REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.2865 prot

Datë 03.11.2025

URDHËR

Nr. 316, datë 03.11.2025

PËR

"MIRATIMIN E METODOLOGJISË TË PËRCAKTIMIT TË MASËS SË DËNIMIT ADMINISTRATIV GJOBË"

Në zbatim të nenit 45, të pikës 2, të ligjit nr. 25/2024, "Për sigurinë kibernetike", si dhe ligjit nr. 10 279, datë 20.5.2010 "Për kundërvajtjet administrative",

URDHËROJ:

1. Miratimin e metodologjisë për përcaktimin e masës së dënimit administrativ gjobë sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohet Autoriteti Kombëtar për Sigurinë Kibernetike.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM
Igli T

REPUBLIKA E SHQIPËRISË - AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE - KËSHILLI I MINISTRAVE

Adresa: Rruga "Papa Gjon Pali II" nr 3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax . 04 2221 039

REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.2865 prot Date 3.11.2025

ORDER

Nr._316, date 3.11.2025

ON

"THE APPROVAL OF THE METHODOLOGY FOR DETERMINING THE AMOUNT OF THE ADMINISTRATIVE FINE"

Pursuant to Article 45, point 2, of Law No. 25/2024, "On Cybersecurity", as well as Law No. 10 279, dated 20.5.2010, "On Administrative Offences",

ORDER:

1. The approval of the methodology for determining the amount of the administrative fine, according to the text attached to this order and forming an integral part thereof.
2. The National Cyber Security Authority is charged with the implementation of this order.
3. This order enters into force immediately.

GENERAL DIRECTOR
Igli TAFA

METHODOLOGY FOR DETERMINING THE AMOUNT OF THE ADMINISTRATIVE FINE

Table of Contents

I. GENERAL RULES

1. This methodology determines the basic general rules for determining the amount of the administrative fine, pursuant to Article 45, point 2, of Law No. 25/2024 "On Cybersecurity", Law No. 10279, dated 20.05.2010 "On Administrative Fines", Decision of the Council of Ministers No. 531, dated 25.09.2025 "On the content and method of documenting organisational, technical and operational cybersecurity measures and the categorisation of deadlines for corrective measures in critical and important information infrastructures", as well as the regulation "On the categorisation of cybersecurity incidents", approved by Order No. 299, dated 21.08.2024 of the General Director of the Authority.
2. The object of this methodology is to determine the rules and procedures for identifying, examining, and imposing administrative fines on operators of information infrastructures and employees of the Authority, in cases of violation of legal obligations provided for in Law No. 25/2024 "On Cybersecurity" and the by-laws issued for its implementation.
3. The purpose of this methodology is to ensure uniform, proportional, and fair application of administrative fines, to strengthen the enforcement of the cybersecurity legislation in force and prevent further violations.
4. This methodology is implemented by the National Cyber Security Authority in cases where, during the controlling process of information infrastructures, the controlling group identifies non-compliance with the legal requirements of the cybersecurity legislation in force that do not constitute criminal offences, as well as for violations identified for employees of the Authority who fail to comply with the obligations set out in the Law "On Cybersecurity" with regard to the preservation of confidentiality during the handling of a cybersecurity incident.
5. The terms used in this methodology have the same meaning as those defined in Law No. 25/2024 "On Cybersecurity", while the following terms have the meanings set out below:
   a) **"Administrative sanction"** means the fine and any other administrative measure or sanction provided for in the cybersecurity legislation in force or other by-laws.
   b) **"Fine"** means the principal administrative sanction of a monetary value, imposed for violations of legal requirements by operators of information infrastructures where the damage caused is significant and aimed at restoring the controlled activity to compliance with legal requirements.
   c) **"Controlling subject"** refers to operators of critical and important information infrastructures who are obliged to comply with the requirements set out in the cybersecurity legislation in force.
   ç) **"Principle of proportionality"** means the principle according to which controlling are carried out and administrative measures are taken in relation to the activity of the inspected subject, ensuring that the imposed administrative measure:
      - is necessary to achieve the legal objective of ensuring an adequate level of cybersecurity.
      - is appropriate and effective in preventing the recurrence of violations and encouraging compliance with legal requirements; and

- is proportionate to the nature, circumstances, consequences, and level of responsibility of the subject that committed the violation, avoiding excessive or unnecessary penalties.

6. In determining the amount of the sanction or administrative measure to be imposed, the controlling group, in accordance with the seriousness of the identified violations and their consequences, and respecting the principle of proportionality, imposes the sanction or measure that is necessary and appropriate to achieve the purpose of the sanction or measure and that least affects the rights or legitimate interests of the inspected subject.

II. ADMINISTRATIVE FINES

1. Types and Imposition of Administrative Fines

1.1 The violation of legal requirements by operators of information infrastructures, identified by the controlling group where it does not constitute a criminal offence, constitutes an administrative fine.

1.2 The identified violations of the legal requirements by the controlling subject are classified as administrative offences for which the following administrative sanctions are provided:

a) Administrative fine.
b) Request to the competent institution for suspension of service activity, in cases of repeated violations related to failure to implement security measures, where up to two (2) consecutive administrative measures have been imposed on the operator of critical information infrastructure.

1.3 Where necessary, the administrative sanction is accompanied by an order requiring the Controlling subject to correct the identified violations and eliminate their consequences, by setting a reasonable deadline for this purpose. In determining the deadline, the controlling group considers the risk level of the violation, its consequences, and the specific circumstances that determine the time required to perform the corrective actions, with maximum efforts on the part of the Controlling subject.

1.4 For each violation of legal requirements, a proportional administrative sanction shall be applied, which must be sufficient to ensure the rapid resolution of the violation, prevent its recurrence in the future, and address the lack of cooperation by the controlling subject.

III. CRITERIA FOR DETERMINING THE ADMINISTRATIVE FINE

1.Administrative Fine

1.1 The administrative fine, is the administrative fine imposed on operators of critical and important information infrastructures when they fail to comply with the legal requirements set out in Law No. 25/2024 “On Cybersecurity”, as well as the by-laws issued for its implementation.

1.2 The amount of the fine is expressed in ranges based on the points accumulated, the percentage (%) of implementation of cybersecurity measures, and the assessment of the risk level, as determined by this methodology.

1.3 The criteria for determining the amount of the fine are based on:

a) The percentage (%) of implementation of technical, organisational, and operational cybersecurity measures, as defined in Law No. 25/2024 "On Cybersecurity" and in Decision of the Council of Ministers No. 531, dated 25.09.2025 "On the content and method of documenting organisational, technical and operational cybersecurity measures and the categorisation of deadlines for corrective measures in critical and important information infrastructures".
b) The level of security risk in critical and important information infrastructures.
c) The category of cybersecurity incidents and their impact.

ç) Whether the responsible party has previously been administratively sanctioned.

2. Cases of Imposition of the Administrative Fine

2.1 The Authority, based on the provisions of this methodology, determines the amount of the fine within the minimum and maximum limits provided for in Law No. 25/2024 "On Cybersecurity".

2.2 Administrative fines are imposed on operators of critical information infrastructures and operators of important information infrastructures as follows:

a) Failure to report cybersecurity incidents occurring in infrastructures to the National CSIRT and the sectoral CSIRT, pursuant to letter "ë", point 3, Article 17, and point 3, Article 23 of Law No. 25/2024 "On Cybersecurity", constitutes an administrative offence and is sanctioned with a fine ranging from 1 000 000 ALL to 10 000 000 ALL;
b) Failure to accurately report information infrastructures during the identification process, pursuant to point 4, Article 12 of Law No. 25/2024 "On Cybersecurity" and the by-laws issued for its implementation, constitutes an administrative offence and is sanctioned with a fine ranging from 200,000 ALL to 400,000 ALL;
c) Failure to report the contact point or its updates to the Authority, pursuant to points 3 and 4, Article 18 of Law No. 25/2024 "On Cybersecurity", constitutes an administrative offence and is sanctioned with a fine ranging from 200,000 ALL to 400,000 ALL;

ç) Failure by operators to comply with the obligations set out in points 1, 3, 4, 5, 7, 8, and 9 of Article 31 of Law No. 25/2024 "On Cybersecurity" constitutes an administrative offence and is sanctioned with a fine ranging from 1 000 000 ALL to 10 000 000 ALL;

d) Failure by operators to comply with obligations related to the implementation of corrective measures, pursuant to points 1, 2, and 4 of Article 43 of Law No. 25/2024 "On Cybersecurity", constitutes an administrative fine and is sanctioned with a fine ranging from 400,000 ALL to 1 000 000 ALL;

dh) Failure by operators to comply with the obligations set out in points 5 and 6 of Article 23 of Law No. 25/2024 "On Cybersecurity" constitutes an administrative offence and is sanctioned with a fine ranging from 200,000 ALL to 400,000 ALL;

e) Failure by operators of critical and important information infrastructures of the public administration to comply with the obligations set out in points 1 and 2 of Article 32 of Law No. 25/2024 "On Cybersecurity" constitutes an administrative offence and is sanctioned with a fine ranging from 2,000,000 ALL to 5 000 000 ALL;

ë) Failure by Authority employees to comply with their obligations, pursuant to Article 27 of Law No. 25/2024 "On Cybersecurity", constitutes an administrative offence and is sanctioned with a fine ranging from 200,000 ALL to 400,000 ALL.

IV. METHODOLOGY FOR DETERMINING THE ADMINISTRATIVE FINE

1. Determination of administrative sanctions for failure to comply with the obligation to report cybersecurity incidents by operators of information infrastructures

1.1 Operators of critical and important information infrastructures are obliged to report all types of cybersecurity incidents to the National CSIRT and the sectoral CSIRT within 4 hours from the moment of identification of the cybersecurity incident. In the case of significant incidents, operators of critical information infrastructures and operators of important information infrastructures shall, within 72 hours from the moment of identification of the significant cybersecurity incident, update the information and conduct an initial assessment of the significant cybersecurity incident, including its severity and impact, as well as, where applicable, indicators of compromise.

1.2 Subjects who fail to report cybersecurity incidents in accordance with point 1.1 of Chapter IV of this methodology shall be sanctioned with a fine based on:

a) The category of the cybersecurity incident, as defined in the regulation "On the categorisation of cybersecurity incidents", approved by Order No. 299, dated 21.08.2024 of the General Director of the Authority.

b)The critical service or important service.

c) The assessment of the risk level.

ç) The established reporting time.

1.3 Failure to comply with the obligation to report cybersecurity incidents by operators of information infrastructures shall be sanctioned with a fine in the amounts set out in the table below:

Classification of cybersecurity incidents according to impact	**Reporting time**	**Fine for operators of critical infrastructures**	**Fine for operators of important infrastructures**
Cybersecurity incidents with **high** impact	Within 4 hours from identification	8 000 000 ALL	5 000 000 ALL
Cybersecurity incidents with **medium** impact	Within 4 hours from identification	5 000 000 ALL	3 000 000 ALL
Cybersecurity incidents with **low** impact	Within 4 hours from identification	2 000 000 ALL	1 000 000 ALL

Table nr.1

Note: The categories of cybersecurity incidents are defined in Article 6 of the regulation* ***"On the categorisation of cybersecurity incidents",*** *approved by Order No. 299, dated 21.08.2024 of the General Director of the Authority.*

1.4 In cases of repeated legal violations, regardless of the impact level of the cybersecurity incident, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

2. Determination of administrative sanctions in cases of failure to submit the final incident report to the National CSIRT, as well as failure to submit the progress report in the case of an ongoing cybersecurity incident

2.1 Pursuant to Article 23, points 5 and 6 of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures are obliged, within one (1) month after notification of the incident, to submit a final report to the National CSIRT, which contains:

a) a detailed description of the incident, including its severity and impact;
b) the type of threat or the main cause that may have caused the incident;
c) the measures implemented and the ongoing measures to mitigate the consequences;
ç) where applicable, the cross-border impact of the incident.

2.2 In cases of an ongoing cybersecurity incident, the operator of the information infrastructure affected by the incident, in addition to the obligation to submit the final report, is also obliged to submit a progress report to the National CSIRT during the occurrence of the cybersecurity incident.

2.3 Pursuant to Article 44, letter "e", of Law No. 25/2024 "On Cybersecurity", failure to submit the final report and/or the progress report constitutes an administrative offence and is sanctioned with a fine as follows:

Classification of cybersecurity incidents according to impact	**Fine for failure to submit the final report / progress report for incidents occurring in operators of critical infrastructures.**	**Fine for failure to submit the final report / progress report for incidents occurring in operators of important infrastructures**
Cybersecurity incidents with **high** impact	350 000 ALL	300 000 ALL
Cybersecurity incidents with **medium** impact	300 000 ALL	250 000 ALL
Cybersecurity incidents with **low** impact	250 000 ALL	200 000 ALL

Table nr.2

2.4 In cases of repeated legal violations, regardless of the impact level of the cybersecurity incident, the maximum fine in the amount of 400 000 ALL shall be applied, as defined in Article 45, point 1, letter "b" of Law No. 25/2024 "On Cybersecurity".

3. Determination of administrative sanctions for failure to report the contact point to the Authority or to update it.

3.1 Pursuant to letter "f" of Article 16 and Article 18 of Law No. 25/2024 "On Cybersecurity", the sectoral CSIRT designates the contact point and reports the data to the National CSIRT. Operators of critical and important information infrastructures designate contact points and report the data to the National CSIRT and the sectoral CSIRT. Any change to the contact point data must be communicated to the National CSIRT and the sectoral CSIRT within seven (7) calendar days.

3.2 Failure to report the contact point or to update it constitutes an administrative offence and is sanctioned with a fine as follows:

a) failure to report the contact point or its updates by operators of critical information infrastructures (CII) is sanctioned with a fine in the amount of 300 000 ALL;
b) failure to report the contact point or its updates by operators of important information infrastructures (III) is sanctioned with a fine in the amount of 200 000 ALL.

3.3 In cases of repeated legal violations, the maximum fine in the amount of 400 000 ALL shall be applied, as defined in Article 45, point 1, letter "b" of Law No. 25/2024 "On Cybersecurity".

4. Determination of administrative sanctions for failure to implement corrective measures

4.1 Pursuant to Article 43, point 1, of Law No. 25/2024 "On Cybersecurity", when the Authority identifies deficiencies in the implementation of security measures, it determines a reasonable deadline within which operators of critical and important information infrastructures must implement the relevant corrective measures. The determination of this reasonable deadline is made in accordance with the provisions of Decision of the Council of Ministers No. 531, dated 25.09.2025 "On the content and method of documenting organisational, technical and operational cybersecurity measures and the categorisation of deadlines for corrective measures in critical and important information infrastructures".

4.2 Pursuant to Article 44, letter "dh", of Law No. 25/2024 "On Cybersecurity", failure by operators of information infrastructures to implement corrective measures shall be sanctioned with a fine in accordance with this methodology.

4.3 For the purposes of assessing the level of non-implementation of cybersecurity measures defined in Decision of the Council of Ministers No. 531, dated 25.09.2025 "On the content and method of documenting organisational, technical and operational cybersecurity measures and the categorisation of deadlines for corrective measures in critical and important information infrastructures", as well as determining the respective administrative sanction (fine), this methodology defines the rules, criteria, and method for assessing the non-implementation of cybersecurity measures based on the specific weight of each security measure according to Annex I of this methodology, as well as the percentage of implementation of each applied measure.

4.4 For each category of organisational, technical, and operational measures, the following table is presented:

ORGANISATIONAL, TECHNICAL AND OPERATIONAL MEASURES	**Weight per measure (Annex No. 1)**	**Percentage of implementation of the measure (determined by the Controlling Group 0–100%)**

MS – 1	-	-
MS – 2	-	-
:	-	-
:	-	-
MS – (N)	-	-

Table nr. 3

4.5 Within this structure:

- **Measure**: identifies the designation of the cybersecurity measure.

- **Weight points** are determined for each security measure on the Decision of the Council of Ministers No. 531, dated 25.09.2025 "On the content and method of documenting organisational, technical and operational cybersecurity measures and the categorisation of deadlines for corrective measures in critical and important information infrastructures", by the Controlling group, based on their categorisation and importance according to Annex No. 1 of this methodology;
- **Percentage of implementation of the measure** is assessed during the Controlling process by the Controlling Team for each measure. All partially implemented or non-implemented cybersecurity measures are subject to assessment according to the formula set out in point 4.7 of Chapter IV of this methodology.

4.7 The formula for calculating the total percentage of non-implementation of cybersecurity measures is as follows:

Percentage not implemented = sum [weight per measure (not implemented, partially implemented) × (100% − percentage of implementation of the measure)] / total weight of applicable measures

The levels for assessing the non-implementation of security measures and the corresponding fines are set out in the table below:

Level	**Total percentage of non-implementation (%)**	**Fine (ALL)**
Level 0	0% – 10%	0
Level 1	11% – 20%	400 000
Level 2	21% – 30%	500 000
Level 3	31% – 45%	600 000
Level 4	46% – 60%	700 000
Level 5	61% – 75%	800 000
Level 6	76% – 90%	900 000
Level 7	91% – 100%	1 000 000

Table nr. 4

4.8 In cases of repeated violations identified by the National Cyber Security Authority, where during the Controlling process it is established that the subject has implemented corrective measures at a higher level than in the first instance, the administrative fine shall be imposed

according to the corresponding level of non-implementation percentage as per Table No. 4 of this methodology.

4.9 In cases where the level of implementation of corrective measures is the same as in the first instance, i.e. no progress has been recorded, the maximum administrative fine in the amount of 1 000 000 ALL shall be applied, in accordance with Article 45, point 1, letter "c" of Law No. 25/2024 "On Cybersecurity".

4.10 Where the Authority identifies repeated violations related to the implementation of cybersecurity measures defined in Law No. 25/2024 "On Cybersecurity" by an operator of critical information infrastructure, for which up to two (2) consecutive administrative measures have been imposed, it shall apply other coercive measures in accordance with Article 46 of Law No. 25/2024 "On Cybersecurity".

5. Determination of the administrative sanction for failure by operators of information infrastructures to report any new infrastructure administered by them that interacts with critical or important information infrastructures

5.1 Pursuant to Article 31, point 2, of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures are obliged to continuously report to the Authority any new infrastructure administered by them that interacts with infrastructures categorised as critical or important.

5.2 Pursuant to Article 43, point 2, of Law No. 25/2024 "On Cybersecurity", where the Authority determines that operators of information infrastructures have failed to comply with the obligation set out in Article 31, point 2, of Law No. 25/2024 "On Cybersecurity", it determines a deadline of ten (10) calendar days within which operators of critical and important information infrastructures shall take measures to fulfil the obligation.

5.3 Pursuant to Article 44, letter "dh", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows::

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 600 000 ALL;

b) operators of important information infrastructures are sanctioned with a fine in the amount of 400 000 ALL.

5.4 In cases of repeated legal violations, the maximum fine in the amount of 1 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "c" of Law No. 25/2024 "On Cybersecurity".

6. Determination of the administrative sanction for failure to comply with the obligations set out in points 1, 3, 4, 5, 7, 8 and 9 of Article 31 of Law No. 25/2024 "On Cybersecurity"

6.1 Pursuant to Article 31, point 1, of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures are obliged to report all their critical and important infrastructures, as well as all other infrastructures that interact with them, to the Authority.

6.1.1 Pursuant to Article 44, letter "d", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows:

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 5 000 000 ALL;
b) operators of important information infrastructures are sanctioned with a fine in the amount of 1 000 000 ALL.

6.1.2 In cases of repeated legal violations, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

6.2 Pursuant to Article 31, point 3, of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures are obliged to document any change and development carried out in their critical and important infrastructures.

6.2.1 Pursuant to Article 44, letter "d", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows:

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 5 000 000 ALL.
b) operators of important information infrastructures are sanctioned with a fine in the amount of 1 000 000 ALL.

6.2.2 In cases of repeated legal violations, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

6.3 Pursuant to Article 31, point 4, of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures are obliged to make available to the Authority any documentation and evidence required by the Authority within the framework of the Controlling process.

6.3.1 Pursuant to Article 44, letter "d", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows:

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 5 000 000 ALL.
b) operators of important information infrastructures are sanctioned with a fine in the amount of 1 000 000 ALL.

6.3.2 In cases of repeated legal violations, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

6.4 Pursuant to Article 31, point 5, of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures, within the framework of supervisory activity, shall provide the National CSIRT with direct access to their premises and information systems, in accordance with the security procedures of each operator, which are related to the services provided by them.

6.4.1 Pursuant to Article 44, letter "d", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows:

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 5 000 000 ALL.
b) operators of important information infrastructures are sanctioned with a fine in the amount of 1 000 000 ALL.

6.4.2 In cases of repeated legal violations, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

6.5 Pursuant to Article 31, point 7, of Law No. 25/2024 "On Cybersecurity", for the effective implementation of cybersecurity measures, operators shall submit to the Authority a conformity assessment report issued by a Conformity Assessment Body, at least once every two (2) years.

6.5.1 Pursuant to Article 44, letter "d", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows:

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 5 000 000 ALL.
b) operators of important information infrastructures are sanctioned with a fine in the amount of 1 000 000 ALL.

6.5.2 In cases of repeated legal violations, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

6.6 Pursuant to Article 31, point 9, of Law No. 25/2024 "On Cybersecurity", operators of critical and important information infrastructures are obliged to cooperate with the Authority in the performance of the supervisory functions provided for by law.

6.6.1 Pursuant to Article 44, letter "d", of Law No. 25/2024 "On Cybersecurity", failure to comply with this obligation constitutes an administrative offence and is sanctioned with a fine as follows:

a) operators of critical information infrastructures are sanctioned with a fine in the amount of 5 000 000 ALL;
b) operators of important information infrastructures are sanctioned with a fine in the amount of 1 000 000 ALL.

6.6.2 In cases of repeated legal violations, the maximum fine in the amount of 10 000 000 ALL shall be applied, as defined in Article 45, point 1, letter "a" of Law No. 25/2024 "On Cybersecurity".

7. Determination of administrative sanctions for failure to comply with the obligations of operators of critical and important information infrastructures of the public administration

7.1 Pursuant to Article 32, points 1 and 2, of Law No. 25/2024 "On Cybersecurity", failure to obtain prior confirmation for operators of critical and important information infrastructures of the public administration from the institution responsible for electronic governance regarding technical specifications prior to initiating the implementation of a system, as well as failure by operators of critical and important information infrastructures of the public administration to comply with the obligation to host the primary node at the Government Data

Center and the secondary node at the Business Continuity Center, constitutes an administrative offence and is sanctioned with a fine as follows:

a) 3 000 000 ALL for operators of critical information infrastructures of the public administration.

b) 2 000 000 ALL for operators of important information infrastructures of the public administration.

7.2 In cases of repeated legal violations, the maximum fine in the amount of 5 000 000 ALL shall be applied, as provided for in Article 45, point 1, letter "ç", of Law No. 25/2024 "On Cybersecurity".

8. Determination of administrative sanctions for failure to comply with confidentiality obligations by Authority employees

8.1 Pursuant to Article 27, point 1, of Law No. 25/2024 "On Cybersecurity", employees of the Authority who participate in the resolution of a cybersecurity incident are obliged to maintain full confidentiality of all data processed during the incident resolution procedure. Confidentiality shall also be maintained after the termination of the employment relationship with the Authority, in accordance with the provisions of the applicable legislation in force.

8.2 Employees of the Authority who fail to comply with the obligation set out in point 8.1 of this methodology shall be sanctioned with a fine in the amount of **200,000 ALL**.

8.3 In cases of repeated legal violations, the maximum fine in the amount of **400,000 ALL** shall be applied, as provided for in **Article 45, point 1, letter "b"**, of **Law No. 25/2024 "On Cybersecurity"**.

ANNEX 1: Weighting for each measure of Council of Ministers Decision No. 531, dated 25.09.2025, "On the content and the manner of documenting organizational, technical, and operational cybersecurity measures, and the categorization of deadlines for corrective measures in critical and important information infrastructures."

Level	Measure	Documentation	Categorization	Weight
1	Establishment of a high-level security policy, approved by the senior management of the infrastructure, addressing the security of communication networks and critical and important information systems, and its periodic review. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).).	Information Security Policy Periodic Review Reports	Organizational	**3**
1	Development of a cybersecurity risk management methodology. (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Cybersecurity Risk Management Methodology document, including versioning, dates, and approval by senior management. Periodic Review Reports	Organizational	**2**

1	Preparation of a list of risks related to the security of communication networks and information systems, taking into account the main threats to critical assets. (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Risk assessment list compiled from various sources, including risks arising from third parties. Notification of senior management regarding the risk list, along with the decisions taken on their treatment. Review of the risk list.	Organizational	**4**
1	Development of a risk treatment plan for the identified risks.	Risk treatment plan document. Reflection of changes in risk levels following the implementation of the risk treatment plan.	Organizational	**2**

1	Assignment of roles and responsibilities for information security management.	List of security roles and a detailed description of responsibilities and duties for each role, e.g. (CISO, ISO, DPO, DBA, SYSADM, NETADM, etc.). Organizational chart showing the hierarchy and relationships among security roles. Contact list for persons responsible for information security (name, position, contact details).	Organizational	**2**
1	Establishment of a security policy for suppliers / third-party contracts and its periodic review. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Security policy for suppliers / third-party contracts (version, publication date, approval). Periodic review reports of the security policy and implemented changes.	Organizational	**2**
1	Incorporation of security requirements into third-party contracts, including confidentiality and secure information transfer.	Clear security requirements included in contracts with third parties. Confidentiality agreements for information protection with third parties.	Organizational	**2**

2	Maintenance of logs/records of cybersecurity incidents related to or caused by third parties.	Register of cybersecurity incidents related to third parties (date, cause, impact, actions taken).	Organizational	**1**
1	Establishment of a Human Resources security policy.	Human Resources security policy (covering all phases: pre-employment, during employment, disciplinary processes, and termination of employment).	Organizational	**1**
		Integrity verification document for key personnel, including criminal record clearance (certificate of no criminal record), references from previous employment, certifications, CVs, etc		
		Personal data protection procedure.		
1	Implementation of a cybersecurity training program. (Reviewed at least once (1) per year).	Detailed training program, tailored to employees' roles and responsibilities.	Organizational	**2**
		List of participants and training dates.		

		Documentation of awareness campaigns and employee trainings related to cybersecurity and the most common cybersecurity attacks, such as “Phishing,” “Malware,” etc.		
1	Information and training of new employees on the applicable cybersecurity policies and procedures.	Records of training provided to new employees. Forms signed by employees acknowledging awareness of applicable policies and procedures. Forms signed by employees for the Confidentiality Agreement (“NDA” – Non-Disclosure Agreement).	Organizational	**2**
2	Testing of employees’ cybersecurity knowledge. (At least once (1) per year for employees who use critical information systems within the infrastructure and/or more frequently depending on cybersecurity incidents.)	Questionnaires and test results assessing employee awareness of cybersecurity.	Organizational	**1**

1	Implementation of measures for the identification and effective management of assets. (At least once (1) per year and/or after any major change in the infrastructure of CII/III).	Comprehensive inventory of Information Technology (IT) / Operational Technology (OT) assets, including, for example, model, asset category, serial number, Internet Protocol (IP) address, location, age, status, etc..	Organizational	**5**
		Inclusion in the asset inventory of impact classification based on Confidentiality, Integrity, and Availability ("C/I/A" – Confidentiality / Integrity / Availability) of each asset.		
1	Establishment and implementation of asset management policies/procedures.	Detailed asset management policies/procedures, including roles and responsibilities, assets covered by the policy/procedure, asset management objectives, and asset disposal. (Reviewed at least once (1) per year and/or after any major change in the infrastructure of CII/III).	Organizational	**2**

		Detailed network and information systems topology.		
1	Implementation of measures for the replacement or isolation of systems that have reached the end of their lifecycle ("EOL" – End of Life).	Document or evidence identifying systems that have reached the end of their lifecycle (EOL) and planning for their replacement or isolation	Technical and Operational	**5**
		Records of replacement/isolation of assets that have reached the end of their lifecycle (EOL).		
		System verification and supporting evidence.		
1	Performance of automatic/manual updates ("patching") on endpoint systems and across the entire Information Technology (IT) and Operational Technology (OT) infrastructure.	Procedure for managing the implementation of updates (patches) for Information Technology (IT) and Operational Technology (OT) equipment and systems, including frequency, responsible roles, and records.	Technical and Operational	**4**
		Verification of systems/tools and supporting evidence.		

1	Definition and implementation of security policies and controls for personal devices used to access the infrastructure's systems and data ("BYOD" – Bring Your Own Device), ensuring information protection and compliance with security standards.	Policy/procedure for the use of personal devices (phones, laptops, tablets, etc.), as well as an inventory of personal devices authorized for use on the infrastructure's internal networks and systems. Evidence of minimum security configurations for personal devices in accordance with the policy.	Organizational	**1**
1	Development of detailed plans and procedures for cybersecurity incident management. (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Cybersecurity incident management plan document (version, date, approval). Procedures for incident identification, classification, and handling (Action manuals – "Playbooks"), including the list of members of the cybersecurity incident response team.	Organizational	**4**

1	Maintenance of records for all cybersecurity incidents.	Incident register including date, cause, impact, and corrective actions. Individual incident handling reports and lessons learned analyses.	Organizational	**3**
1	Ensuring that any change to Information Technology (IT) systems and processes within Critical / Important Infrastructure is managed in a controlled and documented manner.	Change management policy (including description, date, responsibilities, expected impact, implementation plan, etc.). (Reviewed at least once (1) per year). Change management procedure (steps from proposal through approval and implementation). Change Request Form ("RFC" – Request for Change).	Organizational	**3**
1	Development and implementation of a Business Continuity Plan (BCP) to ensure the continuous operation of the infrastructure's critical processes in the event of cybersecurity incidents, natural disasters, or operational disruptions. (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Service continuity strategy policy, including conditions for plan activation, recovery timeframes, crisis communication, incident scenarios, action plan, testing rules, etc.	Organizational	**4**

		Business Impact Analysis (BIA), identification of critical processes, and definition of the Recovery Time Objective / Recovery Point Objective ("RTO" / "RPO").		
		Emergency contact list – information on points of contact in the event of a crisis.		
1	Utilization of data mirroring techniques through redundant configuration of independent disks ("RAID" – Redundant Array of Independent Disks)	Technical verification of redundant configuration of independent disks ("RAID") (1/5/6/10) and the relevant evidence.	Technical and Operational	**3**
1	Establishment of a backup policy/procedure. (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Backup policy/procedure document, including frequencies, types, data, and services.	Organizational	**2**
		List of performed backups and reports of recovery and data integrity testing.		
2	Performance of backups using techniques such as "Backup Lock Retention" or "Tape WORM".	Evidence of the use of "Backup Lock Retention" or "Tape WORM" techniques.	Technical and Operational	**5**
2	Avoidance of single points of failure in the infrastructure's critical and important services	Technical verification of single points of failure.	Technical and Operational	**4**

		Evidence of service redundancy.		
2	Implementation of infrastructure based on high-availability service architectures ("HA" – High Availability).	Documentation of infrastructure architectures based on high-availability (HA) services, covering technical support levels L1, L2, L3, and the perimeter protected by a digital firewall. Verification and supporting evidence.	Technical and Operational	**4**
2	Implementation of a secondary environment for recovery and continuity of Information Technology (IT) systems following a cybersecurity incident ("DRS" – Disaster Recovery Site).	Disaster Recovery Site (DRS) strategy and detailed configurations. (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Technical and Operational	**5**

		Disaster Recovery Plan (DRP/DRS) and procedures for the recovery of Information Technology (IT) systems and infrastructure (tasks and responsibilities, list of key systems and assets). (Reviewed at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).		
		Reports of testing of the secondary environment for recovery and continuity of Information Technology systems for post-incident/disaster recovery (DRS). (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).		

		Verification and supporting evidence.		
2	Implementation of Software Defined Networking (SDN) technology to enable critical services and applications to achieve the fastest possible recovery with minimal (or no) service interruption in the event of disasters or incidents.	Strategy to ensure that critical services and applications (including those relying on Software Defined Networking (SDN) and "Blockchain" technologies) can be recovered as quickly as possible with minimal disruption in the event of disasters or incidents.	Technical and Operational	**No weight (optional measure)**
		Periodic testing of Software Defined Networking (SDN) configurations.		
		Verification of the implementation of "Hashing" techniques.		
2	Implementation of "Blockchain" technology for the decentralization of data management, ensuring data protection and integrity during recovery.	Backup policy for "Blockchain" technology.	Technical and Operational	**No weight (optional measure)**
		Monitoring of "Blockchain" activity.		
1	Policy/procedure for internal control and internal auditing of information security and its periodic review. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Policy/procedure document for controls and audits (version, date, and approval of the policy/procedure by senior management).	Organizational	**1**

1	Monitoring of compliance of standards with legal requirements.	Policy/Procedure for monitoring compliance with applicable standards and legal requirements. List of applicable standards and legal requirements for the infrastructure. Review of policies and procedures for the Information Security Management System (ISMS), at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III.	Organizational	**1**
1	Policy/procedure for internal control and internal auditing of information security and its periodic review. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Policy/Procedure document for controls and audits (version, date, and approval of the policy/procedure by senior management).	Organizational	**1**

1	Performance of internal or third-party controls/audits for information security and the infrastructure's critical systems. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Internal audit reports and remediation plans (date, methodology, findings/results).	Organizational	**2**
		Reports of information security audits conducted by third parties.		
		List of corrective actions undertaken following audits and evidence of their implementation.		
1	Implementation of physical security measures and environmental controls.	Evidence of implementation of physical security measures (locks, cabinets, electronic access control).	Technical and Operational	**4**
		Audit logs of access activities to authorized areas and alerts for unauthorized access.		
		Reports on the operation and maintenance of alarm systems and fire suppression systems.		

		Ensuring the segregation of physical spaces into segmented zones based on authorization levels, including the development of a detailed topology and a clear evacuation plan to guarantee physical security and access management.		
1	Implementation of a policy for physical security measures and environmental controls.	Physical security and environmental controls policy document (version, date, approval, review).	Organizational	**1**
1	Implementation of policies for controlling and protecting access to information networks and systems. (Reviewed at least once (1) per year and/or after any major change in the infrastructure of CII/III).	Access control policy document (roles, groups, rights, procedures for granting and revoking access).	Organizational	**4**
		Access rights granting form.		
		Access rights revocation and asset handover form.		
		Evidence of deletion of generic accounts and reports of periodic access control reviews.		

1	Application of traffic filtering for remote access to systems, as well as encryption of traffic using secure protocols.	Technical verification and supporting evidence for the implementation of traffic filtering and traffic encryption.	Technical and Operational	**5**
1	Verification that the digital firewall is configured with authorized/blocked lists (“Whitelist/Blacklist”) of allowed or blocked Internet Protocol (IP) addresses.	Verification and supporting evidence for configurations on the digital firewall.	Technical and Operational	**5**
1	Use of policies for managing strong/random passwords for users and local administrators.	Password management policy document and verification of the implementation of solutions for managing random passwords for users and local administrators (“LAPS” – Local Administrator Password Solution) or similar technologies.	Technical and Operational	**3**
2	Creation and implementation of a technological solution for Identity and Access Management (IAM) to ensure security, authorization, and auditing of user activities on critical systems.	Technical verification and supporting evidence..	Technical and Operational	**5**
2	Implementation of a technological solution for Privileged Access Management (PAM).	Technical verification and supporting evidence..	Technical and Operational	**4**

2	Implementation of a security service providing network access based on the Zero Trust principle ("ZTNA" – Zero Trust Network Access).	Technical verification and supporting evidence..	Technical and Operational	**5**
1	Implementation of encryption policies, including details on cryptographic algorithms and keys.	Encryption policy document, including, for example, algorithms such as "AES", "RSA", "ECC", "TLS", "IPSec", "SSH", etc. List of cryptographic keys (e.g., type, validity period, generation and storage methods).	Technical and Operational	**2**
2	Encryption of data (in transit and at rest).	List of encryption configurations for data and applications ("on-premises", "hybrid", "cloud"). Technical verification and supporting evidence.	Technical and Operational	**4**
1	Implementation of an automated system for the detection and management of security information and incidents/events ("SIEM" – Security Information and Event Management).	Technical verification and evidence of configuration of the automated system for security information and event management (SIEM), including alerting rules and filtering of logs and activities for incident detection.	Technical and Operational	**5**
1	Continuous monitoring of external cybersecurity threat intelligence sources ("threat intelligence").	Periodic reports from cybersecurity threat intelligence monitoring tools.	Technical and Operational	**3**

		List of sources used for collecting threat information.		
2	Implementation of a cyber threat intelligence program, including defined roles, responsibilities, and procedures.	Cyber threat intelligence program document, including the structure of roles and responsibilities.	Organizational	**1**
1	Implementation of policies for monitoring and logging cybersecurity security events.	Policy document for monitoring and logging of traces and activities (logs), including minimum requirements, retention periods, objectives, approval, and updates.	Organizational	**2**
1	Deployment of tools for collecting logs and activity traces from critical systems.	List of implemented tools for collecting traces and activities/logs (e.g., log servers, etc.). Technical verification and supporting evidence.	Technical and Operational	**3**
1	Installation of devices to monitor, control, and restrict inbound and outbound network traffic using a Next-Generation Firewall (NGFW).	Technical verification of the configuration of the next-generation digital firewall. Technical verification and supporting evidence.	Technical and Operational	**5**
1	Monitoring, detection, and analysis of suspicious behavior on endpoint devices (such as computers, laptops, and servers). This system collects and analyzes endpoint data to detect advanced threats.	Technical verification and evidence of traffic analysis.	Technical and Operational	**5**

1	Segmentation of the network into sub-networks at a micro-segmentation level.	Technical verification and supporting evidence of the network topology, with documented segmentation into sub-networks.	Technical and Operational	**5**
1	Placement of computers and servers into separate network zones/subnets/Virtual Local Area Networks (VLANs) with Access Control Lists (ACLs applied in accordance with the principle of least privilege).	List of implemented Virtual Local Area Networks (VLANs) and network sub-segmentation, including access control lists (ACLs). Technical verification and supporting evidence.	Technical and Operational	**5**
1	Isolation of the wireless network from the rest of the network.	Technical verification and supporting evidence of wireless network isolation configuration.	Technical and Operational	**3**
1	Use of switch port security techniques to limit the number of unique device identifiers (MAC addresses) allowed per port to "1" for regular users and to a limited number for Information Technology or cybersecurity experts.	Technical verification of switch configurations, applying the "Port Security" technique to restrict allowed Media Access Control (MAC) addresses of devices connected to the network.	Technical and Operational	**2**
1	Implementation of techniques and standards for hardening all network devices.	Device hardening manual (PCs, servers, routers, firewalls, etc.).	Technical and Operational	**4**

		Technical verification and supporting evidence.		
1	Logical isolation of databases and web services (e.g., in separate VLANs).	List of Virtual Local Area Networks (VLANs) and technical verification of configurations for the logical isolation of databases and web services.	Technical and Operational	**4**
1	Implementation of DNSSEC to prevent "DNS Amplification" and "DNS Poisoning" attacks.	Technical verification and supporting evidence.	Technical and Operational	**4**
2	Implementation of protection against DoS/DDoS attacks.	Technical verification of the configuration of DoS/DDoS protection mechanisms (e.g., "rate limiting," "WAF" – Web Application Firewall, anti-DDoS tools).	Technical and Operational	**5**
2	Implementation of a solution/system for controlling security parameters of endpoint devices ("NAC" – Network Access Control).	Procedure for defining minimum security baseline parameters. Technical verification and supporting evidence.	Technical and Operational	**5**
1	Implementation of policies for managing user passwords.	Password management policy document (complexity, expiration period, periodic changes).	Organizational	**1**

1	User access granting models (Discretionary Access Control – DAC, Mandatory Access Control – MAC, and Role-Based Access Control – RBAC).	Technical evidence of implemented system configurations and rules, and verification thereof.	Technical and Operational	**5**
1	Management of user access and privileges through the "AD" service.	Technical verification and supporting evidence of the implementation of Active Directory (AD) (group structures, privileges, restrictions).	Technical and Operational	**4**
1	Ensuring and protecting data and restricting unauthorized access to information.	Verification of the implementation of the "Clean Desk" policy/procedure and the policy/procedure for automatic screen locking after a defined idle period.	Technical and Operational	**2**
2	Implementation of Two-Factor Authentication (2FA) at the application/web/email/device level for all users of critical systems.	Verification and supporting evidence.	Technical and Operational	**4**
1	Implementation of Multi-Factor Authentication (MFA) at the application/web/email/device level for administrators.	Verification and supporting evidence of the implementation of Multi-Factor Authentication (MFA).	Technical and Operational	**5**

2	Use of Data Loss Prevention (DLP) methods to identify and prevent unauthorized leakage of sensitive data outside the infrastructure.	Verification of the implementation of Data Loss Prevention (DLP) methods to prevent leakage of sensitive data.	Technical and Operational	**4**
1	Conducting security testing of information technology applications and networks for Vulnerability Assessment (VA) and preparation of a remediation plan for the identified issues. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Vulnerability assessment report and remediation plan.	Technical and Operational	**5**
1	Verification that web services operate using the secure "HTTPS" protocol.	Technical verification and supporting evidence (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**5**
1	Configuration of anti-spoofing mechanisms: DMARC/SPF/DKIM in the email system.	Technical verification and supporting evidence (e.g., evidence of anti-spoofing implementation in the email system).	Technical and Operational	**5**
1	Conducting software development testing ("staging/testing") in a dedicated environment separate from the production environment, where the infrastructure has a development department.	Verification of evidence of a dedicated software testing environment, separated from the production environment.	Technical and Operational	**3**

2	Implementation of a solution for filtering, monitoring, and blocking malicious internet traffic using a Web Application Firewall (WAF).	Technical verification and supporting evidence (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**5**
2	Implementation of a Reverse Proxy on a server positioned between clients and internal backend servers, acting as an intermediary to process client requests and forward them to internal servers.	Verification of the implementation of a Reverse Proxy on web servers (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**3**
2	Conducting security testing of applications and networks (Penetration Testing – Black Box, Gray Box, White Box) and development of a remediation plan for identified issues. (At least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CII/III).	Reports of security testing ("black," "grey," "white") for application and network security assessment (penetration testing) and the associated remediation plan.	Technical and Operational	**5**
1	Implementation of a security procedure for software design and development. (Reviewed at least once (1) per year).	Documentation of the security procedure for software design and/or development.	Organizational	**1**

		The procedure must be approved by senior management and reviewed periodically.		
1	Control and monitoring of access for software developers and users.	Inclusion in the procedure of specific requirements, such as authentication, authorization, and encryption methods for software developers. Clear definition of rights and access privileges for software users	Technical and Operational	**3**
1	Maintenance of a history of changes, configurations, and approvals related to the development of software source code.	Technical verification and supporting evidence (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**3**
1	Risk and security analysis of software prior to production release.	Risk and security analysis reports for software prior to production release, including dependencies on third-party libraries.	Technical and Operational	**5**

1	Handling and documentation of cybersecurity incidents related to software development.	Audit reports and incident logs related to software development activities.	Technical and Operational	**5**
1	Monitoring of the software source code repository.	Monitoring reports of the software source code repository.	Technical and Operational	**3**
1	Encryption of source code at rest and in transit.	Technical verification and supporting evidence (e.g., evidence of encrypted code at rest and in transit).	Technical and Operational	**3**
1	Implementation of an encrypted application-to-database connection (“connection string”).	Technical verification and supporting evidence (e.g., evidence of encryption of the application-to-database connection).	Technical and Operational	**5**
1	Backup of source code and testing of backup integrity.	Technical verification and supporting evidence (e.g., evidence of the existence of source code backups and tests for code recovery from the stored backup).	Technical and Operational	**5**

2	Automation through pipelines (“CI/CD” – Continuous Integration / Continuous Delivery / Deployment) for continuous integration, development, testing, and deployment of software.	Technical verification and supporting evidence (e.g., visual evidence of CI/CD configurations and operation through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**5**
2	Implementation of security measures for microservices, including resource isolation, continuous monitoring, and enforcement of access controls.	Technical verification and supporting evidence (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**5**
1	Application of the principle of least privilege by implementing Role-Based Access Control (RBAC) for users, Access Control Lists (ACLs) for traffic filtering, and disabling unnecessary services on critical Operational Technology (OT) systems.	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Implementation of TLS/SSL and VPN for protocols (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Implementation of “Hot” and “Cold” backup techniques for data storage.	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Implementation of a Zero Trust–based remote access management solution (ZTNA).	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Controlled management of patches and configurations, with prior testing in test environments.	Technical verification and supporting evidence.	Technical and Operational	**5**

1	Implementation of a solution for software control in the production zone, using techniques such as Application Whitelisting, manually or automatically, to allow only authorized applications to execute.	Technical verification and supporting evidence.	Technical and Operational	**4**
1	Implementation of endpoint protection, including detection, response, and/or isolation mechanisms at both signature-based and behavior-based levels.	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Application of hardening techniques for Operational Technology (OT) devices such as PLCs, RTUs, HMIs, SCADA, BMS, etc.	Technical verification and supporting evidence.	Technical and Operational	**4**
1	Segregation of Information Technology (IT) infrastructure from Operational Technology (OT) by ensuring separate services for each infrastructure, such as Active Directory, Antivirus, Next-Generation Firewall (NGFW), and SIEM dedicated to Operational Technology.	Technical verification and supporting evidence.	Technical and Operational	**5**
2	Implementation of real-time monitoring of operational activities in Operational Technology systems, including logging, analysis, and alerting of events based on their functions and criticality to operations.	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Development, approval, implementation, and periodic review of procedures for the security of IoT devices and systems.	Procedure for the security of IoT devices and systems.”.	Organizational	**1**

1	Security of IoT devices • Definition of minimum requirements for hardware devices. • Use of mechanisms that ensure integrity (“tamper-proof”) and confidentiality (Trusted Platform Module – TPM). • Application of secure updates/patches for operating systems and firmware. • Ensuring the security of authentication keys. • Conducting traffic analysis at a behavioral level (where applicable).	Technical verification and supporting evidence (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**5**
2	Ensuring the integrity and confidentiality of data transmitted between IoT devices • Use of secure authentication certificates (for devices connected via an IoT Hub or IoT Central). • Ensuring secure communication (TLS 1.2 or higher). • Protection of IoT data during transmission and at rest. • Clear definition of access controls (IoT Hub and IoT Central application). • Implementation of security monitoring for IoT solutions.	Technical verification and supporting evidence (e.g., visual evidence of configurations through screenshots, logs, and detailed documentation of technical parameters).	Technical and Operational	**5**

1	Establishment of a governance policy/procedure for Cloud services.	Cloud security policy/procedure.	Organizational	**1**
1	Inclusion of technical, organizational, and security requirements in Service Level Agreements (SLAs) with Cloud service providers.	Service Level Agreement (SLA) document including key performance indicators, monitoring metrics, security requirements, and recovery objectives.	Organizational	**1**
1	Implementation of strong authentication mechanisms, such as Multi-Factor Authentication (MFA), for access to the Cloud management platform and services.	Verification and supporting evidence for the implementation of Cloud authentication.	Technical and Operational	**5**
1	Implementation of encryption mechanisms for data at rest and in transit.	Technical verification and supporting evidence.	Technical and Operational	**4**
1	Regular backup of critical and important Cloud services.	Technical verification and supporting evidence.	Technical and Operational	**5**
1	Enabling logging and monitoring of Cloud infrastructure activities.	Technical verification and supporting evidence.	Technical and Operational	**5**
2	Implementation of a network security architecture that combines networking and Information Technology security functions into a unified, Cloud-based platform, using Secure Access Service Edge (SASE).	Technical verification of the Secure Access Service Edge (SASE) solution. Verification and supporting evidence of users' utilization of the Secure Access Service Edge (SASE).	Technical and Operational	**3**