Aprovo.

Luís Miguel Pereira dos Santos

Assinado de forma digital por Luís Miguel Pereira dos Santos
DN: c=PT, title=Presidente do Conselho Diretivo do IAVE, ou=Conselho Diretivo, o=Instituto de Avaliação Educativa IP, sn=Pereira dos Santos, givenName=Luís Miguel, cn=Luís Miguel Pereira dos Santos
Dados: 2023.06.29 15:56:54 +01'00'

INTERNATIONAL PUBLIC TENDER No. CPI/01/2023

TENDER SPECIFICATIONS No. 9/IAVE/2023

Acquisition of Endpoints, Displays and Security Software Package

CPV Classification: 30213300-6 - Portable Computers

30231310-3 - Flat panel displays

48730000-4 – Security software package

PART I - Legal Clauses

Article 1

Object

1. The object of these Tender Specifications is the acquisition, for the Instituto de Avaliação Educativa, I.P. (*Institute for Educational Assessment*), hereinafter IAVE, I.P., of:

Type	Description	Quantity
Endpoint Type 1	Basic Endpoint	200
Endpoint Type 2	Advanced Endpoint	150
Display	Monitor 23.8”	200
Device Security	Device Security	300

2. 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 Tender Specifications.

Article 2

Contract form and documents

1. The contract to be signed includes the following elements:

a) These Tender Specifications;

b) Correction of errors and omissions identified by the tenderers, provided that these errors and omissions have been expressly accepted by the competent body for the decision to contract;

c) Clarifications and rectifications to the Tender 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 number, the prevalence is determined in the order provided therein, without prejudice to the application of the principle of prevalence revised in Article 51 of the Public Procurement Code, henceforth only PPC.

3. In case of divergence between the documents referred to in number 2 and the clauses of the contract and its annexes, the former will prevail, except for the suggested adjustments, in accordance with the provisions of article 99 of the PPC and accepted by the successful tenderer, in the terms of the provisions of article 101 of the PPC.

4. In addition to the documents referred to in paragraph 2, the successful tenderer is also obliged to respect, when applicable, the European and Portuguese norms, specifications and approval by official bodies and manufacturers or entities holding patents.

Article 3

Good faith

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

Article 4

Place, manner and time for the execution 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 period of 60 (sixty) days after IAVE, I.P. receives and validates the conformity of the equipment, the execution being understood as the implementation of configuration and the installation of the security component in the various equipment, without prejudice to the provisions of article 45 of Law No. 98/97 of 26 August – Law of Organization and Process of the Court of Auditors, regarding the effects produced by contracts subjected the prior inspection by this Court.

2. The goods that are the object of the contract must be made available at the premises of Instituto de Avaliação Educativa, located at Travessa Terras de Sant'Ana, 15, 1250-269 Lisboa, within 120 days after the award of the contract.

Article 5

Base price

1.The base price, established in accordance with article 47 of the PPC, is €840,120.00 (eight hundred and forty thousand one hundred and twenty euros), value to which VAT is added at the legal rate in force. This base price is established in accordance with market prices practised in previous procedures referring to the equipment to be acquired, namely:

Equipment	Quantity	Unit Price	Total
Endpoint Type 1	200	1 950,00€	390 000,00€
Endpoint Type 2	150	2 150,00€	322 500,00€
Display	200	338,10€	67 620,00€
Device Security	300	200,00€	60 000,00€
Base Price			840 120,00€

Article 6

Payment conditions

1. The amounts owed by IAVE under the contract will be paid under the terms set out in the following numbers.

2. Payments will be made within a maximum period of 60 (sixty) days after acceptance of the goods, verification of their compliance by IAVE, I.P. and receipt of the respective invoices.

3. Under no circumstances will there be advance payment.

4. In case of disagreement on the part of IAVE, I.P. regarding the values indicated in the invoices, the successful tenderer must be notified of the reasons in writing, being obliged to provide the necessary clarifications, or issue a new corrected invoice.

5. The invoices must contain the commitment number generated by the contracting entity under the terms of the law, as well as a description of the goods.

6. Provided that they are regularly issued, and in compliance with the provisions of the preceding paragraphs, invoices are paid by bank transfer to the bank account number (IBAN) provided by the successful tenderer in the supplier form, without prejudice to what results from the submission of this contract to the approval by the Court of Auditors.

Article 7

Successful tenderer's obligations

1. In addition to other obligations derived from what is established in the parts of this procedure and in the applicable legislation, the obligations of the successful tenderer are the ones set out below, which must be object of specific clauses to be included in the contract to be signed:

a) Ensure the delivery of the goods and the execution of all contractual obligations, as defined in these tender specifications and respective annexes, as well as in the other contractual documents;

b) Communicate, in advance, to IAVE, I.P., any fact that makes it totally or partially impossible to deliver any of the goods object of this procedure, or that implies the non-compliance of any other obligations;

c) Change the underlying conditions for the provision of services agreed between the parties, through the signing of a written contract between them, only with prior written consent from the contracting entity;

d) Ensure all the human and material resources considered necessary and indispensable for the execution of the contract;

e) Ensure, in a correct and reliable manner, the information regarding the conditions under which the provision of goods will be performed, providing all clarifications that are justified and within the period indicated by IAVE, I.P.;

f) Communicate any fact that, occurring during the execution of the contract, proves to be relevant for the normal provision of the goods and for the contractual execution, namely, the change of the corporate name or of its legal representatives.

Article 8

Patents, licenses and trademarks

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

Article 9

Use of distinctive signs

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

Article 10

Secrecy

1. The successful tenderer will guarantee secrecy regarding any information related to the activity of IAVE, I.P. which the tenderer may become aware of due to the acquisition of the goods object of this contract.

2. Excluded from the duty of secrecy, referred to in the previous number, are information and documentation proven to be in the public domain on the date of the respective acquisition by the provider of goods, or that the latter is obliged to reveal by force of law in a judicial proceeding, or at the request of regulatory authorities or other competent administrative entities.

Article 11

Data Protection Regulation

1. The successful tenderer must comply with all applicable legal provisions regarding the processing of personal data, in the sense given 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 or for the purpose of providing the goods, namely, personal data of customers, employees, collaborators and suppliers of goods of IAVE, I.P.

2. The parties acknowledge and accept that, regarding all personal data to which the successful tenderer has access or transmitted by IAVE, I.P. for the purposes of providing the goods:

a) The IAVE, I.P. will act as data controller (as defined in the General Data Protection Regulation) and determine the purposes and terms of data processing by the successful tenderer;

b) The successful tenderer will act as a subcontracting entity (as defined in the General Data Protection Regulation), processing personal data in strict compliance with the instructions of the person responsible for processing such data;

c) For this purpose, the processing of personal data is understood to be the operations, with or without the use of automated means, carried out on the personal data of employees of IAVE, I.P., 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 to which it has access or is transmitted by the person responsible for the data processing under this contract, without having been expressly instructed, in writing, by that person 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 the applicable legislation regarding the processing of personal data and in particular to:

a) Treat them only in accordance with the instructions of IAVE, I.P., solely and exclusively for the purposes of this provision of goods, complying with the statutory obligations on data protection;

b) Provide all the collaboration required by IAVE, I.P. in order to clarify any issue related to the processing of personal data carried out under this contract and keep IAVE, I.P. informed regarding the processing of personal data;

c) Provide assistance to IAVE, I.P., taking into account the nature of the treatment and the information at its disposal, in order to ensure the obligations regarding the notification of violations of personal data, namely through communication, whenever possible, up to 72 hours after the knowledge (of the occurrence) of any violation of personal data that occurs, and also collaborating with IAVE, I.P. in the adoption of measures to respond to the occurrence, in its investigation and in the elaboration of the notifications that are necessary under the terms of the law;

d) Collaborate with IAVE, I.P. taking into account the nature of the treatment and, as far as possible, adopting 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 its obligation to respond to requests from data subjects, with the purpose of enabling them to exercise their rights under the terms of the law;

e) Not to communicate personal data to third parties and providers of goods not authorized or not indicated by IAVE, I.P.;

f) Depending on the choice of IAVE, I.P. or of the data subject, to delete or return the personal data at the time of the cessation of the contract, deleting and destroying any existing copies, except if the conservation or transmission of the data is required by law;

g) 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) Comply with all other legal provisions with regard to 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) Provide the data controller with all the information necessary to demonstrate compliance with the obligations provided for by law within its scope, as well as facilitate and contribute to audits, including inspections conducted by person responsible for processing the data or by another auditor mandated by this person;

k) Ensure that the personnel authorized to process personal data assume a commitment to confidentiality, and that they are aware of and undertake to fulfil all obligations set forth herein.

5. The successful tenderer undertakes to implement the necessary technical and organizational measures to protect the personal data processed on behalf of IAVE, I.P., against their accidental or unlawful destruction, accidental loss, alteration, dissemination, or unauthorized access, as well as against any other form of illicit processing of this personal data.

6. The measures referred to in the previous number must guarantee an adequate level of security in relation to the risks that the processing of data presents, the nature of the data to be protected and the risks, of various probability and severity, for the rights and freedoms of the natural persons.

7. The successful tenderer agrees that the access to personal data processed under this contract will be strictly limited to personnel who need to have access for the purposes of fulfilling the obligations assumed herein.

8. The successful tenderer undertakes to notify the data controller of any situation that may affect the processing of personal data or in any way will lead to non-compliance with the legal provisions on data protection and must also take all necessary measures in its power to stop it immediately.

9. The successful tenderer will be responsible for any damage caused to IAVE, I.P. as a result of the processing, by the tenderer or its staff, of personal data or of violation of applicable legal rules and of the provisions of this contract, when such violation is attributable to the successful tenderer and to their staff within the scope of the service provided.

10. Whenever IAVE, I.P. receives a request for access or rectification of personal data or an opposition to its processing by the data subjects, the successful tenderer must assist the person responsible for the personal data through appropriate technical and organizational measures, in order to allow IAVE, I.P. to fulfil its obligation to respond to requests from the data subjects and thus allowing them to exercise their legal rights.

Article 12

Changes to the contract

1. The contract may be amended, in accordance with articles 311 and 312, both of the PPC, namely, by:

a) Agreement of the parties, which cannot be less solemn than that of the contract;

b) Abnormal and unforeseeable change of the circumstances on which the parties have based their decision to contract, when the demands concerning the obligations undertaken seriously affect the principles of good faith and are not covered by the risks associated with the contract;

c) Reasons of public interest resulting from new needs or from a new consideration of the existing circumstances, without prejudice to the indemnities that may occur under the terms of the law.

Article 13

Assignment of the contractual position

2. The successful tenderer may not assign its contractual position without prior consent from IAVE, I.P.

3. The successful tenderer will be authorized to subcontract a third party to collaborate in the provision of the goods, provided that it ensures that this third party will comply with the provisions of the applicable legislation, such obligation being the object of a written contract that the tenderer signs with this third party, in which the latter is bound by the fulfilment of obligations arising from Regulation (EU) 2016/679 and other applicable legislation relating to Personal Data, linking its actions to the essence, nature and purposes of this contractual provision, in strict compliance with the duty of secrecy and confidentiality.

4. For the purposes of the consent provided for in the previous number, the assignee must present all the documentation required of the successful tenderer in this procedure, so that IAVE I. P. will verify that the assignee is not in any of the situations provided for in article 55 of the PPC, and that the assignment does not change the circumstances of compliance with contractual and legal obligations.

Article 14

Cessation of the contract

1. Failure by one of the parties to meet its contractual obligations gives the other party the right to cease the contract under the terms provided for in the applicable legal regime, without prejudice to the corresponding legal indemnities and other general grounds for legally ceasing the contract.

2. For the purposes of the provisions of the previous number, a definitive default exists when there is a delay in the provision for a period exceeding 10 working days.

3. The cessation occurs upon prior notice, by 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 number of this article.

4. The cessation of the contract does not affect the application of any pecuniary penalties, under the terms of the following article.

Article 15

Penalties

1. In the event of non-compliance with the contractual obligations, the contracting entity may apply the following pecuniary contractual penalties to the successful tenderer, depending on the seriousness or repetition of the infringement:

a) For non-compliance with obligations relating to the duty of secrecy, 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) Failure to comply with the duty to inform, up to €250.00 (two hundred and fifty euros), per infringement;

d) For non-compliance with the determination which is addressed to the successful tenderer under the terms of these Tender Specifications, which include the obligations provided for in Clause I, up to €250.00 (two hundred and fifty euros), per infraction;

e) The penalties may be applied for non-compliance with the obligations listed above, 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 PPC.

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 clause will be subject to a prior hearing, under the terms provided for in paragraph 2 of article 308 of the PPC.

4. The successful tenderer will be notified, in writing, so that within 10 (ten) working days it can give its opinion. If the successful tenderer does not respond within this period of time, the contracting entity applies the penalty in accordance with paragraph 2 of this article.

Article 16

Delay of the contracting entity

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 entity bear interest, at the legal rate, from the date on which they became due and until full payment, under the terms of article 326 of the PPC.

3. In case of disagreement on the amount due, the public contracting entity must make the payment on the amount about which there is agreement with the co-contracting party.

4. The amounts contested by the contracting entity, which may be 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 shall incur liability if it is prevented from fulfilling the obligations assumed in the contract due to acts of God or *force majeure*, being understood as such the circumstances that make it impossible to carry out the respective execution, beyond the will of the affected party, which it could not have known or foreseen on the date of the 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 number are verified, namely, earthquakes, floods, fires, epidemics, sabotage, strikes, international embargoes or blockades, acts of war or terrorism, riots and injunctive governmental or administrative determinations.

3. The following do not constitute *force majeure*, namely:

a) Strikes or labour disputes limited to the companies of the second party or to groups of companies in which it is a part, as well as to 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 the non-compliance by the second party with the duties or burdens that fall upon it;

d) Popular demonstrations resulting from the non-compliance, by the second party, with legal norms;

e) Fires or floods originating in the premises of the second party, whose cause, propagation or proportions are due to its fault or negligence or to non-compliance with safety standards;

f) Malfunctions in the computer or mechanical systems of the second party not due to sabotage;

g) Events that are or should be covered by insurance.

4. The party that invokes acts of God or *force majeure* must immediately communicate and justify such situations to the other party, by any written means, as well as inform the foreseeable period for re-establishing the situation.

5. *Force majeure* determines the extension of the deadlines for compliance with the contractual obligations which are affected by the period of time provably corresponding to the impediment resulting from *force majeure*.

Article 18

Counting deadlines in the execution phase of the contract

When calculating deadlines in the execution phase of the contract, the following rules apply:

a) The deadlines are continuous, not suspended on Saturdays, Sundays and holidays;

b) The deadline that falls on a Saturday, Sunday, holiday or on a day when the service, for which the act is carried out, is not open to the public, or does not operate during the normal period, is transferred to the first next business day.

Article 19

Signing of the written contract

In accordance with No. 1 of article 94 of the PPC, the contract will be in writing.

Article 20

Communications and Notifications

1. All notifications and communications between the contracting entity and the successful tenderer must be made in writing, by mail, email or fax, to the domicile or contractual headquarters of each one, identified in the contract with sufficient clarity, 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 international public tender procedure is adopted pursuant to the provisions of paragraph a) of article 20 and article 130 and following of the of the PPC and the decision to contract was taken by the President of the Board of Directors, Luís Pereira dos Santos.

Article 22

Competent court

1. Regarding everything that the present specifications do not refer to, the provisions of the PPC and other applicable legislation and regulations will be observed.

2. Any disputes arising from this procedure and the contract, namely regarding the respective interpretation, execution, non-compliance, invalidity, termination or reduction, must be addressed to the district court of Lisboa.

Part II

Technical specifications

Article 23

Equipment technical specifications

1. The technical characteristics of the equipment to which the present Tender Specifications apply are detailed according to the following specifications (The symbol ">=" means greater or equal, i.e., the quantities referred to are the minimum necessary, being possible to present higher quantities).

• **Basic Endpoint**

REQ	Requirement	Mandatory Requirement
Processor		
1	12th Generation Intel® Core™ i7-1255U Processor (E-cores up to 3.50 GHz P-cores up to 4.70 GHz) or equivalent	x
Operating System		
2	Windows 11 Pro 64 Portuguese/English	x
Screen		
3	Ability to support up to 4 displays (native display and 3 external displays via HDMI, USB-C and Thunderbolt)	x
4	HDMI support up to 3840x2160@60Hz	x
5	USB-C support up to 5120x3200@60Hz	x
6	Thunderbolt support up to 5120x3200@60Hz	x
7	14" FHD (1920x1080), IPS, Anti-Glare, Non-Touch, 100%sRGB, 400 nits, 60Hz, FHD IR/RGB Hybrid with Microphone, WWAN	x
Memory		
8	16GB (2x 8GB) DDR4-3200MHz SoDIMM	x
9	Support capacity up to 64GB DDR4-3200 + 2 DDR4 SO-DIMM slots, with dual-channel capability	x
Disk		
10	256 GB SSD M.2 2242 PCIe Gen4 TLC Opal (Included Encryption Capability)	x
11	Support capacity up to 1TB M.2 2242 SSD	x
Several		
13	NFC, Smart Card Reader, Fingerprint Reader, Wired Ethernet	x
14	3 Cell Li-Polymer 57Wh	x
15	Up to 10.3 hr with 999 performance score @200nits JEITA 2.0 Up to 14.9 hr @150nits Local video playback Up to 16.1 hr @150nits	x
16	65W USB-C AC Adapter	x
17	Intel® Wi-Fi 6 AX201 2x2 AX vPro® & Bluetooth® 5.1 or above	x

Certifications		
18	18 EPEAT Gold ENERGY STAR 8.0 ErP Lot 3 TCO Certified RoHS compliant MIL-STD-810H military test passed	x
Interfaces		
19	Doors: >= 1x USB 3.2 Gen 1 >= 1x USB 3.2 Gen 1 (Always On) >= 1x USB-C 3.2 Gen 1 (support data transfer, Power Delivery 3.0 and DisplayPort 1.4) >= 1x Thunderbolt 4 / USB4 40Gbps (support data transfer, Power Delivery 3.0 and DisplayPort 1.4) >= 1x HDMI, up to 4K/60Hz >= 1x microSD card reader >= 1x Ethernet (RJ-45) >= 1x Headphone / microphone combo jack (3.5mm) >= 1 x Smart card reader	x
20	Must include a docking station, which should be supported by the endpoints, with the following capabilities: Refresh rate - 2x 3840x2160 @60 Hz; 1x 3840x2160 @30Hz Power - 65 W with 90 W power adapter connected; 100 W with 135 W power adapter connected Compliance - FCC/ICES; EC; KCC; RCM; BSMI; VCCI; CB; cULus; EAC; TUV-Mark; Serbia Kvalitet; LoA; Israel SII; Ukraine DoC; NOM Interfaces: >= 1x Combo Audio Jack >= 3x USB3.1 >= 2x USB2.0 >= 1x USB-C >= 2x DisplayPort >= 1x HDMI Port >= 1x Gigabit Ethernet	x
21	Must include 5 years warranty	x

- **Advanced Endpoint**

REQ	Requirement	Mandatory Requirement
Processor		
1	12th Generation Intel® Core™ i7-1265U Processor (E-cores up to 3.60 GHz P-cores up to 4.80 GHz) or equivalent	x
Operating System		
2	Windows 11 Pro 64 Portuguese/English	x
Screen		
3	1080P FHD IR/RGB Hybrid with Microphone	x
4	Ability to support up to 4 displays (native display and 3 external displays via HDMI and Thunderbolt)	x

5	HDMI support up to 4K@60Hz	x
6	Thunderbolt support up to 5K@60Hz	x
7	13.3" WUXGA (1920 x 1200), IPS, Anti-Glare, Touch, 72%NTSC, 300 nits, LED Backlight, Low Cost Low Weight, FHD IR/RGB Hybrid with Microphone & Camera Cover of internal camera, Human Present Detection, 4G WWAN, PPS	x
Memory		
8	16GB LPDDR5-6400MHz (Soldered)	x
Disk		
9	512 GB SSD M.2 2280 PCIe TLC Opal (Encryption capability included)	x
10	Support capacity up to 2TB M.2 2280 SSD	x
Several		
12	Ethernet - USB-C to RJ45	x
13	NFC, Smart Card Reader	x
14	4 Cell Li-Polymer 54.7Wh Rapid Charge support (up to 80% charge in 1hr)	x
15	Up to 11.3 hr with 982 performance score @200nits Up to 9.7 hr with 791 performance score @250nits JEITA 2.0 Up to 19.5 hr @150nits Local video playback Up to 15.2 hr @150nits	x
16	65W USB-C AC Adapter	x
17	Intel® Wi-Fi 6E AX211 2x2 AX & Bluetooth® 5.2 or above with vPro®	x
Certifications		
18	EPEAT Gold EPEAT Gold ENERGY STAR 8.0 ErP Lot 3 TCO Certified 9.0 RoHS compliant MIL-STD-810H military test passed	x
19	Doors: >= 1x Smart card reader >= 2x Thunderbolt 4 / USB4 40Gbps (support data transfer, Power Delivery 3.0 and DisplayPort 2.0) >= 1x USB 3.2 Gen 1 >= 1x USB 3.2 Gen 1 (Always On) >= 1x HDMI, up to 4K/60Hz >= 1x Headphone / microphone combo jack (3.5mm)	x
20	Must include 5 years warranty	x

• **Display**

Below are described the characteristics of the displays to be acquired, and they must be 100% compatible with the endpoints.

REQ	Requirement	Mandatory Requirement
Characteristics		
1	WLED	x
2	Support Capability for Windows® 10, Windows 11	x
3	Diagonal Size – 23.8”	x
4	Interfaces – USB 3.2 Gen 1 / USB-C hub	x
5	Aspect Ratio – 16:9	x
6	Reproposed solution - 2560x1440 300 nits	x
7	Refresh Rate – 60Hz	x
8	Contrast Ratio – 1000:1	x
9	>= 1x HDMI® 2.0, >=1x DP 1.4, >=1x DP Out, >=1x USB-C® 3.2 Gen 1 (DP 1.4 Alt Mode)	x
10	>= 4x USB 3.2 Gen 1 (1x BC 1.2), 1x USB-C® 3.2 Gen 1	x
11	>= 1x RJ45, Ethernet (10M/100M/1000M)	x
12	Must include 5 years warranty	x

• **Device Security**

The intention is to acquire a tool for monitoring and detecting threats, vulnerabilities and malware to be used in our infrastructure for a total of 300 endpoints and/or servers.

Below are described the characteristics of the tool to be acquired, which must include all the necessary licenses for the intended functionalities, during the period equivalent to the warranty period of the equipment to be supplied.

REQ	**Requirement**
1	Prevention against exploits, including those that use Zero-Day type of vulnerabilities
2	Prevention against running malware, without requiring any prior knowledge
3	Ensuring a detailed forensic analysis of prevented attacks
4	Ability to restrict the execution of certain files
5	Protection against ransomware
6	Effective prevention of Exploits and Malware when there is no connectivity or management server updates and/or access to cloud resources
7	Control of USB devices
8	Disk Encryption
9	Host Firewall
10	Automatically isolation of machines infected with malware from the network
11	Endpoint Detection and Response module (EDR)
Management	
12	The proposed solution must be managed through a graphical web interface.
13	The proposed solution should be able to export your logs in syslog format to any log management proposed solution.

14	The proposed solution must have centralized cloud-based management.
15	The proposed solution must come from a base already configured with the manufacturer's best practices in order to simplify its deployment.
16	The proposed solution should allow the use of a logging service in the cloud to host both firewall and endpoint logs, so that it can then be integrated with several other manufacturers through a Framework and APIs.
17	The proposed solution must have a licensing model by endpoint and/or bandwidth and not by other parameters such as number of users, CPUs, etc.
18	The proposed solution must support the software update of endpoint agents directly from the cloud.
Exploits Prevention	
19	The proposed solution must support operating system processes and applications with the ability to add proprietary, third-party or custom applications to the list of protected applications.
20	The proposed solution must be able to provide real-time prevention against exploits of any application vulnerability (including zero-day or unknown types) by blocking exploit techniques such as “Software Logic Flaws”, “Memory Corruptions”, “DLL Hijacking”, “heap spray”, “JIT”, “ROP”, “SEH”, etc.
21	The proposed solution must be able to prevent exploits by blocking exploit techniques without requiring connectivity to the management server and/or cloud service and without using signatures.
22	As soon as the proposed solution prevents or blocks an exploit technique, it must immediately stop the related process, collect forensic information (process name, source file and path, date and time, memory dump, operating system version, identification of the user and identification and version of the vulnerable application, etc.) and just finish this process.
23	The proposed solution must use exploit techniques modules to prevent or block exploits. It should not base exploit prevention or blocking on file signatures, reputation and heuristics.
24	The proposed solution must not use endpoint resources intensively or use analysis techniques based on specific hardware, such as local sandbox based on software virtualization or containers. The proposed solution must have minimal impact on performance through the use of a lightweight and non-intrusive agent that can be completely invisible to the user.
25	The proposed solution must simultaneously protect all endpoint applications and processes against exploit techniques.
26	The proposed solution must allow the granular configuration of policies to prevent and block exploits by user, groups or machine (endpoint) and have pre-configured policies for the most common processes of the Microsoft Windows system.
27	The proposed solution must be able to protect the endpoint against “Kernel privilege escalation”.
28	The proposed solution must also be able to protect against exploits for MacOS and Linux, such as “local privilege escalation”.
Malware Prevention	
29	The proposed solution must support protection against the execution of malicious executables.
30	The proposed solution must guarantee the monitoring or learning functionality of the environment where it is installed (i.e., processes and applications installed and running on the endpoints). This should be used in the initial installation and configuration phase.

31	The proposed solution must have the ability to control what can be executed on the endpoint, from where it can be executed and with what parameters.
32	The proposed solution must prevent a process from launching any legitimate process that could be used for malicious purposes. This technique is often used in ransomware and other malware to bypass endpoint security.
33	The proposed solution must be able to block child processes initiated by a given process through whitelist (block all except those listed) and blacklist (block only those listed).
34	The proposed solution must be able to prevent the execution of malware through the analysis of behaviours triggered by the malware.
35	The proposed solution must guarantee the possibility of configuring global whitelists to allow the execution of certain executable files.
36	The proposed solution must be able to create rules to exclude protection capabilities for specific endpoints.
37	The proposed solution must detect and block malware through the use of machine learning and must not use local signatures regardless of the operating system.
38	The proposed solution must be able to analyze mach-o, ELF and APK files.
39	The proposed solution must have the option to integrate with Advanced Persistent Threat (APT) proposed solutions in the cloud, having the ability to provide effective prevention even when there is no connection to the cloud or to the centralized management service. The APT proposed solution in the cloud must be from the same manufacturer as the proposed solution, in order to ensure greater integration.
40	The proposed solution should be able to ask APT services in the cloud for hash values, in order to verify whether a given file is malicious or benign.
41	The proposed solution should use local machine learning techniques to detect unknown malware.
42	The proposed solution must monitor the different processes as well as their relationships and origins (parent processes) in order to be able to block processes with malicious behaviour.
Requirements	
43	The proposed solution must be able to submit potentially malicious files to APT cloud services.
44	The proposed solution must be able to view the malware analysis reports on the centralized management platform.
45	The proposed solution must not analyse files that have already been previously submitted to APT cloud services.
46	The proposed solution should be able to prevent unknown malware using APT sandbox technology in the cloud and provide a report with the verdict and analysis of the submitted file. The APT sandbox proposed solution in the cloud must be from the same manufacturer as the proposed solution to ensure greater integration.
47	The proposed solution must have the ability to manually modify the decision made by APT cloud services for a particular hash.
48	The proposed solution must have the ability to prevent the execution of a file in case its hash is unknown to APT cloud services.
49	The proposed solution must have the ability to prevent the execution of a file in case the endpoint cannot contact the APT services in the cloud and the hash value of the file is not known locally.

50	The proposed solution must guarantee the ability to perform static analysis (machine learning) in offline mode for Windows, Linux and macOS.
51	The proposed solution must prevent processes running on the endpoint from loading malicious DLLs. The solution must examine the DLLs and create a verdict on whether or not to upload a certain DLL.
52	The proposed solution must be able to analyse ransomware behaviour before its execution and must be able to stop encryption-based attacks through real-time analysis of encryption activities.
53	The proposed solution must be able to prevent attacks that take advantage of the kernel to upload and run malicious shell code.
54	The proposed solution must make the ransomware behaviour analysis module operate in notification or prevention mode.
55	The proposed solution must have a ransomware behaviour analysis module that supports the following file systems: NTFS, FAT, exFAT.
56	The proposed solution must be able to block any external USB device that connects to an endpoint monitored by the appliance. It should be possible to block a certain type of USB device, but only allow devices from a specific vendor or with a specific serial number. It must be possible to create only temporary policies.
57	The proposed solution must have the ability to automatically create an exclusion rule and an exclusion hash from the detected threats report, to ensure that a given process can be executed on a particular endpoint.
58	The solution must support the following operating systems:
59	Android 5, 6, 7, 8, 9 and 10
60	Debian 8 and 9
61	CentOS 6 and 7
62	Oracle 6 and 7
63	Red Hat 6 and 7
64	SUSE 12
65	Ubuntu 12, 14, 16 and 18
66	macOS 10.11, 10.12, 10.13, 10.14 and 10.15
67	Windows 7, 8, 10 and 11
68	Windows Server 2008R2, 2012, 2016 and 2019
69	The solution must also support the following virtual environments: Citrix XenApp, Citrix App layering, VMware AppVolumes, Vmware ThinApp
Endpoint Detection and Response	
70	Ability to monitor all endpoints, namely information relating to: processes, files, network traffic, registry and memory. Any activity related to these points must be saved for at least the last 30 days. It must be possible to extend this retention indefinitely.
71	Based on the information available for the last 30 days, the solution must be able to detect compromised machines, either based on the analysis of processes, files, registry, and network traffic on the machines, or based on the analysis of the behaviour of the user connected in the machine.
72	Allowing the analyst to define rules and search for patterns related to all the information that is retained for the endpoints. For example, it should be possible to search for endpoints where a particular registry key was modified, without having to use or learn a new query language.
73	When different alerts are related, the proposed solution must be able to automatically aggregate them into a single incident.
74	It must be possible to aggregate different incidents into a single one.

75	When a new incident is identified, the proposed solution must be able to automatically identify the root cause of the incident and show the entire sequence of events that caused the incident, as well as all the changes introduced by these events. For each event, it must be possible to view the associated process, the network traffic generated by that process, the files accessed, changed or created, any changes in the registry, as well as all modules/DLLs loaded by this process in memory.
76	For each incident, the proposed solution must indicate: all alerts associated with this incident, all artifacts relevant to the investigation, the machines and users involved. Each incident should have chat and notes functionality, so that analysts can collaborate with each other.
77	For each artifact there must be information on whether there are valid signatures for them, a verdict on the artifact from the manufacturer's own cloud, as well as from OpenSource tools (e.g., VirusTotal).
78	The proposed solution must map the different alerts to the Miter ATT&CK Framework.
79	Through additional licensing, the solution must be able to ingest data from the customer's network (on-prem and cloud) in order to have visibility of all network traffic and perform behavioural detection on the network, endpoint and cloud in a single proposed solution and graphical interface. In order to collect network traffic, the solution must be able to integrate with at least 4 firewall manufacturers.
80	Through additional licensing, it must be possible to ingest logs from identity providers, namely AzureAD, Okta and PingID, in order to detect anomalies in user authentication patterns.
81	There must be a “search&destroy” functionality that allows searching for any existing document on the machines and automatically deleting it.
82	The solution must learn the behaviour of each machine and create profiles, in order to be able to identify anomalous behaviour.
83	Based on behavioural learning for each machine and user, the solution should be able to generate alarms for these scenarios:
84	Rare SSH session
85	Use of unusual commands (arp -a, ipconfig, etc)
86	Rare processes communicating with machines outside the organization
87	Processes communicating with external machines that are not normally accessed by machines in the organization.
88	Scripts communicating with external hosts.
89	Domain user listing
90	Abnormal powershell command
91	High volume of connections between machines
92	Ability to automatically revert changes made to the machine by certain malware. The solution must list the changes made by any malicious processes and allow you to revert those changes.
Visibility over the machines	
93	The solution must include, through additional licensing, a visibility module with the following characteristics:
94	The ability to identify:
95	Users and groups configured on each machine
96	Services running on the machines
97	Drivers installed on machines

98	Processes, drivers, services that are automatically started whenever the user connects the machines.
99	Network Shares configured on machines.
100	Disks existing in the machines.
101	“Search&destroy” functionality that allows the search for any existing document on the machines and its automatic deletion.
102	Identifying vulnerabilities and their criticality for Windows and Linux environments.
103	Identifying the applications that run on each device
Incident Response	
104	The proposed solution must allow the initiation of malware scans on the infected machine
105	It must be possible to blacklist and whitelist hashes
106	It must be possible to quarantine certain processes
107	During the investigation of an incident, the proposed solution must allow the isolation of infected machines from the network
108	The solution must allow the automatic reversal of changes that have been made by a malicious process. Example: changing a registry key to the value before the machine was compromised.
109	There must be a Live Terminal functionality, where the analyst can remotely access the machines in order to: manage processes and files, run Python scripts, run Powershell commands and access the machine's command line.
110	It must be possible to run Python scripts on all the machines installed simultaneously. The solution must provide scripts for the most common use cases and allow the creation of new scripts.
111	Ability to create custom correlation rules that allow the detection of attacks retroactively.
112	The solution must include an advanced query language that supports wildcards, regular expressions, JSON, data aggregation, manipulation of fields and values, aggregation of data from different sources and data visualization.
113	The solution must include licensing for the intended functionalities for a period of 5 years.

1. Implementation services must be included in the provision of endpoint security software, software installation and configuration services on the equipment.

2. The tenderer must put together a technical team with the skills necessary for the proper performance of the implementation work, and in accordance with good practices in the area, i.e., with the skills necessary for the installation and configuration of the security component.

It should also be accompanied by a project manager with the following objectives:

• Monitoring and daily reporting to the IAVE team any deviations from the stipulated intervention plan and the reasons for this;

• Reporting to the IAVE team the detection of possible faults in the new equipment at the time of installation, for warranty purposes.

• Intervening whenever the field team has a doubt within the scope of the service provided.

• Daily management of acceptance reports, duly validated by the person in charge of the Location/Site.

The services to be developed cover the following activities:

• Preparation of plans for:

- Implementation/migration
- Tests and service reports
- Risks

• Project documentation

• Passing on the knowledge