INTERNATIONAL PUBLIC TENDER No. CPI/02/2023

TENDER SPECIFICATIONS No. 12/IAVE/2023

Opening of the international public tender procedure for the acquisition and installation of a networking and security solution to support the design, writing, administration, marking and production of results regarding large-scale national assessment in a dematerialized environment.

CPV Classification: 32420000-3 – Network equipment
48820000-2 – Servers
48730000-4 – Security software package

PART I
Legal Clauses

Article 1
Object of the procedure

1. The object of the Tender Specifications of the present procedure is the acquisition and installation of:

1.1. **Wireless Solution**

The aim is to upgrade the wireless network currently existing at IAVE, I.P. according to a standardized and stratified model in watertight logical layers, with clearly defined responsibilities and capabilities, which will allow, on the one hand, to optimize investment in the network and, on the other hand, to guarantee flexible implementation and maintenance, with the ability to granularly adapt to the high-level concepts applied to the intrinsic reality of each site/functional layer.

To this end, IAVE, I.P. intends to acquire the following equipment:

Type	Description	Quantity
Wireless Controller	Wireless Controller	1
Access Point	Access Point	30

1.2. **Switching Solution**

The aim is to upgrade the switching network currently existing at IAVE, I.P. according to a standardized and stratified model in watertight logical layers, with clearly defined responsibilities and capabilities, which will allow, on the one hand, to optimize investment in the network and, on

the other hand, to guarantee flexible implementation and maintenance with the ability to granularly adapt to the high-level concepts applied to the intrinsic reality of each site/functional layer.

To this end, IAVE, I.P. intends to acquire the following equipment:

Type	Description	Quantity
Management	Management Platform	1
Type 1 Switch	Core Switch	2
Type 2 Switch	48 Port Switch	9
Type 3 Switch	48 Port mGig Switch	5
Transceivers	Enterprise Class Multimode	26
Transceivers	Enterprise Class Single mode	16

1.3. **Security Solution**

The aim is to upgrade the security infrastructure currently existing at IAVE, I.P. according to a standardized and stratified model in watertight logical layers, with clearly defined responsibilities and capabilities, which will allow, on the one hand, to optimize investment in the network and, on the other hand, to allow flexible implementation and maintenance with the ability to granularly adapt to the high-level concepts applied to the intrinsic reality of each site/functional layer.

To this end, IAVE, I.P. intends to acquire the following equipment:

Type	Description	Quantity
Server	Virtualization Support Server	1
Switch	Perimeter Switch	2
Firewall	Perimeter Firewall	2
Access control	Access control	1
MFA	Multi Factor Authentication	500
Analytics	IOT Probe	1

The execution of all services inherent to after-sales services are considered to be covered by the object of this procedure., in accordance with the specifications described in article 23 of these specifications.

Article 2

Format and contractual documents

1. The contract to be signed includes the following documents:
   a) These Tender Specifications;
   b) Correction of errors and omissions in the specifications identified by the tenderers, provided that these errors and omissions have been expressly accepted by the body responsible for the decision to contract;
   c) Clarifications and corrections relating to the specifications;
   d) The awarded tender;

e) Clarifications on the awarded tender provided by the successful tenderer.

2. In case of divergence between the documents referred to in the previous paragraph, the prevalence is determined in the order set out therein, without prejudice to the application of the principle of prevalence revised in article 51 of the Public Contracts Code, henceforth only PCC.
3. In case of divergence between the documents referred to in paragraph 1 and the clauses of the contract and its annexes, the former will prevail, except for suggested adjustments, in accordance with the provisions of article 99 of the PCC and accepted by the successful tenderer, and in accordance with the provisions in article 101 of the PCC.
4. In addition to the documents referred to in paragraph 1, the successful tenderer is also obliged to respect, where applicable, the European and Portuguese norms, specifications and approval by official bodies and manufacturers or entities holding patents.

Article 3
Good faith

1. The parties undertake to act in good faith in the performance of the contract and not to exercise the rights provided for therein, or in the law, in an abusive manner.

Article 4
Place, mode and time period for the performance of the contract

1. The contract to be signed will be in force under the terms set out in its clauses, and must be executed within a maximum of 60 (sixty) days, without prejudice to the period foreseen for technical assistance.
2. The goods and services that are object of the contract must be made available at Instituto de Avaliação Educativa, located at Travessa Terras de Sant'Ana 15, 1250-269 Lisboa.

Article 5
Base price

1. The base price, established in accordance with article 47 of the CCP, is €743,502.82, (seven hundred and forty-three thousand, five hundred and two euros and eighty-two cents), amount to which VAT is added at legal rate in force.
2. The definition of the base price is based on preliminary market consultations, in which three companies were consulted. The base price results from the average of the amounts proposed by these companies to IAVE, I.P.

Article 6
Payment conditions

3. Payments will be made within a maximum period of 60 (sixty) days after acceptance and verification, by IAVE, I.P., of the conformity of the goods and services supplied and the receipt of the respective invoices.
4. Under no circumstances will there be advance payment.

5. In case of disagreement on the part of IAVE, I.P. regarding the values indicated in the invoices, the respective reasons must be communicated in writing to the successful tenderer, who is obliged to provide the necessary clarifications or issue a new corrected invoice.
6. Invoices must contain the commitment number generated by the contracting authority in accordance with the law, as well as the description of the goods and services.
7. Provided they are regularly issued, and in compliance with the provisions of the preceding paragraphs, invoices are paid by bank transfer to the IBAN indicated by the tenderer, upon filling in the supplier form.

Article 7

Obligations of the successful tenderer

1. The following are the obligations of the successful tenderer, in addition to others resulting from the provisions of this procedure and applicable legislation, which must be the subject of specific clauses to be included in the contract to be concluded:
   a) Ensure the delivery of goods and the provision of services as defined in these specifications and its annexes, as well as in other contractual documents;
   b) Communicate in advance to IAVE, I.P., any fact that makes the provision of any of the services subject to this procedure totally or partially impossible, or that implies non-compliance with any other obligations;
   c) Change the conditions underlying the provision of service agreed between the parties, through the signing of a written contract between them, only with prior written authorization from the contracting authority;
   d) Ensure all human and material resources that are necessary and indispensable for the performance of the contract;
   e) Ensure, in a correct and reliable manner, the information regarding the conditions under which the provision of goods and services will be carried out, and provide all the clarifications considered necessary by IAVE, I.P. within the appropriate time for this purpose;
   f) Report any fact occurred during the performance of the contract that is relevant to the normal provision of goods and services and to the contractual execution, namely, the change of company name or its legal representatives.

Article 8

Patents, licenses and registered trademarks

1. The successful tenderer is responsible for any costs arising from the use of registered trademarks, registered patents, licenses or other similar rights.

Article 9

Use of distinctive signs

1. Neither party may use the name, brands, commercial names, logos and other distinctive trade signs belonging to the other without prior written consent.

Article 10

Confidentiality

1. The successful tenderer will guarantee confidentiality regarding any information related to the activity of IAVE, I.P. that may become aware of due to the acquisition of the goods and services that are object to this contract.
2. Excluded from the duty of confidentiality referred to in the previous paragraph are information and documentation proven to be in the public domain on the date they were obtained by the provider of goods and services, or that the latter is obliged to reveal in legal proceedings, or at the request of regulatory authorities and other competent administrative entities.

Article 11

Data Protection Regulation

1. The successful tenderer undertakes to comply with all applicable legal provisions regarding the processing of personal data, as defined by Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April, 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation) and other applicable Community and national legislation, in relation to all personal data accessed within the scope or for the purposes of the provision of goods and services, namely, personal data of clients, workers, collaborators and suppliers of IAVE, I.P.
2. The parties acknowledge and accept that, in relation to all personal data to which the successful tenderer has access or is transmitted by IAVE, I.P. for the purposes of providing the goods and services:
   a) IAVE, I.P. will act as data controller (as defined in the General Data Protection Regulation), determining the purposes and terms of these data processing by the successful tenderer;
   b) The successful tenderer will act as a subcontracting authority (as defined in the General Data Protection Regulation), processing personal data in strict compliance with the instructions of the person responsible for processing this data;
   c) For this purpose, the processing of personal data is understood as the operations, with or without the use of automated means, carried out on the personal data of IAVE, I.P. employees, including the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transfer and/or provision to third parties, alignment, combination, blocking, deletion and destruction of the aforementioned data.
3. The successful tenderer undertakes, namely, not to copy, reproduce, adapt, modify, alter, delete, destroy, disseminate, transmit, disclose or, by any other person, make available to third parties the personal data accessed or transmitted by the data controller under this contract, without having been expressly instructed to do so, in writing, by the data controller or by the data subjects in the exercise of their respective rights.
4. Without prejudice to any other obligations provided for in this contract, the successful tenderer undertakes to strictly comply with the provisions of applicable legislation regarding the processing of personal data and, in particular:
   a) To treat them only in accordance with the instructions of IAVE, I.P., solely and exclusively, for the purposes of the present provision of the goods and services, complying with the established obligations on data protection;

b) To provide all necessary collaboration to clarify any issue related to the processing of personal data carried out under this contract/agreement and keep IAVE, I.P. informed of the processing of personal data;
c) To provide assistance to IAVE, I.P. , taking into account the nature of the processing and the information at its disposal, in order to ensure the obligations regarding the notification of violation of personal data, namely through communication, whenever possible, within 72 hours of becoming aware (of the occurrence) of any breach that occurs, and also providing collaboration with IAVE, I.P. in the adoption of measures to respond to the occurrence, investigating it and preparing notifications deemed necessary in compliance with the law;
d) To collaborate with IAVE, I.P. taking into account the nature of the processing and, as far as possible, adopt the technical and organizational measures referred to in this article, which include encryption or pseudonymization of personal data to reduce the risks for the data subjects in question, not excluding other possible data protection measures, and allowing IAVE, I.P. to fulfil the obligation to respond to requests from data subjects, allowing them to exercise their rights under the law;
e) Not to communicate personal data to third parties and service providers not authorized or not indicated by IAVE, I.P.;
f) Depending on the choice of IAVE, I.P. or the data subject, to delete or return personal data at the time of assignment of the contract, deleting and destroying any existing copies, unless the conservation or transmission of data is required by law;
g) To keep records of data processing activities carried out on behalf of IAVE, I.P. under this contract, in accordance with the requirements provided for by law;
h) To comply with all other legal provisions regarding the registration, transmission or any other processing operation of personal data provided for by law;
i) Not to transfer data outside the European Economic Area without the prior written consent of the person responsible for processing the data;
j) To provide the data controller with all the information necessary to demonstrate compliance with the obligations provided for by law in the respective scope, as well as to facilitate and contribute to audits, including inspections conducted by the data controller or another auditor mandated by the data controller;
k) To ensure that the personnel authorized to process personal data commit to confidentiality, and that they are aware of and undertake to comply with all obligations set forth herein.

5. The successful tenderer undertakes to implement the technical and organizational measures necessary to protect the personal data processed on behalf of IAVE, I.P. against their accidental or unlawful destruction, accidental loss, alteration, unauthorized dissemination or access, as well as against any other form of unlawful processing of this personal data.
6. The measures referred to in the previous paragraph must guarantee an adequate level of security in relation to the risks that data processing presents, the nature of the data to be protected and the risks, of varying probability and severity, for the rights and freedoms of the natural persons.
7. The successful tenderer agrees that access to personal data processed under this contract will be strictly limited to personnel who need this access for the purposes of fulfilling the obligations assumed herein.

8. The successful tenderer undertakes to communicate to the data controller any situation that may affect the processing of personal data or that in any way gives rise to non-compliance with legal provisions on data protection, and must also take all necessary measures and within its power to stop it immediately.
9. The successful tenderer will be responsible for any damage in which IAVE, I.P. may incur as a result of the processing, by the tenderer or its staff, of personal data or in violation of the applicable legal standards and the provisions of this contract, when such violation is attributable to the successful tenderer/contractor and jointly with its staff within the scope of the service provided, when the violation is attributable to the performance of the latter.
10. Whenever IAVE, I.P. receives a request for access or rectification of personal data or an opposition to its processing from the data subjects, the successful tenderer must provide assistance to the data controller through appropriate technical and organizational measures, in order to enable IAVE, I.P. to fulfil the obligation to respond to data subjects' requests and thus allowing them to exercise their legal rights.

Article 12
Amendments to the contract

1. The contract may be amended in accordance with articles 311 and 312, both of the PCC, namely, by:
   a) Agreement of the parties, which cannot be in a less solemn form than that of the contract;
   b) Abnormal and unforeseeable change in the circumstances on which the parties based their decision to contract, as long as the fulfilment of the assumed contractual obligations seriously affect the principles of good faith and are not covered by the risks inherent to the contract;
   c) Reasons of public interest arising from new needs or from a new consideration of existing circumstances, without prejudice to indemnities that may be due, in compliance with the law.

Article 13
Assignment of contractual position

1. The successful tenderer may not assign its contractual position without prior authorization from IAVE, I.P.
2. The successful tenderer will be authorized to subcontract a third party to collaborate in the provision of the goods and services, as long as it is ensured that this third party will comply with the provisions of the applicable legislation; this obligation must be the object of a written contract signed by the tenderer and this third part, in which the latter is bound to comply with the obligations arising from Regulation (EU) 2016/679 and other applicable legislation relating to personal data, and observe the essence, nature and purposes of the contract, in strict compliance with the duty of secrecy and confidentiality.
3. For the purposes of the authorization provided for in the previous paragraph, the assignee must present all the documentation required from the successful tenderer in this procedure, so that IAVE, I.P. can verify that the assignee is not in any of the situations provided for in article 55 of

the CCP, and that the assignment does not change the circumstances of compliance with contractual and legal obligations.

Article 14

Termination of the Contract

1. Failure by one of the parties to fulfil the obligations arising from the contract gives the other party the right to terminate the contract, under the terms set out in the applicable law, without prejudice to the corresponding legal indemnities and other general grounds for legally terminating the contract.
2. For the purpose of the provisions of the previous paragraph, definitive non-compliance exists when there is a delay in provision of goods and services for a period exceeding 10 working days, elapsed after a warning notice, which sets a deadline for compliance of never less than ten days.
3. Termination will come in effect upon prior notice, via registered letter with acknowledgment of receipt, sent at least 10 working days in advance, counting from the date of what is considered to be the definitive non-compliance, provided for in the previous paragraph of this article.
4. The termination of the contract does not affect the application of any pecuniary penalties, in accordance with the following article.

Article 15

Penalties

1. In the event of non-compliance with contractual obligations, the contracting authority may apply the following contractual pecuniary sanctions to the successful tenderer, depending on the severity or repetition of the infringement:
   a) For non-compliance with obligations relating to the duty of confidentiality, up to €1000.00 (one thousand euros), per infringement;
   b) Failure to comply with obligations relating to intellectual property and personal data, up to €1000.00 (one thousand euros), per infringement;
   c) For non-compliance with the duty to inform, up to €250.00 (two hundred and fifty euros), per infringement;
   d) For non-compliance with the determination addressed to the successful tenderer in accordance with these specifications, which include the obligations set out in Clause 1, up to €250.00 (two hundred and fifty euros), per infringement;
   e) For non-compliance with the obligations listed above, the aforementioned penalties may be applied, not exceeding 20% or 30% of the total amount awarded, depending on the case and, in accordance with the provisions of article 329 of the PCC.
2. Payment of any penalties incurred by the successful tenderer will be deducted from the net value of the second party's billing.
3. The application of the penalties provided for in this article will be the subject of a prior hearing, under the terms set out in paragraph 2 of article 308 of the PCC.
4. The successful tenderer will be notified, in writing, in order to make a decision within 10 (ten) working days. If the successful tenderer does not respond within the given period, the contracting authority applies the penalty in accordance with paragraph 2 of this article.

Article 16

Delay of the contracting authority

1. The delay in any payment does not determine the maturity of the remaining payment obligations.
2. In case of delay, payments due by the contracting authority bear interest at the legal rate, from the date on which they became due and until full payment, in accordance with article 326 of the PCC.
3. In case of disagreement over the amount due, the public contractor must make the payment based on the amount which the co-contractor agrees to.
4. The amounts contested by the contracting authority, and which are subject to correction, do not earn default interest in the event of non-payment.

Article 17

Acts of God or *force majeure*

1. Neither party will incur liability if it is prevented from fulfilling the obligations assumed in the contract due to unforeseeable circumstances or *force majeure*, understanding as such any circumstance that makes it impossible to perform it, beyond the control of the affected party, which could not have been known or foreseen on the date of signing of the contract, and whose effects the party was not reasonably required to circumvent or avoid.
2. The following may constitute *force majeure* if the requirements of the previous paragraph are met: namely, earthquakes, floods, fires, epidemics, sabotage, strikes, international embargoes or blockades, acts of war or terrorism, riots and injunctive governmental or administrative orders.
3. The following do not constitute *force majeure*:
   a) Strikes or labour conflicts limited to the companies of the second party or groups of companies of which it is part, as well as companies or groups of companies of its subcontractors;
   b) Circumstances that do not constitute *force majeure* for the subcontractors of the second party, in the part in which they intervene;
   c) Governmental, administrative, or judicial determinations of a sanctioning nature or otherwise resulting from non-compliance by the second party with duties or burdens that fall upon it;
   d) Popular demonstrations resulting from the non-compliance, by the second party, of legal norms;
   e) Fires or floods originating in the premises of the second party, whose cause, spread or proportions are due to its fault or negligence or to non-compliance with safety standards;
   f) Malfunctions in the second party's computer or mechanical systems not due to sabotage;
   g) Events that are or should be covered by insurance.
4. The party that invokes unforeseeable circumstances or *force majeure* must immediately communicate and justify such situations to the other party, by any written means, as well as inform of the foreseeable period for re-establishing the situation.
5. *Force majeure* determines the extension of the deadlines for compliance with contractual obligations that are affected during the period of time demonstrably corresponding to the impediment resulting from *force majeure*.

Article 18

Deadlines in the performance of the contract

1. The following rules are applied to establish deadlines in the performance phase of the contract:
   a) Deadlines are continuous, not suspended on Saturdays, Sundays and holidays;
   b) The deadline that falls on a Saturday, Sunday, holiday or on a day on which the service, before which the act must be carried out, is not open to the public, or does not operate during the normal period, is transferred to the first following working day.

Article 19

Signing of the written contract

1. In accordance with paragraph 1 of article 94 of the PCC the contract will be in writing.

Article 20

Communications and notifications

1. All communications and notifications between the contracting authority and the successful tenderer must be made in writing, by post, email or fax, to the domicile or contractual headquarters of each, identified in the contract with sufficient clarity, to so that the recipient is aware of its nature and content.
2. Any change to the contact information contained in the contract, even if occasional or temporary, must be communicated immediately and in writing to the other party.

Article 21

Grounds for initiating the procedure

1. This public tender procedure is adopted in accordance with the provisions of paragraph a) of article 20, article 130 et seq. of the PCC, and the decision to contract was taken by the President of the Board of Directors, Luís Pereira dos Santos.

Article 22

Competent court

1. In everything that is omitted in these specifications, the provisions of the PCC and other applicable legislation and regulations will be observed.
2. The Lisboa district court has jurisdiction over any disputes arising from the contract, namely related to its interpretation, performance, non-compliance, invalidity, resolution or reduction.

PART II

Technical Clauses

Article 23
Technical specifications of the equipment

1. The technical features of the equipment that are object of the present Tender Specifications are detailed in the following clauses:

1.1. **Wireless Solution**

Full compatibility must be ensured between the equipment and software to be provided in this procedure.

The solution to be proposed must include the plugs and cabling necessary to connect all the equipment, in line with the best practices.

The solution to be acquired is based on the following assumptions:

- Distinction and control between internal customer (Corp) and external customer (GUEST).
- Visibility over access to network resources.

1.1.1. **Equipment and software to be acquired**

Type	Description	Quantity
Wireless Controller	Wireless Controller	1
Access Point	Access Point	30

1.1.1.1. **Wireless controller**

The wireless controller must provide redundancy to the existing controller, in order to allow high availability in the solution through a cluster and eliminating any single point of failure.

Below are the requirements to be met.

REQ	Requirements
1	The controller must be supported in IaaS environments on the Google and AWS public cloud platform, being made available via the respective Marketplace; the controller must be certified for AWS GovCloud environments
2	In private cloud environments it should be possible to implement the controller in the following hypervisors:
3	VMware ESXI;
4	Microsoft Hyper-V;
5	KVM.
6	It must support centralized topologies for control traffic and user traffic
7	It must support centralized topologies for control traffic and local topology for user traffic

Capacity	
8	Maximum number of access points – 6 000 per controller
9	Maximum number of clients – 64 000 per controller
10	Maximum transfer rate - 5 Gbps in central switching mode
11	Maximum WLANs – 4.096
12	Maximum VLANs – 4. 096
13	High availability topologies
14	IPv6
Wireless Norms	
15	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave 1 and Wave 2, 802.11ax
Wired, Switching and Routing Norms	
16	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
Data Norms	
17	RFC 768 User Datagram Protocol (UDP)
18	RFC 791 IP
19	RFC 2460 IPv6
20	RFC 792 Internet Control Message Protocol (ICMP)
21	RFC 793 TCP
22	RFC 826 Address Resolution Protocol (ARP)
23	RFC 1122 Requirements for Internet Hosts
24	RFC 1519 Classless Interdomain Routing (CIDR)
25	RFC 1542 Bootstrap Protocol (BOOTP)
26	RFC 2131 Dynamic Host Configuration Protocol (DHCP)
27	RFC 5415 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol
28	RFC 5416 CAPWAP Binding for 802.11
Security Norms	
29	Wi-Fi Protected Access (WPA)
30	IEEE 802.11i (WPA2, RSN)
31	Wi-Fi Protected Access 3 (WPA3)
32	RFC 1321 MD5 Message-Digest Algorithm
33	RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform
34	RFC 2104 HMAC: Keyed-Hashing for Message Authentication
35	RFC 2246 TLS Protocol Version 1.0
36	RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile
37	RFC 4347 Datagram Transport Layer Security (DTLS)
38	RFC 5246 TLS Protocol Version 1.2
Encryption Norms	
39	Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits
40	Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP)
41	Data Encryption Standard (DES): DES-CBC, 3DES

42	Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit
43	DTLS: AES-CBC
44	IPsec: DES-CBC, 3DES, AES-CBC
45	802.1AE MACsec encryption
Authentication, Authorization and Accounting (AAA) Norms	
46	IEEE 802.1X
47	RFC 2548 Microsoft Vendor-Specific RADIUS Attributes
48	RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)-TLS
49	RFC 2865 RADIUS Authentication
50	RFC 2866 RADIUS Accounting
51	RFC 2867 RADIUS Tunnel Accounting
52	RFC 2869 RADIUS Extensions
53	RFC 3576 Dynamic Authorization Extensions to RADIUS
54	RFC 5176 Dynamic Authorization Extensions to RADIUS
55	RFC 3579 RADIUS Support for EAP
56	RFC 3580 IEEE 802.1X RADIUS Guidelines
57	RFC 3748 Extensible Authentication Protocol (EAP)
58	TACACS support for management users
Management Norms	
59	Simple Network Management Protocol (SNMP) v1, v2c, v3
60	RFC 854 Telnet
61	RFC 1155 Management Information for TCP/IP-based Internets
62	RFC 1156 MIB
63	RFC 1157 SNMP
64	RFC 1213 SNMP MIB II
65	RFC 1350 Trivial File Transfer Protocol (TFTP)
66	RFC 1643 Ethernet MIB
67	RFC 2030 Simple Network Time Protocol (SNTP)
68	RFC 2616 HTTP
69	RFC 2665 Ethernet-Like Interface Types MIB
70	RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions
71	RFC 2819 Remote Monitoring (RMON) MIB
72	RFC 2863 Interfaces Group MIB
73	RFC 3164 Syslog
74	RFC 3414 User-Based Security Model (USM) for SNMPv3
75	RFC 3418 MIB for SNMP
76	RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs
77	RFC 4741 Base NETCONF protocol
78	RFC 4742 NETCONF over SSH
79	RFC 6241 NETCONF

80	RFC 6242 NETCONF over SSH
81	RFC 5277 NETCONF event notifications
82	RFC 5717 Partial Lock Remote Procedure Call
83	RFC 6243 With-Defaults capacity for NETCONF
84	RFC 6020 YANG
Management Interfaces	
85	Web-based: HTTP/HTTPS
86	Command-line interface: Telnet, Secure Shell (SSH) Protocol
87	SNMP
88	NETCONF
Radio frequency	
89	The controller must support multiple RF management profiles per group of APs, including the control over the assignment of the transmission of power and dynamic channel at 2.4 GHz and 5 GHz
90	The controller must identify and avoid interference through an analysis report on the impact of network performance
92	It must enable/disable 11ax resources per WLAN
93	It must support SSIDs per radio in Dual 5G
Application Recognition Control	
94	The controller must support application recognition per user and per WLAN, as well as bandwidth control
95	The controller's application recognition technology must support the export to third-party compatible formats, such as NetFlow v9
96	The controller must support new application signatures without updating controller software
Software	
97	The access point must proactively distribute the client connection before and after association and analyse the user condition in real time using RSSI data packet
98	The controller must support data and control data security with CAPWAP
99	The controller must support wireless roaming between controllers
100	The controller must maintain usage statistics per application per user and must be able to export for network analysis.
101	The controller must support built-in GUI management options of multiple languages
102	The controller must provide the connection quality status per client
103	Visibility of clients with random MAC addresses
High availability	
104	The high availability mode must allow for geographically dispersed installation among controllers
105	Controller failover must not trigger client deauthentication and reassociation
106	The keepalive interval must not exceed 100 msec.
107	The controller must support software patching on the WLC in order to fix bugs, without the need for reloading
108	The controller must support AP software patching to fix bugs, no reload needed to fix bugs

109	The controller must support new AP hardware without the need to update all the controller software
110	The redundant controller must synchronize the access point and client status, including the clients' DHCP IP concession status
BYOD & Security	
111	The controller must be able to incorporate a customized webpage portal (HTML) in order to fully personalize the user's experience.
112	The controller must provide rule-based classification of rogue apps and perform mitigation actions.
113	The controller must be able to detect the user device connections to the rogue access point and contain it.
114	The controller must support content security using DNS integration; web classification must be fully customizable.
115	The system must support control plane encryption in IPv4 and IPv6.
116	The update of the controller image must be done via secure encrypted transport.
117	The controller must be able to provide unique pre-shared keys to devices that do not support the 802.1x security protocol
118	The controller must provide FIPS-140/CC certification, including pending certification
119	The controller must support PSK Identity
120	The controller must be able to disable clients with random MAC addresses
Network Configuration	
121	The controller must support mapping of specific VLANs for single SSID, depending on the location of the access point and of the user.
122	The controller must support automatic VLAN assignment by SSID for the load-balanced user connection.
123	The controller must support packet fragmentation between the access point and communication with the controller.
QOS/Voice/Video	
124	The access point must be capable of supporting fast roaming based on 802.11r and generic WPA2 devices under the same SSID.
125	The controller must be able to prioritize the Skype4Business call with a prioritization policy of applications per user.
126	The access point must postpone channel scanning due to high priority traffic activity.
127	The access point must be compatible with bandwidth-based call admission control.
128	The controller will provide options to choose a reliable QoS rating from multiple sources (DSCP, UP) and maintain the priority rating over the network.

1.1.1.2. Access points

Below are the requirements to be met.

REQ	Requirements
Interfaces	
1	1x 100, 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz

2	Management console port (RJ-45)
Architecture	
3	Management in centralized controller
4	Local and independent management
5	Embedded controller for managing other access points
6	50 access points, 1000 clients
Capacity	
7	Maximum number of access points - 6.000 per controller
8	Maximum number of clients – 64.000 per controller
9	Maximum transfer rate - 5 Gbps in central switching mode
10	Maximum WLANs – 4.096
11	Maximum VLANs – 4. 096
12	High availability topologies
13	IPv6
802.1n version 2.0 norm	
14	4x4 MIMO with four spatial streams
15	Maximal Ratio Combining (MRC)
16	802.11n and 802.11a/g beamforming
17	20- and 40-MHz channels
18	PHY data rates up to 890 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz)
19	Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive)
20	802.11 Dynamic Frequency Selection (DFS)
21	Cyclic Shift Diversity (CSD) support
Norms 802.1ax	
22	4x4 MIMO with four spatial streams
23	4x4:4 on 5 GHz with MU-MIMO and downlink/uplink OFDMA
24	4x4:4 on 2.4 GHz with MU-MIMO and downlink/uplink OFDMA
25	Combined data rate of 5.2 Gbps
26	Built-in BLE radio (Bluetooth 5.0)
27	Supports up to 500 Wi-Fi devices
28	Uplink/downlink OFDMA
29	TWT
30	BSS colouring
31	MRC
32	802.11ax beamforming
33	20-, 40-, 80-, and 160-MHz channels
34	PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz)
35	Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive)
36	802.11 DFS
37	CSD support
38	WPA3 support

Functionalities	
39	The access point must be able to support the VXLAN protocol
40	The access point must be ready for IoT (BLE)

1.2. Switching Solution

It must be ensured that there is total compatibility between the equipment and the software to be supplied according to this procedure, including the transceivers.

The solution to be acquired is based on the following assumptions:

- Functionalities Layer2/3
- Uplinks at 10G/25G
- Downlinks mGig
- To support stack
- 48 PoE+ ports

1.2.1. Equipment and software to be acquired:

Type	Description	Quantity
Management	Management Platform	1
Type 1 Switch	Switch Core	2
Type 2 Switch	48 Port Switch	9
Type 3 Switch	48 Port mGig Switch	5
Transceivers	Multimode Enterprise Class	26
Transceivers	Single mode Enterprise Class	16

1.2.1.1. Management Platform

A single management system must be provided that will allow the centralized management of network elements, capable of managing switches, routers, wireless access points and wireless controllers.

The management system must allow installation in a virtualized Vmware ESXi and Hyper-V environment.

Along with the platform, the necessary licensing must be provided for the equipment to be supplied (switches, routers, wireless access points, wireless controllers).

The system must be capable of supporting the following functionalities:

REQ	Requirements
Functionalities	
1	To document the network and its modifications
2	To apply global modifications to the equipment
3	To back up settings automatically and regularly, enabling:

4	Viewing of the configuration history;
5	Comparison between configurations at different points in time;
6	Comparison of configurations between equipment;
7	Rollback of settings to previously saved settings.
8	To back up software images of network elements enabling:
9	Transfer of software images to/from network elements;
10	Activation of software images on network elements.
11	Visualization of network inventory
12	Network audit
13	To monitor faults and alarms
14	Email notification for fault and alarm categories
15	Support for management virtual domains with access management for different users
16	To monitor network performance
17	Intuitive web-based graphical interface
18	Visualization of the network topology, enabling:
19	Automatic link detection through LLDP;
20	Presentation of active alarms on network elements;
21	Support for views differentiated by location and with identification of the type of devices and number of devices per location;
22	Direct access to the element via telnet/SSH;
23	To make pings and traceroutes;
24	Visualization of maps based on the number of hops away from an element.
25	Support of contextual dashboards, allowing to quickly obtain information about:
26	Number of managed elements;
27	Type of elements managed (router, switch, access point, server, etc);
28	Failure alarms and event correlation;
29	Status of the interfaces (Up/Down) and their utilization rate;
30	Use of interfaces, CPU, memory, uptime, software versions;
31	Number of wireless clients connected by access point;
32	Number of wired and wireless clients connected to the network and details about them (IP, Mac Address, VLAN, element/port/AP to which the client is connected);
33	Top clients in terms of bandwidth usage;
34	Most used applications on the network at the L7 level (Gmail, Office365, Skype, etc);
35	Most used applications by site, equipment, interface and user;
36	Top clients in terms of bandwidth usage per application at L7 level;
37	Support for templates of network element configuration; templates must be able to be applied to several network elements simultaneously;
38	Inclusion of base of configuration template for:
39	802.1X
40	Access-Lists
41	Interface configuration

42	LACP configuration
43	VLAN configuration
44	Logging, SNMP, NTP, DNS configuration
45	Radius, TACACS+ configuration
46	Spanning-Tree configuration
47	Routing protocols configuration
48	VPN configuration
49	Flow export configuration (Netflow or similar)
50	QoS configuration
51	L7 Application Visibility Configuration (Gmail, Office365, Skype, etc.)
52	Support for the creation of "jobs" with tasks for implementing changes to the configuration of network elements. These "jobs" may be defined to be executed at a specific future time (day/hour);
53	Support for carrying out a packet capture directly on the management platform, which allows the network to have sniffer's functionality in real time;
54	Wireless controller configuration support;
55	High availability configuration support in wireless controllers;
56	Support for the configuration of equipment that has LAN and WLAN integration in a unified way, allowing to manage the configuration of the switching and wireless component in a single authority
57	Access point configuration support in standalone and controller-based mode;
58	To support identification of the following parameters for endpoints in wireless environments:
59	MAC address;
60	IP address (IPv4 and IPv6);
61	VLAN;
62	Authentication type;
63	Vendor;
64	Endpoint location;
65	Name of the access point;
66	Name of the associated wireless controller;
67	To support the identification/statistics of the following parameters in a wireless environment:
68	RSSI (history);
69	Tx/Rx packets and bytes;
70	Air quality statistics on 802.11 a/b/g/n/ac;
71	Identification of the number of clients on each radio: 2.4GHz and 5GHz;
72	History of associations by access points;
73	Duration of associations;
74	SSID;
75	Troubleshooting of association steps:
76	802.11 association;
77	802.1X authentication;
78	Address assignment;

79	Final result association.
80	Identification of rogue APs and interference, namely Bluetooth;
81	In a wireless environment, support for integration with systems that track the location of endpoints;
82	Support for the inclusion of building plans, enabling:
83	Visualization of the location of access points and endpoints;
84	Visualization of predicted wireless coverage (heat maps);
85	Optimization of wireless coverage through the simulation of adding/removing access points and obstacles.
86	Support for the definition of several management platform administration profiles, allowing for different access privileges to network assets;
87	Support for integration with LDAP systems and access control systems;
88	Support for the integration of equipment from different vendors.

1.2.1.2. Type 1 switch

Below are the requirements to be met.

REQ	Requirement
Physical characteristics	
1	Fixed ethernet equipment L2/L3
2	Dimensions: 1RU
3	12 x ports 1/10/25G SFP28
4	Support for the following SFP+ type optics
5	Support for the following SFP type optics
6	The equipment must be able to support the following modules:
7	8 x Multigigabit ports (1/2,5/5,10G)
8	8 x SFP28 ports (1/10/25G)
9	2 x 40/100G ports
10	Flash support with a minimum of 16GB to save settings and logs
11	Support Capacity for DC and AC power supply
12	Support capacity for external storage of up to 240G SSD
13	Stacking support through a dedicated module, ensuring the capacity for a minimum of 8 devices to be managed as a single device, through a single management address
14	The architecture of the equipment and the stack must be the same between the stack elements
15	Support stacking between equipment with different access port densities, with and without PoE
16	Support for power sharing between stack elements
17	Stateful switchover support, when switching from active to standby in a stack
18	Support for redundant and hot-swappable power supplies (included)
19	Support for redundant and hot-swappable fans
20	Equipment-embedded RFID support for asset management

21	Support of 128 Port-Channels allowing for up to 16 members per port-channel
22	Blue Beacon support for switch identification
Scalability and Performance	
23	Minimum switching capacity: 1T Gbps
24	Minimum forwarding capacity:744.0 Mpps
25	Minimum stack bandwidth throughput capacity: 1Tbps
26	Minimum number of VLAN IDs: 4094
27	Minimum number of SVIs: 1000
28	Minimum number of router ports per stack: 448
29	Minimum number of MAC Addresses: 32000
30	Minimum number of IPv4 routes: 39000
31	Minimum number of IPv6 routes: 19500
32	Minimum number of ACL entries: 5000
33	MST instances: 64
34	RSTP/PVSTP instances: 256
35	Jumbo Frames support
36	Support of a minimum of 16MB of buffers
37	Support up to 64 000 network streams in hardware, with the ability, through flows:
38	To identify Top Talkers;
39	To customize flows by user profile;
40	To use multiple collectors;
41	To export bandwidth consumption, depending on the number of flows;
42	To export information from flows in netflow v9 or IPFIX.
Functionalities	
43	Support for LLDP
44	LACP 802.3ad support
45	Web management support
46	LACP support through different stack members
47	Support for IPv6 in hardware
48	Support for 8 egress queues per port
49	802.1ad support (QINQ)
50	Selective QINQ or Vlan Mapping support
51	ACL support
52	STP, RSTP support
53	VRRP support
54	HQoS, WRED, CBWFQ support
55	MACSec (802.1AE) support with 128-bit encryption on all interfaces
56	MACSec (802.1AE) support with 256-bit encryption on all interfaces
57	IP SLA Support capacity
58	NAT and PAT support
59	IPSEC support, supporting up to 100G hardware performance
60	IP SLA Responder support
61	IPv4 and IPv6 static route support

62	RIPv1, RIPv2, RIPnG support
63	OSPFv2 and OSPFv3 support
64	Inter-vlan routing support
65	BGP and IS-IS support
66	PBR support
67	GRE tunnels support
68	EoMPLS support on GRE tunnels
69	PBR support with VRF visibility
70	MPLS Layer 3 VPN support
71	MPLS Layer 2 VPN support
72	MPLS Multicast VPN support
73	VRF-Lite support
74	BGP EVPN on VXLAN support
75	VXLAN support
76	NETCONF/YANG and RESTCONF support
77	Support for hosting third party applications in containers directly on the switch
78	Python support
79	Patching support for fixing bugs without need to install new software images
80	Support for Port Mirroring and sending monitored traffic to remote equipment over an L3 network
81	Support for capturing traffic flows in IPFIX format or similar in hardware and without resorting to packet sampling
82	Flow detection support at application level - Layer L7. Examples of applications: Facebook, Skype, Yahoo, Http, Https/ssl, Youtube
83	Support for applying QoS policies at the application level - Layer 7. Examples of applications: Facebook, Skype, Yahoo, Http, Https/ssl, Youtube
84	Support for VLAN ACLSs
85	Support for Port Based ACLs
86	Support for DAI (Dynamic ARP inspection)
87	Support for Port security
88	Support for 802.1X
89	Support for 802.1X with Change of Authorization
90	Support for 802.1X with downloadable ACLs
91	Support for 802.1X with guest VLAN
92	Support for web authentication for clients non-802.1X
93	Support for RADIUS Authentication, Authorization and Accounting
94	Support for TACACS Authentication, Authorization and Accounting
95	IGMP support
96	PIM Stub support
97	PIM-BIDIR, DM, SM and PIM SSM support
98	SSHv2 support
99	SNMPv3 and Syslogs support
100	Malware identification support in encrypted traffic

101	Support of security features to defend the integrity of the switch hardware and software, namely:
102	Image signing to ensure software image authenticity;
103	Secure switch boot based on immutable hardware chip (IEEE 802.1AR).

1.2.1.3. Type 2 Switch

Below are the requirements to be met.

REQ	Requirements
Physical characteristics	
1	Fixed Ethernet L2/L3 equipment
2	Dimensions: 1RU
3	48 1G ports with RJ-45 interface;
4	To support 48 15.4 W PoE ports (IEEE 802.3af) or 24 30 W PoE+ ports (IEEE 802.3at) without using external power (e.g., RPS), and only with a power supply on the equipment;
5	To support 48 PoE+30W (IEEE 802.3at) ports with the addition of redundant power
6	The equipment must have an uplink base with a minimum of 4-line rate 10G SFP+ ports;
7	Support for the following SFP+ optics (in uplink module)
8	10G Base SR, 10G Base LR, 10G Base ER, 10G Base ZR
9	Support of the following SFP type optics (in uplink module)
10	1000Base T, 1000Base SX, 1000Base LX/LH, 1000Base EX, 1000Base ZX
11	Flash support with a minimum of 4GB to save configurations and logs;
12	Capacity for stacking support through a dedicated module, ensuring the capacity for a minimum of 8 devices to be managed as a single device, through a single management address;
13	Capacity for stacking support through a dedicated module (devices that use the uplink for stacking are not allowed)
14	The architecture of the equipment and the stack must be the same between the elements of the stack
15	Ability to support stacking between devices with different access port densities, with and without PoE
16	Stateful switchover support capacity, when switching from active to standby in a stack
17	Support capacity for redundant and hot-swappable power supplies
18	Support capacity for redundant fans
19	RFID support embedded in equipment for asset management
20	Blue Beacon support for switch identification
21	Minimum MTBF: 346,200 hours
Scalability and Performance	
22	Minimum switching capacity: 176 Gbps
23	Minimum forwarding capacity: 130Mpps

24	Minimum stack bandwidth throughput capacity of 80 Gbps
25	Minimum number of VLAN IDs: 4096
26	Minimum number of SVIs: 512
27	Minimum number of MAC Addresses: 16 000
28	Minimum number of IPv4 routes: 3 000
29	Minimum number of IPv6 routes: 1 500
30	Minimum number of ACL entries: 1 500
31	6M Buffers Support
32	MST instances: 64
33	RSTP/PVSTP Instances: 128
34	Jumbo Frame Support: 9198 Bytes
35	Minimum number of multicast routing entries: 1 000
Functionalities	
36	LLDP support
37	Web management support (HTTPS) embedded in the equipment
38	LACP support - 802.3ad
39	LACP support through diferente stack members
40	Support for IPv6 in Hardware
41	Perpetual POE Support on Interfaces
42	Support for 8 egress queues per port
43	802.1ad support (QINQ)
44	Support capacity Selective QINQ or Vlan Mapping
45	ACL support
46	STP, RSTP support
47	Application Visibility capacity
48	VRRP Support
49	HQoS support, WRED
50	MACSec (802.1AE) support with 128-bit encryption
51	IP SLA support capacity
52	IP SLA responder support
53	IPv4 and IPv6 static route support
54	RIPv1, RIPv2, RIPnG support
55	OSPFv2 and OSPFv3 support
56	ISIS support capacity
57	Inter-vlan routing support
58	PBR support
59	VRF support capacity
60	VXLAN support capacity
61	NETCONF/YANG support
62	Patching support capacity to fix bugs without the need to install new software images
63	Support for capturing traffic flows in IPFIX format or similar in hardware and without using packet sampling

64	Support for up to 16,000 Full Flexible Netflow flows or equivalent
65	Ingress and Egress FNF support or equivalent
66	IPv4 and IPv6 VLAN ACLSs support
67	Support capacity of IPv4 and IPv6 Port Based ACLs
68	Support for DAI (Dynamic ARP inspection)
69	Support for port security
70	Support for 802.1X
71	Support for 802.1X with Change of Authorization
72	Support for 802.1X with downloadable ACLs
73	Support for 802.1X with guest VLAN
74	Support for web authentication for non-802.1X clients
75	Support for RADIUS Authentication, Authorization and Accounting
76	Support for TACACS Authentication, Authorization and Accounting
77	IGMPv1, v2 and v3 support
78	PIM Stub support
79	PIM, PIM-SM, PIM-SSM support capacity
80	SSHv2 support
81	SNMPv1, SNMPv2, SNMPv3 and Syslogs support
82	Support of Hardware and Software Integrity Protection Functionalities:
83	Software and Firmware Signing
84	Secure Boot

1.2.1.4. Type 3 Switch

Below are the requirements to be met.

REQ	Requirements
Physical Characteristics	
1	Fixed Ethernet L2/L3 equipment
2	Dimensions: 1RU
3	48 1G ports with RJ-45 type interface;
4	To support 48 15.4 W PoE ports (IEEE 802.3af) or 24 30 W PoE+ ports (IEEE 802.3at) without using external power (e.g., RPS), and only with a power supply on the equipment;
5	To support 48 PoE+30W ports (IEEE 802.3at) with the addition of redundant power
6	To support speeds of up to (1,2.5,5 and 10Gbps) on 12 of the RJ-45 ports;
7	The equipment must have an uplink base with a minimum of 4-line rate 10G SFP+ ports;
8	Support of the following SFP+ type optics (in uplink module):
9	10G Base SR, 10G Base LR, 10G Base ER, 10G Base ZR
10	To support of the following SFP type optics (in uplink module):
11	1000Base T, 1000Base SX, 1000Base LX/LH, 1000Base EX, 1000Base ZX

12	Flash support with a minimum of 4GB to save configurations and logs;
13	Capacity for stacking support through a dedicated module, ensuring the capacity for a minimum of 8 devices to be managed as a single device, through a single management address;
14	Stacking support capacity through a dedicated module (devices that use the uplink for stacking are not allowed);
15	The architecture of the equipment and the stack must be the same between the elements of the stack
16	Ability to support stacking between devices with different access port densities, with and without PoE
17	Stateful switchover support capacity, when switching from active to standby in a stack
18	Support capacity for redundant and hot-swappable power supplies
19	Support capacity for redundant and hot-swappable fans
20	RFID support embedded in equipment for asset management
21	Blue Beacon support for switch identification
22	Minimum MTBF: 337 300 hours
Scalability and Performance	
23	Minimum switching capacity: 391 Gbps
24	Minimum forwarding capacity: 290Mpps
25	Minimum stack bandwidth throughput capacity of 80 Gbps
26	Minimum number of VLAN IDs: 4096
27	Minimum number of SVIs: 512
28	Minimum number of MAC Addresses: 16000
29	Minimum number of IPv4 routes: 3000
30	Minimum number of IPv6 routes: 1500
31	Minimum number of ACL entries: 1500
32	Support of 12M Packet Buffers
33	MST instances: 64
34	Instances of (RSTP/PVSTP): 128
35	Jumbo Frame Support: 9198 Bytes
36	Support of 48 Port-Channels with support of up to 16 members per port-channel
Functionalities	
37	LLDP support
38	LACP support - 802.3ad
39	LACP support through different stack members
40	Perpetual POE support on Interfaces (not removed with reboot)
41	Support for 8 egress queues per port
42	802.1ad support (QINQ)
43	Support capacity Selective QINQ or Vlan Mapping
44	Support for IPv6 in Hardware
45	Support for 8 egress queues per port
46	ACL support
47	STP, RSTP support

48	Application Visibility capacity
49	VRRP Support
50	HQoS support, WRED
51	MACSec (802.1AE) support with 128-bit encryption on all interfaces
52	IP SLA support capacity
53	IP SLA Responder support
54	IPv4 and IPv6 static route support
55	Support of RIPv1, RIPv2, RIPnG
56	OSPFv2 and OSPFv3 support
57	IS-IS support capacity
58	Inter vlan routing support
59	PBR Support
60	NETCONF/YANG support
61	VRF support capacity
62	VXLAN support capacity
63	Support for SPAN and Remote SPAN
64	Patching support capacity to fix bugs without need to install new software images
65	Support for capturing traffic flows in IPFIX format or similar in hardware and without using packet sampling
66	Support of up to 32,000 streams.
67	Ingress and Egree FNF support
68	Support of IPv4 and IPv6 VLAN ACLSs
69	Support capacity of IPv4 and IPv6 Port Based ACLs
70	Support for DAI (Dynamic ARP inspection)
71	Support for port security
72	Support for 802.1X
73	Support for 802.1X with Change of Authorization
74	Support for 802.1X with downloadable ACLs
75	Support for 802.1X with guest VLAN
76	Support for web authentication for non-802.1X clients
77	Support for RADIUS Authentication, Authorization and Accounting
78	Support for TACACS Authentication, Authorization and Accounting
79	IGMP support
80	PIM, PIM-SM, PIM-SSM support capacity
81	PIM-Stub support
82	SSHv2 support
83	Support of SNMPv1, SNMPv2, SNMPv3 and Syslogs
84	Web management support (HTTPS) built into the equipment
85	Support of security features to defend the integrity of the switch hardware and software, namely:
86	Image signing to ensure software image authenticity

1.3. Security Solution

Full compatibility must be ensured between the equipment and software to be provided in this procedure, including transceivers.

The solution to be acquired is based on the following assumptions:
• Firewall
• Access control
• MFA
• IoT probe

1.3.1. Equipment and software to be acquired:

Type	Description	Quantity
Server	Virtualization Support Server	1
Switch	Perimeter Switch	2
Firewall	Perimeter Firewall	2
Access control	Access control	1
MFA	Multi Factor Authentication	500
Analytics	IOT Probe	1

1.3.1.1. Virtualization Support Server

In addition to the platforms, the purpose of this procedure is also the supply of HW (server) and SW (virtualization), necessary for the functioning of the solution in the proposed versions and in accordance with the manufacturer's requirements and recommendations.

IAVE, I.P. expects that the solution will be supported on virtualization and that the necessary servers will be proposed, in order to allow the correct functioning of the solution.

The solution to be proposed must include the plugs and cabling necessary to connect all the equipment in compliance with the best practices.

The proposed server must have the following specifications or equivalent:

- 2 x 2.4 GHz 6336Y/185W 24C/36MB Cache/DDR4 3200MHz
- 2 x 64GB DDR4-3200-MHz RDIMM/DRx4
- 3 x 1.2TB 12G SAS 10K RPM SFF HDD
- 1 x 4x 10/25G SFP28 Interfaces
- 2 x 1050W AC Power Supply for Rack Server
- Hypervisor system supporting virtual machines for centralized firewall management and access control.

1.3.1.2. Switch

Below are described the characteristics of the equipment to be acquired.

REQ	Requirements
Physical characteristics	
1	Fixed Ethernet L2/L3 equipment
2	8 dedicated ports for 10/100/1000 BaseT downlink with support for a minimum of 8 15.4 W PoE ports (IEEE 802.3af) or 8 30 W PoE+ ports (IEEE 802.3at), without resorting to external power (e.g. RPS), and only with a power supply on the equipment
3	The equipment must have 2 copper uplink ports and 2 1GE uplink ports with SFP type interfaces, supporting the following SFP types:
4	1000 Base T
5	1000 Base SX
6	1000 Base LX/LH
7	1000 Base EX
8	1000 base ZX
9	1000 BASE-BX10-D
10	1000 BASE-BX10-U
11	Support for having the equipment's 4 uplink interfaces working simultaneously regardless of whether they are GE or SFP
12	The switch must have a flash with a minimum of 128MB for storage
13	The switch must have a minimum of 512MB DRAM
14	USB interface support for storage and console port
15	Maximum power consumption with 0% throughput and without PoE ports of 23W
16	Maximum power consumption with 100% throughput and without PoE ports of 25W
17	Minimum MTBF: 528,480 hours
18	Support for mounting on Rack and DIN Rail
Scalability and Performance	
19	Minimum switching capacity: 92 Gbps
20	Minimum forwarding capacity: 68.4 Mpps
21	Support for a minimum of 4000 VLAN IDs
22	Support for a minimum of 1023 VLANs active simultaneously
23	Support for a minimum of 16000 MAC Addresses
24	Support for a minimum of 1000 entries in the IPv4 routing table
25	Support for a minimum of 1000 entries in the IPv6 routing table
26	Support of a minimum of 1000 IGMP groups
27	Support of 6 Port-channels with 8 members per port-channel
28	Support of jumbo frames 9198 Bytes
Functionalities	
29	VLAN support (IEEE 802.1Q)
30	IPv4 and IPv6 static route support
31	Support for inter-Vlan routing
32	RIP support

33	BGP, OSPF support
34	VRRP support
35	VRF support
36	LLDP support
37	PBR support
38	LACP support
39	Spanning-Tree, RSTP (802.1w) and MSTP (802.1s) support
40	DHCP v6 Client/Server/Relay support
41	Auto-MDIX support
42	Perpetual POE support
43	IEEE 802.1AE MACsec support
44	Port security support
45	Port support of ACLs IPv4 and IPv6 through VLAN
46	RADIUS support
47	RADIUS change of authorization support
48	Voice VLAN support
49	Support for simplified QoS configuration for voice on a port via a single command per port
50	802.1X support
51	802.1X with downloadable ACLs support
52	802.1X Guest VLAN support
53	802.1X support with dynamic VLAN assignment
54	Support of 802.1x multi-domain authentication (allowing a PC to be connected behind an IP phone, where the phone is in the voice domain and the PC is in the data domain)
55	802.1X MAC authentication bypass support
56	Web authentication support for non-802.1X clients
57	Multicast VLAN Registration (MVR) support
58	IGMP Snooping v1,v2,v3 support
59	IPv6 MLDv1 and MLDv2 snooping support
60	Support capacity PIM-SM, PIM-DM, PIM-SSM
61	Support up to 8 egress queues per port
62	Strict priority queuing support
63	Policer support per port
64	Port mirroring support
65	SSHv2 e SNMPv3 support
66	Plug-and-play agent support for automatic software image provisioning and configurations without user intervention
67	IPv6 host support (addressing, ICMPv6, SNMP for IPv6 objects, traceroute, SSH)
68	Support for capturing and exporting traffic flows (in Netflow v9 format) for traffic flow analysis tools, allowing you to detect security anomalies and top talkers
69	To allow, through the CLI, the plug and play of equipment connected to the switch, namely PCs, switches, APs, telephones, printers, without user intervention, automatically configuring/unconfiguring and adapting the VLAN parameters, QoS, port type to the type of device (access/trunk), spanning-tree, trunking protocol. When the device is disconnected

	from the port, the configuration should be removed automatically without user intervention. In the case of PCs and printers, detection based on MAC address and OUI (Organizational Unique Identifier) must be possible. This functionality must be implemented without having to resort to IEEE 802.1X
70	IEEE 802.3az Energy Efficiency Protocol Support
71	Native support for energy efficiency features, allowing, just from the software installed on the switch, to measure the energy consumption of equipment connected to the switch, and apply energy consumption optimization policies.

1.3.1.3. Firewall

Below are described the characteristics of the equipment to be acquired, which must include all the necessary licenses for the functionalities required.

REQ	Requirement
Architecture	
1	The same system must support the following operating modes:
2	Routed stateful firewall or transparent stateful firewall and IPS inline set (“bump in the wire” – without switching or learning MACs)
3	IPS inline set with Tap mode (1 single copy of the packet is inspected, but the IPS is inline)
4	IPS SPAN and ERSPAN interfaces.
Performance and Scalability	
5	FW + AVC Minimum: 3.3 Gbps
6	FW + AVC + NGIPS Minimum: 3.3 Gbps
7	Minimum concurrent sessions: 400 000
8	Minimum new sessions per second: 22 000
9	IPSEC VPN Minimum throughput: 1.4 Gbps
10	Minimum number of VPN peers: 400
Hardware	
12	Must support at least:
13	8 interfaces at 10M/100M/1GBASE-T Ethernet (RJ-45)
14	4 interfaces at 1G SFP
15	Serial port
16	USB port
17	HDD at 200GB
Identity Firewall	
18	The firewall must be able to authenticate users through LDAP or Active Directory groups as a condition of access control policies
19	The Firewall must be able to identify a passive user with 'traffic-based detection' through inspection of LDAP, AIM, Oracle, SIP, HTTP, FTP, MDNS, POP3, IMAP protocols
Intrusion Prevention System	
20	The system must have an IPS engine, which must be able to be activated through additional licensing
21	The IPS engine must be compatible with snort signatures and support customized rules

22	When activating the IPS engine there should be no degradation in firewall performance
23	The IPS mechanism must support different IPS policies and pre-processing (normalization and fragmentation) for each access control policy
24	IPS configuration policies must support a layered approach; modifications to the rule must be collected on top of the base layers provided by the manufacturer. These layers can be deleted or copied between policies
25	The system must have the following IPS policies by default: Connectivity under security, Balancing, Security under Connectivity and Maximum detection
26	The system should automatically suggest IPS rules to be applied according to the devices existing on the network and the known vulnerabilities for these devices
27	The system will be able to prioritize IPS events according to the relevance of the events to the client's infrastructure and the danger they pose
28	The system must be capable of detecting new applications and operating systems on the network and automatically suggesting new IPS rules to implement, in order to protect the organization against vulnerabilities existing in these applications and systems
29	'Dynamic Rule State' or a similar functionality must be supported, which allows to modify the actions of rules based on rate counters by Origin, Destination or both
30	Support of packets with latency thresholds that can cease packet inspection when the latency threshold is exceeded
31	The system must support automatic IPS signature updates
IPS Pre-processor	
32	The pre-processor must support protocol normalization and optionally certain attack detection functions before the IPS mechanism
33	It must be capable of defragmenting according to the following methods: Windows, BSD, BSD-right, HP-UX, MAC-OS, Linux, Cisco IOS and Solaris
34	It must prevent SYN attacks and control the maximum number of connections simultaneously on the network or on a device
35	The system must be capable of detecting and decoding packet data:
36	That exceeded the Length Value;
37	Invalid IP options;
38	Obsolete TCP options;
39	Protocol header anomalies.
40	The system must perform DCE/RPC, DNS, FTP, GTP, HTTP, SIP, SMTP, SSH, SSL, SunRPC, ModBus, DNP3 decoding and/or normalization
41	The system must be able to normalize and control TCP sessions; it must be able to control small segments, limit segment duplication, control timeouts, control the maximum TCP window size, detect session hijacking and control 'handshake timeout'
Application Visibility and Control	
42	The system must be capable of recognizing and controlling more than 4000 applications and micro applications by default
43	The system must support OpenAppID
44	The system must support the creation of simple application detectors through a GUI with static parameters and recognition of application characteristics through the import of captured packets
45	Application or application categorization must be available as a condition for access control policies
46	The system must have visibility over the devices and applications on the network, namely:
47	Applications used by the client

48	Operating system and respective version of servers and computers used on the network
49	Mobile devices
50	Browsers
51	Virtual machines
Host Detection and Profiling Capabilities	
52	The system must be capable to detect and create a profile for each host with passive and active methods (e.g., NMAP)
53	The management system must contain a vulnerability database that can be automatically compared to Host profiles
54	The host profile must include: IP addresses, MAC addresses, Last Seen timestamp, User (if available), Operating System, Server Services, Applications viewed, Host Protocols and relevant vulnerabilities
55	The system must be able to correlate active events of indications of compromise (IoC) with host profiles.
56	Host profiles must support customizable attributes.
Network Discovery and Traffic Profiling Capacities	
57	The system must be capable of discovering networks and creating traffic profiles for networks and zones.
58	Traffic profiles must be created based on network traffic inspected at the firewall and based on Netflow information through external Netflow exporters.
Anomaly Detection and Correlation	
59	The System must be capable of detecting anomalies in traffic profiles and user profiles
60	The system must be able to correlate events of IPS, Malware, files, hosts and new connections with events related to changes in host profiles and traffic profiles, and with this automatically apply measures to prevent these scenarios.
61	In case correlation events occur, the system must be capable of automatically activating standard and customizable remediation measures.
Reputation filtering, DNS sinkhole and Geolocation	
62	The system must support reputation feeds provided by the seller as well as customizable feeds.
63	The system must support and process reputation feeds through URL, domain and IP
64	Domain reputation must be checked before communication is initiated between an internal user and an external user.
65	The system must be able to drop or modify A and AAAA records when a request is made for blocked or suspicious domains.
66	The feed provided by the supplier must have multiple categories, including the following:
67	Attackers Bogon Bots CnC Dga Exploitkit Malware Open proxy Open relay Phishing Spam Suspicious Global Blacklist

	Global Whitelist
68	The system must be capable of using geolocation information to create reports, as a condition for access control policies and correlation policies.
Dynamic URL Filtering	
69	It must be possible through additional licensing to filter web pages. This functionality must:
70	Be able to determine the category and risk level of URLs.
71	Have automatic updates to the URL database and allow the system to consult a cloud platform in case a URL is not known.
72	Support at least 80 categories of URLs and the database behind this solution must include at least 280 million URLs.
Malware Protection and File Control	
73	The solution must contain an anti-malware engine with the following characteristics:
74	File and malware inspection must support HTTP, FTP, SMTP, POP3, IMAP and NetBIOS protocols.
75	The file inspection engine must be able to dynamically recognize file types.
76	It must be able to verify the structure of executable files and verify their structure against the provider's cloud service.
77	Traditional signature-based antivirus.
78	Cloud service that only checks hashes against the provider's cloud service.
79	It must be able to upload files for sandboxing in the cloud or through dedicated sandboxing appliances.
80	The system must be able to dynamically visualize the trajectory of files within the network through a temporal graph.
81	The management console must report the result of files sent to the sandboxing platform.
82	The system must support retrospective events; the system must be able to categorize a file as malware if it has passed through the system undetected and is later identified as malware. Retrospective alerts must be generated, and it must be possible to visualize events through a graph where it is possible to identify the entry point into the network, the file's trajectory within the network and the protocols used for this propagation.
Event and Asset Management	
83	The system must have widgets.
84	Widgets must be customizable.
85	The system must be able to maintain a dynamic network map.
86	The system must be able to log connection events based on inspected traffic and Netflow data exported from external network devices.
87	In addition to connecting events, the system must be capable of generating events when:
88	A new host is discovered or when the attributes of an existing host change;
89	An IPS signature triggers;
90	There is a direct correspondence to a malware or file policy;
91	There is a direct correspondence to policies or correlation rules;
92	There are changes in the system configuration;
93	There are changes in the health status.
94	The management system must have a single overview page that graphically displays detailed and interactive information on the status of the network, including data on applications, connections, geolocation, indications of compromise, intrusion events, hosts, servers, users, files (including files with malware) and relevant URL. This page should also allow you to filter what you want to see.

95	The management system must have pages with real-time data (or almost) on:
96	Malware events
97	File events
98	Captured file events
99	Connection events
100	Compromise indication events for hosts and network
101	Reputation-Based Filtering
102	Network host profiles
103	Application analysis
104	Analysis of user behaviour
105	Vulnerability analysis
Access Control Policies	
106	Access control policies should include:
107	Origin and destination zones
108	Source and destination networks
109	Ports of origin and destination
110	Applications
111	Reputation of URLs and Ips
112	URL categories and risk levels
113	VLAN Tag (for inline implementation)
114	Geolocation
115	The supported actions for access control must be at least:
116	Applying file and IPS inspection policies (different access control rules may have different IPS or file policies)
117	Logging the beginning and/or end of connections
118	Forwarding without any additional inspection
119	Blocking with TCP reset
120	Dropping the packet
121	Allowing interactive blocks for HTTP(S) so that the user can approve an Acceptable Use Policy to proceed with the connection.
122	Interactive blocking with TCP reset
SSL/TLS decryption	
123	The proposed device must be capable of decrypting, inspecting, and re-encrypting the data.
124	SSL/TLS decryption must be controlled by a policy that is reusable and that allows exceptions defined in rules.
125	SSL/TLS decryption should not be limited to HTTPS, other protocols that use SSL or TLS encryption should be supported.
Integration	
126	The solution must provide an API for integration with third parties.
127	API integrations must have the ability to use and manage third-party block lists
128	Pre-defined integrations for third-party solutions
129	The central management console must allow integration with: email and web security, endpoint security, network analytics, strong authentication, network access control solution and application security. It must also allow:

130	Orchestration and automation: must integrate with the various solutions mentioned and simplify security operations by allowing the creation and management of incident response workflows
131	Incident investigation and response: addressing indicators of compromise (IoC) and carrying out security investigations, providing information from intelligence sources, analyzing the risk and impact of these IoCs in the context of endpoints and with other indicators. Once the investigation materializes in a security incident, it should be possible to develop automatic workflows and remediation processes, such as blocking malicious IPs, domains, URLs and files.
132	Providing dashboards of the tools it integrates with
133	Providing single sign-on
Centralized management solution	
134	The centralized management solution must have a GUI.
135	The management solution must support environments – multi-tenant, multi-domain and RBAC (Role Base Access Control)
136	The management solution must support authentication through RADIUS or LDAP for administrators.
137	The management platform must allow centralized firmware upgrades for all platforms managed by it.
138	The management platform must manage licenses centrally.
139	The management platform must apply monitoring policies. These policies must include:
140	CPU Monitoring
141	Hardware module monitoring
142	Cluster status monitoring
143	Monitoring Disk Usage
144	Monitoring links and interfaces
145	Monitoring intrusion and file events
146	Monitoring of reputational information feeds collected from the cloud
147	Time synchronization monitoring

1.3.1.4. Access control

The aim is to acquire a system for controlling/identifying access to the network infrastructure, in compliance with security policies, and speeding up the troubleshooting/detection of security anomalies.

Below are described the characteristics of the platform to be acquired, which must include all necessary licenses for the functionalities required.

REQ	Requirements
1	This system must allow the obtainment of information in real time, contextualized information about the network, users and devices, fixed or mobile.
2	The system must be a single platform, with support capacity to guarantee AAA, posture, profiling, guest access management, TACACS and Enterprise Mobility Management capacities. Solutions that have these components segmented, on different equipment, are not accepted, as the aim is to provide a unified solution.
3	The system must be able to be acquired in the form of physical or virtual appliances. In the case of the virtual format, Vmware and Hyper-V must be supported.

4	Therefore, the system must comply with the following macro requirements:
5	Support for managing a base of 500 endpoints and with scalability to manage up to 500,000 endpoints
Compliance support	
6	Implement corporate management through a consistent access policy for all users, allowing monitoring, auditing and reporting;
Security Extension	
7	Extend security uniformly to the entire network infrastructure, ensuring consistent security policies that speed up the internal mobility of devices without requiring the reconfiguration of devices, depending on their location within the organization's network;
Increased efficiency	
8	Reduction of IT team OPEX, through centralized management, integrated with enforcement policies, combined with the dynamic registration of devices, corporate or guest users, thus guaranteeing the user experience;
Specific requirements	
9	AAA support for users and devices
10	Ability to ensure Endpoint Compliance, checking the posture of all devices connected to the network, including environments with 802.1X.
11	Trackability, profiling, policy-based control, and endpoint post-monitoring
12	Compliance record
13	Device lifecycle management
14	Context aware: The system should be seen on the network, as a “single source of truth”, ensuring the achievement of:
15	Connection status
16	User and device identification
17	Location
18	Time: hour at which the device connects/disconnects from the network
19	Device status
20	Ability to apply enforcement policies, regardless of the type of access: 802.1x wired, wireless, VPN
21	Allowing to define unified access policies regardless of how the device connects (cable, wifi or VPN)
22	Database for profiling equipment with automated updates
23	Possibility to define policies based on device type and user type
24	Allow deployment in 3 modes (monitoring mode, low impact mode and closed mode)
25	Web page (GUI) for centralized management. Ensuring centralized management for Wired and wireless devices
26	Support access control mechanisms:
27	802.1X
28	URL redirects
29	MAB
30	Web Authorization
31	Support for dynamically changing VLANs and for downloadable ACLs
32	RFC 3176/5176(CoA) Support
33	Support of multiple use cases:
34	Single-host
35	Multi-host
36	Multi authentication domain
37	Switch authentication to switch

38	Data/voice support on one port
39	Access control independent of topology;
40	Ensuring the confidentiality and integrity of the information, through IEEE 802.1AE(MACSEC) support. The access control/identification system has the capacity to function as an authentication and policy server, in communication between a mobile client and a switch in 802.1X
41	Supplicant provisioning and ensuring device onboarding for mobile devices such as iOS, Android and also workstations (PC, MAC)
42	To allow a monitor mode model in guest access and without implementing enforcement policies
43	RADIUS support for AAA
44	Support for authentication protocols such as:
45	PAP
46	EAP
47	PEAP
48	EAP-FAST
49	EAP-TLS
50	In the application of control associated with Posture, it must be possible:
51	To check OS patches
52	Antivirus
53	Spyware
54	PC self-remediation
55	To validate the existence of software with vulnerabilities (through integration with a vulnerability detection tool)
56	Periodic reassessment to ensure compliance with policies
57	Capacity of integration with MDM (Mobile device management)
58	Capacity for endpoint protection, allowing through device states:
59	Quarantine;
60	Shutdown.
61	Control of policies associated with IP phones, printers
62	The system must be scalable up to 500,000 devices, regardless of whether they are wired or wireless
63	The system must be able to collect information from the AD (Active Directory)
64	User notifications must occur without IT intervention, and the solution must be configurable in order to provide support numbers for clients
65	Device detection/isolation must be OS and HW agnostic
66	It must be possible to create customized exceptions to implemented policies, for groups of users
67	Support of non-802.1X clients
68	Support for certificates and ability to act as a CA (Certificate Authority) for BYOD environments
69	Support for TACACS+
70	At the monitoring level, it must be possible:
71	To add a security panel
72	To get compliance reports: DiaCAP, SOX, COBIT, HIPAA, PCI/DSS
73	Authenticated / unauthenticated / guest device inventory report
74	To report with timestamp, user name, IP, device name of authenticated and guest devices
75	To send alarms when policies are not applied through SNMP and syslog

1.3.1.5. MFA (Multi-Factor Authentication)

It is intended to acquire a multi-factor authentication tool to be used in the IAVE, I.P. infrastructure for a total of 500 endpoints.

Below are described the characteristics of the tool to be acquired, which must include all necessary licenses for the desired functionalities.

REQ	Requirement
1	The solution must allow users to register multiple devices for authentication
2	The solution must allow users to select a preferred device for authentication
3	The solution must allow users to select an alternate device (provisioned for that user) if the primary device is unavailable
4	The solution must allow users to securely manage their devices to reduce administrative workload configurable per user and application
5	The solution must support multiple authentication types: Mobile Push, Soft Token, SMS, Phone Call, U2F, Wearables, Biometrics and Hardware Tokens
6	The solution must support YubiKey tokens
7	The solution must be able to authenticate with a one-time password generated from a mobile application
8	The solution must provide bypass codes to authenticate
9	The solution must provide a second-factor authentication method that can work without any data or network connectivity
10	The solution must support IP/geolocation whitelisting
11	The solution must provide visibility into the security health of laptops and desktops
12	The solution must support U2F tokens for authentication in browser-based applications
13	The solution must enable customized policies to block or alert users with outdated browser software, in order to control risk, based on group or application
14	The solution must enable customized policies to block or strengthen authentication for users in specific geographic locations, in order to control risk, based on group or application
15	The solution must enable customized policies to block users with devices with jailbreak/root, in order to control risk, based on group or application
16	The solution must monitor and optionally prevent authentication attempts originating from known anonymous IP addresses, such as those provided by TOR and I2P, HTTP/HTTPS proxies, or anonymous VPNs
17	The solution must apply policies based on the user's location
18	The solution must provide automatic provisioning tools to synchronize Active Directory users
19	The solution must allow users to be added via a CSV import
20	The solution should allow administrators to enable a self-enrolment process for end users to reduce deployment times
21	The solution should allow administrators to generate a single-use bypass code based on the appropriate rights
22	The solution should allow administrators to configure outgoing caller ID for phone call authentication
23	The mobile application must support Apple iOS, Google Android, Palm, Windows Phone 7, Windows Mobile 8.1 and 10 and J2ME/Symbian
24	The solution must provide the ability to export logs to a third-party SEIM
25	The solution must support role-based administration controls for administrators

26	The solution should provide a dashboard overview of devices at risk based on outdated operating systems, browsers or plug-ins
27	The solution must allow personalized branding with a corporate logo
28	The solution must be able to identify unmanaged devices that access internal applications
29	The solution must provide reporting on managed versus unmanaged devices accessing any on-premises and cloud-based applications
30	The solution must allow the creation of security policies for unmanaged devices that access specific applications
31	The solution must integrate with the existing MDM solution in order to identify trusted and unmanaged devices
32	The solution should allow pilot group testing of users and prevent applications from accessing their unmanaged devices without impacting the rest of the organization
33	The solution must be able to allow users to access local websites, applications and SSH servers
34	The solution must identify corporate and BYOD devices
35	The solution must identify whether a third-party agent is enabled on the device

1.3.1.6. IoT Probe

The aim is to acquire a machine learning tool that allows the control of unmanaged devices through artificial intelligence algorithms that accurately identify and classify them.

Below are described the characteristics of the tool to be acquired, which must include all necessary licenses for the required functionalities.

REQ	Requirement
Architecture	
1	Number of 1Gbit/s RJ45 ports >= 4
2	eMMC hard drive >= 128GB
3	USB port >= 2
4	Dedicated "Out of Band" management port
5	RJ45 console port
6	The FW appliance must have an architecture with dedicated and independent hardware resources between management services and inspection services
7	It must be ensured that the FW appliance, when managed locally and when faced with an overload of traffic inspection services, does not in any way affect the performance of the management services and vice versa
Performance	
8	Appliance performance with firewall functionality with identification and control of applications (L7 inspection of all traffic) >= 4.4 Gbps
9	Appliance performance with IDS/IPS, Antivirus and Anti-Spyware, URL Filtering and Sandboxing functionalities >= 2.4 Gbps
10	Appliance performance with IPSec VPN functionality >= 3.0 Gbps
11	Number of new sessions per second >= 73 000
12	Maximum number of sessions >= 400 000
Device Security	
13	The platform must provide a security cloud service for devices.

14	The firewall must collect metadata of network traffic from devices, generate logs with this information and send them to a data repository. The IoT Service must be able to analyze this metadata using a patented engine based on artificial intelligence and machine learning algorithms to detect and identify devices on the network.
15	Device identification should not be based on fingerprinting, such as MAC address identification.
16	The identification engine must have 3 levels: identification of the device category (e.g., surveillance camera), identification of its profile (e.g., manufacturer, model and version) and identification of each instance of the device.
17	After identifying the devices, the solution must create a behaviour pattern for each one and automatically detect abnormal behaviours that may suggest that the device is compromised. For this type of event, alerts must be generated on the dashboard. It must be possible to receive these alerts via email and SMS.
18	When abnormal behaviour is observed, the solution must automatically suggest security policies to be applied on the firewall that will allow the device to function correctly, but block any abnormal connection.
19	The firewall must allow the creation of rules based on the types of devices that must be identified through brand, model and version, thus it is not necessary to create rules based on IPs or zones.
20	This service must observe more than 200 parameters in the network traffic metadata, including DHCP parameters (option 55), HTTP user agent IDs, protocols, protocol headers, etc.
21	The service must identify vulnerabilities present in the software, which runs on the respective devices and differentiate between vulnerable and potentially vulnerable devices. The service must identify software vulnerabilities as well as vulnerabilities associated with their incorrect use/configuration. Example: use of default credentials.
22	There must be the possibility of the Data Lake being used for another set of use cases through additional licensing, namely: NTA (Network Traffic Analysis), UEBA (User Authority Behaviour Analytics), shadow IT and integration with CASB (Cloud Access Security Broker).
23	The data repository must have a log storage capacity of 1 TB.

PART III
SERVICES

Article 24
Technical assistance and guarantees

The activities to be carried out within the scope of technical assistance and predicted guarantees that are in force for at least three years, without prejudice to what may be agreed in the awarded tender, due to the application of the award criteria, are as follows:

- Technical support directly from the manufacturer to IAVE, I.P., as contracting authority, without the need to use the manufacturer's partners;
- Direct access to the manufacturer's portal to open and monitor cases;
- Direct access to the manufacturer's portal to download software for the equipment under contract;
- Direct access to the manufacturer's portal to replace hardware in the event of malfunction;
- Replacement in case of malfunction on the following working day. (NBD);
- Technical support from the manufacturer by telephone during the minimum period of validity of the guarantees and of the technical assistance.
- Provision of support and technical assistance services;
- Repair of malfunctions;
- Disassembly/assembly of defective or discrepant parts, components or goods;
- Repair or replacement of defective or discrepant parts, components or goods;
- Supply, assembly or installation of repaired or replaced parts, components or goods;
- Transport of defective or discrepant equipment, parts or components to the location of their repair or replacement, return of those goods and delivery of missing, repaired or replaced parts or components;
- Transportation to the equipment installation site;
- Labour.

Article 25
Audit of solution implementation

The service provider must guarantee the performance of the contract through an audit at the end of its execution, with the aim of validating and approving the methodologies adopted.
The audit team must be made up of analysts/specialists with knowledge in WAN, LAN, and network security, and the team must comply with the duly certified requirements, or equivalent, namely:

- Must have certification from the manufacturer of the proposed solution;
- Must have the Lead Auditing 27001 Certification;
- Must have the Certified Information System Security Professional (CISSP) or Information Technology Infrastructure Library (ITIL) Certification or equivalent.

The audit team must have the following capabilities and knowledge of:

1. Experience in security audits and technical analysis.
2. Experience audits and penetration tests (e.g., Nessus, Acunetix, among others).
3. Proven experience in the following areas in network administration:
    a) WAN
    b) LAN Wired and Wireless
4. Proven experience in the following products in network security systems management;
    a) Firewalls
    b) VPN
    c) Other security systems such as:
    - Authentication server (TACACS, Radius and 802.1x);
    - Diagnostic tools (e.g., Wireshark);
    - Management, hardening and monitoring of network assets (SNMPV3, NTP, SSH, etc.)