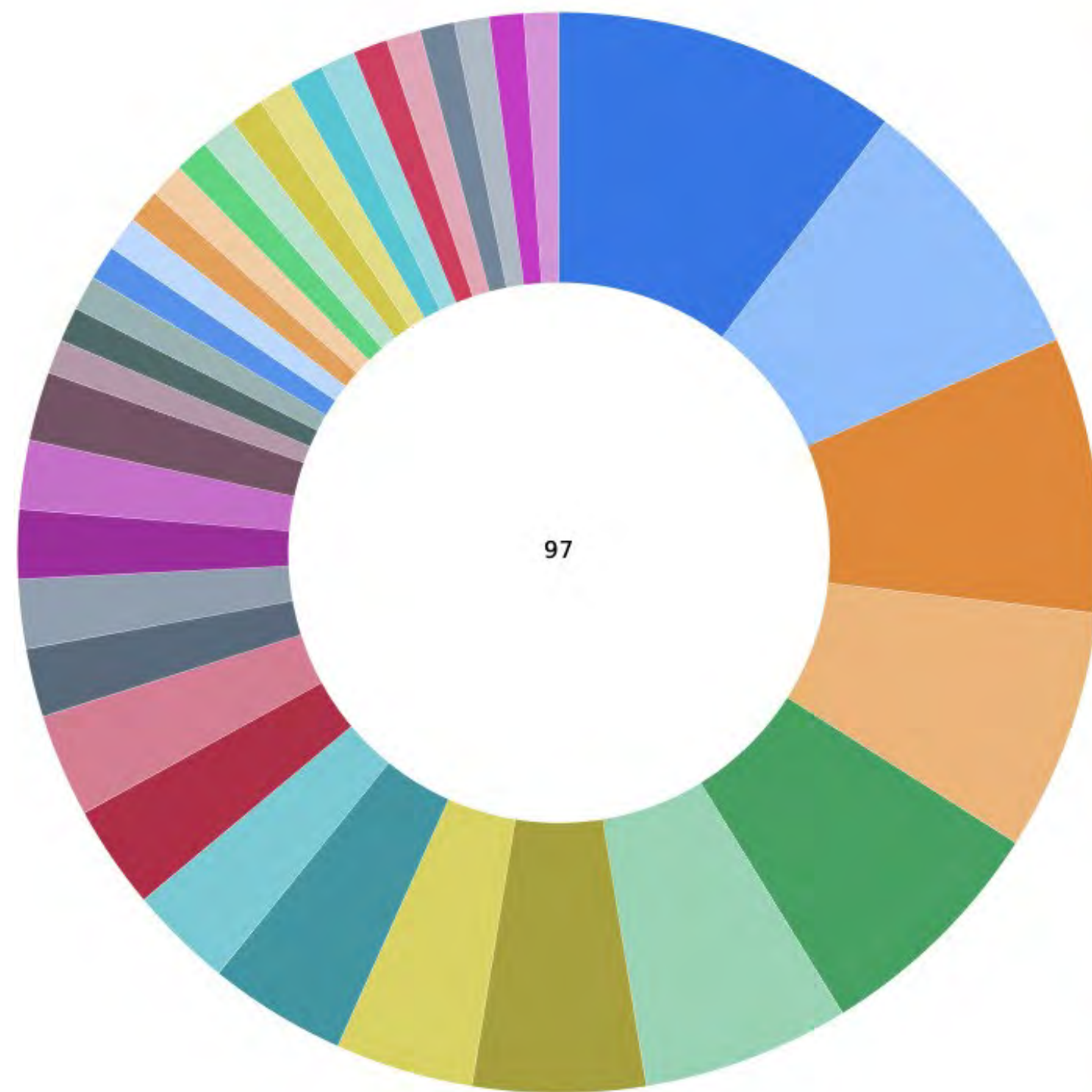
Legend:
- Sin acceso red wifi/ETH - 10 - 10.31%
- Equipo no enciende PC - 8 - 8.25%
- No responde impresora - 8 - 8.25%
- Error equipo PC - 7 - 7.22%
- Sin acceso internet - 7 - 7.22%
- Error perifericos PC - 6 - 6.19%
- Error aplicativo PC - 5 - 5.15%
- Atasco de Papel - 4 - 4.12%
- Torniquetes inactivos - 4 - 4.12%
- Acceso sitio(s) internet - 3 - 3.09%
- No lee tarjetas torniquetes - 3 - 3.09%
- No visualización - 3 - 3.09%
- Acceso carpeta compartida - 2 - 2.06%
- Ajustes escaner - 2 - 2.06%
- Atasco Papel - 2 - 2.06%
- Daño teléfono - 2 - 2.06%
- Liberación MEM/HDD SRV - 2 - 2.06%
- Accesos AD - 1 - 1.03%
- Agregar impresora - 1 - 1.03%
- Ajustes impresión - 1 - 1.03%
- Alerta/Detección AV - 1 - 1.03%
- Bandeja atascada - 1 - 1.03%
- Colocar contraseña correo - 1 - 1.03%
- Decarga información PC - 1 - 1.03%
- Desbloqueo de usuario AD - 1 - 1.03%
- Desbloqueo usuario AD - 1 - 1.03%
- Desconexión SRV - 1 - 1.03%
- Ejecutar privilegios admin AD - 1 - 1.03%
- Error CIM - 1 - 1.03%
- Impresora apagada - 1 - 1.03%
- Impresora desactivada - 1 - 1.03%
- Intermitencia Wifi - 1 - 1.03%
- Realizar ajustes de impresión - 1 - 1.03%
- Restablecimiento contraseña AD - 1 - 1.03%
- Restablecimiento contraseña correo - 1 - 1.03%
- Sin acceso servidor/aplicativo - 1 - 1.03%

Process Implementation

During the first phase, it will be possible to identify and classify the type of service requests that occur most frequently, considering the above, it is important to define and agree by both parties the SLAs defined and the KPIs that will rule the performance of the subsequent months.

With the mentioned above, a Service Desk will be implemented to process tickets addressed to IT, we will work on operational processes aligned with the requirements of the Information Security area and we will continue working on the optimization of the support flow to the end user.

Continuous improvement phases

Resource optimization

The steps to be taken will be evaluated to optimize the
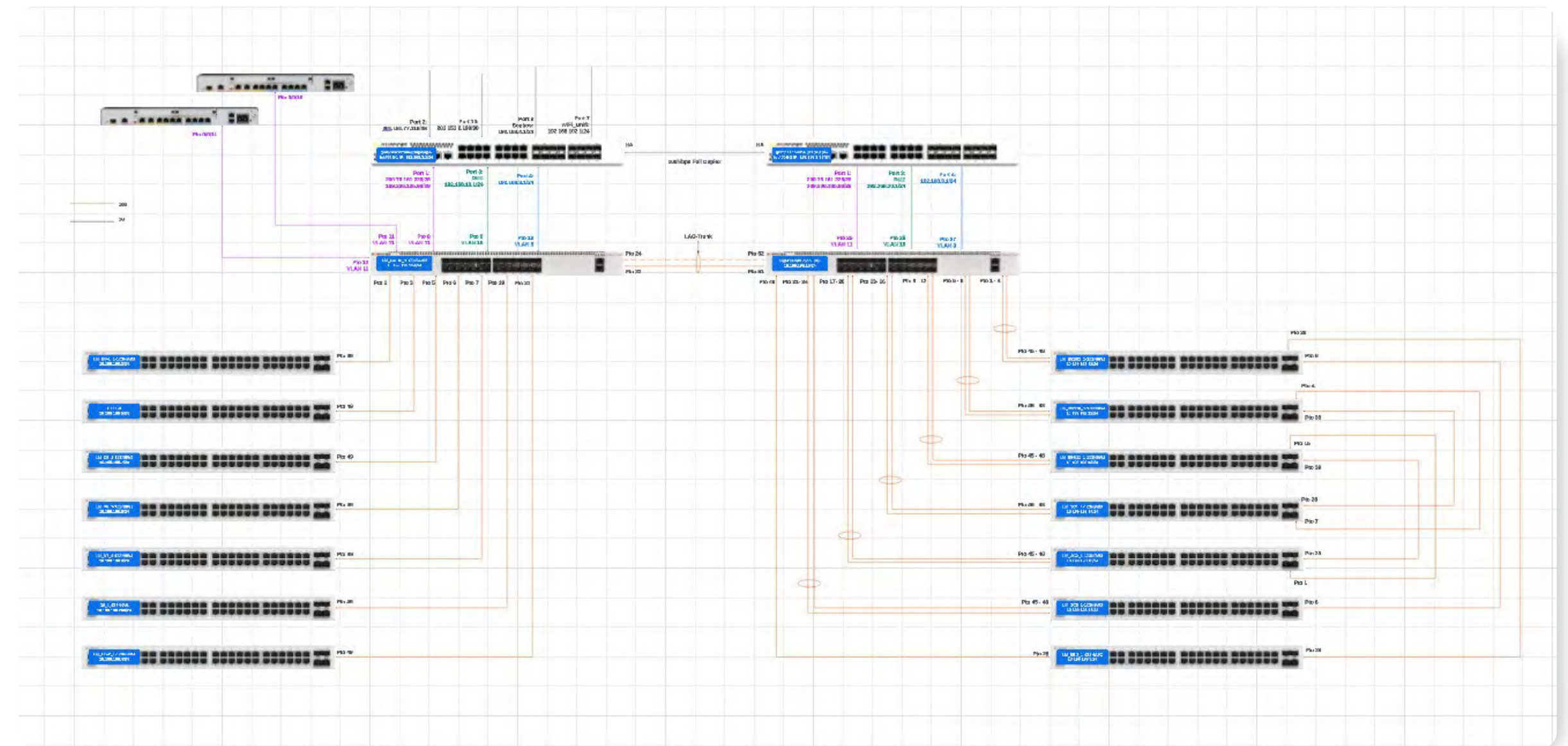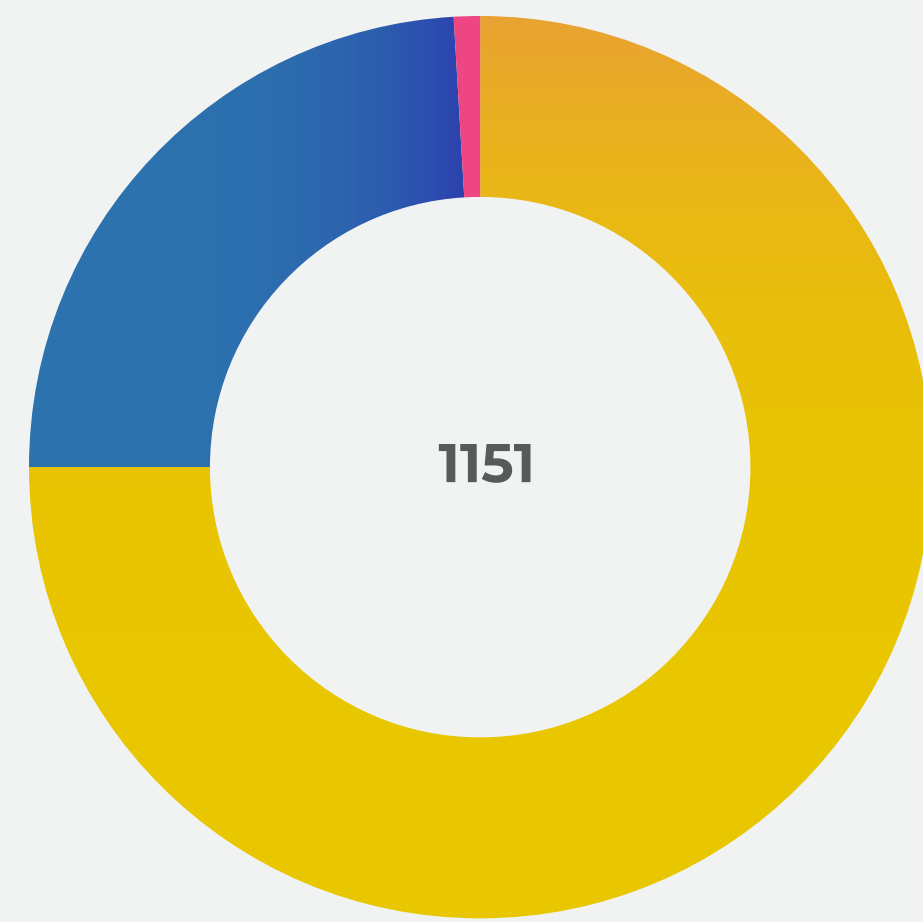use and utilization of the server
For example:

- ○ The implemented DRP logic, LAN network implications will evaluate
  whether it extends or if the current infrastructure is
  designed or no for this type of recommendation.

- ○ access to the storage unit

- ○ Identify whether the servers used are obsolete and whether they
   are supported or not.

Convergence
SERVICES

10
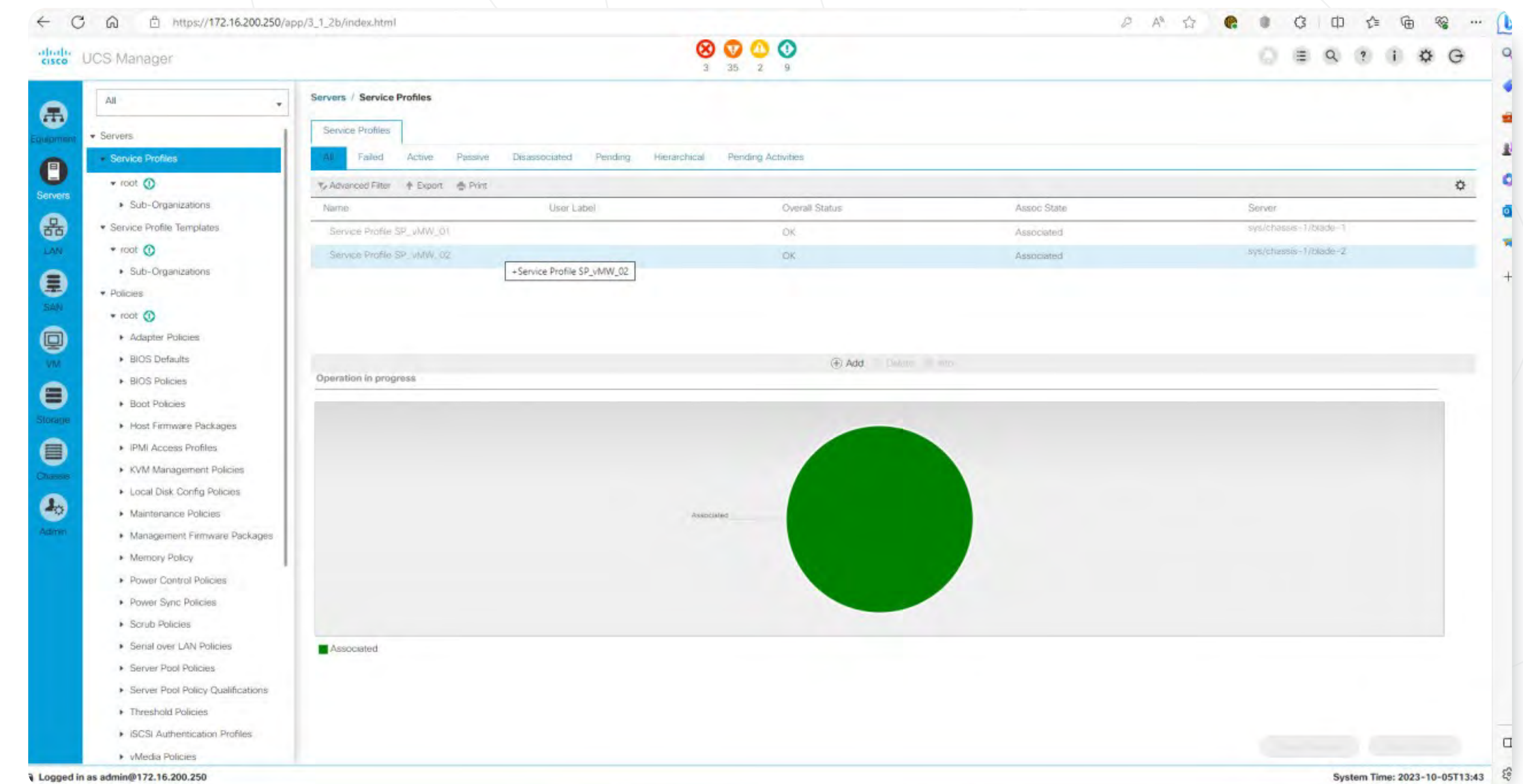
Network documentation

In case of finding deficiencies in the network, such as the lack of documentation and network diagrams, work will be done to update the documentation and generate network diagrams that will allow better control of the network.

Working Capital

Report generation in our web solution, for example:

- ⟳ Service metrics
- ⟳ Recurring schedules
- ⟳ Types of recurrence
- ⟳ Types of requirements
- ⟳ Analysis

Tickets by type

Service Request - 878 - **76.28%**
Alerta - 266 - **23.11%**
Incidente - 7 - **0.61%**

1151
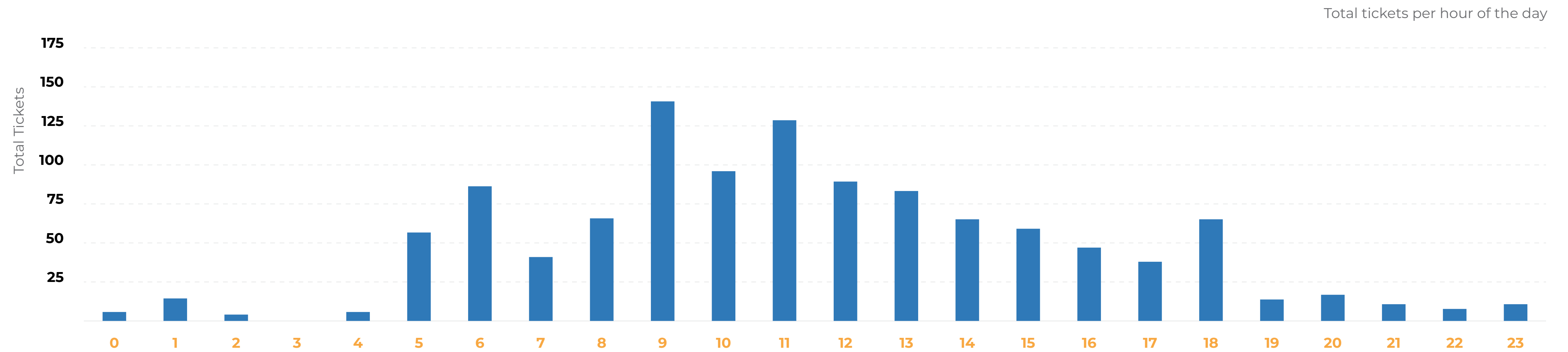
Total tickets per hour of the day

Business continuity strategy

Implementation of DRP, evaluate if the strategy and switching logic is in place, this is critical when building the policies and procedures that allow a proper business continuity.

It is highly advisable to work together with the client to determine what should be included in the strategy, and based on this, determine what additional actions or projects are required for its fulfillment.

Convergence
SERVICES

HA implementation services
High Availability services for your critical systems

○ It is common not to have an efficient High Availability scheme for the main site.

○ This is independent of the DRP strategy

○ Two Firewalls are proposed to enable High Availability

○ Integrates into the fiber optic connection, one more backup connection

○ The efficiency of the server will be evaluated and a replication service will be implemented.

○ Implement a backup strategy to enable proper control and monitoring of what is being backed up.

Convergence
SERVICES

14

Convergence
SERVICES

THANK YOU

✉ contacto@convergence-services.com   📞 +52 55 5555 5555

Customized proposals based on needs, legislation;
national and international