D E C I S I O N

No. 531, dated 25.09.2025

ON

THE CONTENT AND METHOD OF DOCUMENTING THE ORGANIZATIONAL, TECHNICAL, AND OPERATIONAL CYBERSECURITY MEASURES AND THE CATEGORIZATION OF DEADLINES FOR CORRECTIVE MEASURES IN CRITICAL AND IMPORTANT INFORMATION INFRASTRUCTURES

Pursuant to Article 100 of the Constitution and to Article 20(5) and Article 43(5) of Law no. 25/2024, "On Cybersecurity", upon the proposal of the Prime Minister, the Council of Ministers,

H E R E B Y D E C I D E D:

1. On adoption of the content and the method of documenting the organizational, technical, and operational cybersecurity measures in critical and important information infrastructures and of the categorization of the deadlines for corrective measures, according to the enclosed text to this decision and constituting an integral part thereof.
2. Operators of critical information infrastructures and the operators of important information infrastructures shall be in charge with the implementation of this decision.

This decision shall enter into force after its publication in the Official Journal.

P R I M E M I N I S T E R
EDI RAMA

CONTENT AND METHOD OF DOCUMENTING THE ORGANIZATIONAL, TECHNICAL AND OPERATIONAL CYBERSECURITY MEASURES AND THE CATEGORIZATION OF DEADLINES FOR CORRECTIVE MEASURES IN CRITICAL AND IMPORTANT INFORMATION INFRASTRUCTURES

CHAPTER I

GENERAL PROVISIONS

1. This decision aims to determine the method of documenting and verifying the implementation of organizational, technical, and operational measures by operators of critical information infrastructure (CII) and operators of important information

infrastructure (III), as well as the categorization of deadlines for corrective measures.

2. The provisions of this decision shall be applied by all operators of critical information infrastructures and operators of important information infrastructures.
3. The provisions of this decision shall be implemented without prejudice to the application of the security requirements for electronic communications networks and services set out in Chapter VII "Security" of Law no. 54/2024 "On electronic communication in the Republic of Albania."
4. The definitions in this decision have the same meaning as those provided by the legislation in force on cybersecurity.

CHAPTER II

CATEGORISATION AND CLASSIFICATION OF CYBERSECURITY MEASURES

1. The cybersecurity measures implemented by operators of critical information infrastructures and operators of important information infrastructures are divided into three main categories: organisational measures, technical measures, and operational cybersecurity measures.
2. Organisational measures of cybersecurity are administrative and procedural actions undertaken by operators of critical and important information infrastructures, including, among others, the assignment of roles and responsibilities for security, the drafting and adoption of security policies and procedures, cyber risk management, awareness and training of human resources, as well as the establishment of an organisational structure dedicated to cybersecurity.
3. Technical cybersecurity measures are technological solutions and mechanisms that ensure the protection and integrity of communication networks and information systems of the operators of information infrastructures, including the implementation of access control, authentication and authorization, data encryption, monitoring and logging of security events, protection against cyberattacks, as well as the implementation of technologies for the detection and prevention of cybersecurity incidents.
4. Operational cybersecurity measures are the processes, practices, and daily activities of information infrastructure operators for ensuring information security and the stable functioning of critical and important systems, including the management of cybersecurity incidents, ensuring service continuity and disaster recovery, management of changes in the infrastructure, as well as the application of procedures for reporting and communicating security events to the responsible authorities.
5. Cybersecurity measures categorized into organizational measures, technical measures, and operational measures are classified into two levels:
   a) level one (1): Mandatory for implementation by important information infrastructure operators (III) and critical information infrastructure operators (CII);
   b) level two (2): Mandatory for implementation by operators of critical information infrastructures (CII).
6. For each cybersecurity measure (SM1, SM2, etc.), operators of information

infrastructures must document and maintain records on their implementation and application in accordance with the requirements of this decision.

7. Cybersecurity measures and the method of their documentation shall constitute the list of minimum requirements for implementation by CII and III.

CHAPTER III

ORGANIZATIONAL MEASURES

1. Organizational measures include:

1.1.SM1: Security policy

The security policy shall include the security objectives related to the governance and management of security risks of communication networks and information systems**.**

Level	Security measure	Documentation/Verification of implementation
1	a. Establishment of a high-level security policy, approved by the senior management staff of the infrastructure, that addresses 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 after any major change in the CI/II infrastructure).	i. Information Security Policy • Document approved by the senior management staff, containing the objectives, scope of application, and security principles for networks and information systems, etc. • Version, date of approval, etc., ii. Periodic Review Reports • Records showing review dates and details of changes made to the security policy.

1.2.SM2: Cyber risk management

An appropriate risk management framework shall be established and implemented to identify and address cyber risks to communication networks and information systems.

Level	Security measures	Documentation/Verification of implementation
	a. Establishment of a a methodology for cyber risk management. (Review at least	i. Cyber risk management methodology document

1	once (1) per year and/or after each cybersecurity incident or after any major change in the CI/II infrastructure).	including the version, dates, and approval by senior management. ii. Periodic Review Reports • Records showing the dates of review and the details of changes made to the methodology for risk management.
1	b. Drafting a list of risks on the security of communication networks and information systems, taking into account key threats to critical assets. (Reviewe at least once (1) a year and/or after each cybersecurity incident or after any major change in the CI/II infrastructure).	i. Risk assessment list arising from various sources, including risks originating from third parties. ii. Notification of the managerial staff regarding the risk register as well as the decision taken for their remediation. iii. Review of the risk list.
1	c. Drafting a plan for addressing identified risks.	i. Document of the risk remediation plan. ii. Reflection of changes in the risk level after the implementation of the risk remediation plan.

1.3.SM3: Organisational security

An appropriate structure of security roles and responsibilities shall be established and implemented for the management of information security.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Assignment of roles and responsibilities for information security management.	i. List of security roles and detailed description of responsibilities and duties for each role, e.g. (*CISO, ISO, DPO, DBA, SYSADM, NETADM* etc.).

		ii. The organizational chart showing the hierarchy and links between security roles. iii. List of contacts for persons responsible for information security (name, position, contact details).

1.4.SM4: Cybersecurity requirements for third parties

A policy with security requirements for contracts with third parties shall be established and implemented in order to ensure that relationships with third parties do not adversely affect the security of communication networks and information systems.

Level	Security measures	Documentation/Verification of implementation
1	a. Establishment of a security policy for third-party supplies/contracts and its periodic review. (At least once (1) per year and/or after any cybersecurity incident or after any major change in the ICT/Information Resources Infrastructure).	i. Security policy for supplies/contracts with third parties (version, publication date, approval). ii. Periodic review reports of the security policy and the changes implemented.
1	b. Inclusion of security requirements in contracts with third parties, including confidentiality and secure transfer of information.	i. Clear security requirements in contracts with third parties. ii. Confidentiality agreement for the protection of information with third parties.

2	c. c) Maintenance of incident records and traces related to or caused by third parties.	i. Register of cyber incidents related to third parties (date, cause, impact, actions).

1.5.SM5: Security of human resources and access of individuals

A policy for the security and awareness of human resources as well as for access of individuals shall be established and implemented based on the security objectives regarding personnel.

Level	Security measures	Documentation/Verification of implementation
1	a. Establishment of a security policy for human resources.	i. Security policy for human resources (including all phases: pre-recruitment, during employment, disciplinary procedures, upon termination of the employment relationship). ii. Integrity verification document for key personnel (verification certificate of judicial status (criminal record certificate), references from previous jobs, certifications, CV, etc.). iii. Procedure for the protection of personal data.
1	b. Implementation of a cybersecurity training program. (Review at least once (1) per year).	i. Detailed training program, tailored according to the roles and responsibilities of the employees. ii. List of participants and training dates.

		iii. Document on the implementation of awareness campaigns/trainings for employees regarding cybersecurity and the most common cybersecurity attacks such as "*Phishing", "Malware",* etc.
1	c. Informing and training new employees on the current policies and procedures for cybersecurity.	i. Record of training for new employees. ii. Forms signed by employees for acknowledgment of policies and procedures. iii. Forms signed by employees for the Non-Disclosure Agreement ("NDA*").*
2	ç. Testing of employees' knowledge on cybersecurity. (At least once (1) per year for employees who use critical information systems in the infrastructure and/or more frequently depending on cyber incidents.)	i. Questionnaires and test results for employee awareness regarding cybersecurity.

1.6.SM6: Asset management

Asset management procedures and configuration controls shall be established and implemented to ensure the availability of critical assets and the configurations of communication networks and information systems.

Level	**Security measures**	**Documentation/Verification of implementation**

1	a. Measures taken to identify and effectively manage assets. (At least once (1) per year and/or after any major change in CI/II infrastructure).	i. Full inventory of Information Technology ("IT") assets/Operational Technology (OT*)*, including e.g. the model, asset category, serial number, internet protocol ("*IP"*), location, obsolescence , their status, etc. ii. Inventory classification of impact according to Confidentiality, Integrity, and Availability *("*C/I/A*")* of the asset.
1	b. Establishment and implementation of asset management policies/procedures.	i. Detailed policies/procedures for asset management including roles and responsibilities, the assets subject to this policy/procedure, asset management objectives, as well as the destruction of assets. (Review at least once a year and/or after any major change in the CI/II infrastructure). ii. Detailed topology of the network and information systems.
1	c. Measures taken for the replacement or isolation of systems whose life cycle has ended ("EOL*"- End of Life)*.	i. Document or record of identification of systems that have reached their end of life (EOL) ii. Record of replacement/isolation of the asset which has reached the end of its life cycle (EOL). iii. Verification of systems and records.

1	ç. Automatic/manual patches carried out in the end-point systems and throughout the information technology (IT) and operational technology (OT) infrastructure.	i. Procedure for managing the implementation of patches for information technology (IT) and operational technology (OT) equipment and systems, including frequency, responsible persons, records. ii. Verification of systems/ *tools* and records.
1	d. 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 the protection of information and compliance with security standards.	i. Policy/procedure for the use of personal devices (phones, laptops, tablets, etc.), as well as an inventory of personal devices authorized for use in the internal networks and systems of the infrastructure. ii. Records of minimum security configurations of personal devices according to the policy.

1.7.SM7: Management of cybersecurity incidents

Plans and procedures for the management of cyber incidents, including their detection, response, reporting, and communication, shall be drafted and implemented.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Drafting of detailed plans and procedures for the management of cybersecurity incidents. (Review at least once (1) per year and/or after each	i. Document of the plan for the management of cyber incidents (version, date, approval). ii. Procedure for the identification, classification and handling of incidents (Action Manual -

	cybersecurity incident or after any major change in the CI/II infrastructure).	"*Playbooks")*, the list of the members of the cyber incident response team).
1	b. Keeping records of all cybersecurity incidents.	i. Incidents register which includes: the date, the cause, the impact, and the corrective actions. ii. Individual reports on incident handling and analyses of lessons learned.
1	c. Determing and implementating communications and reporting of cyber incidents to the authorities and the notification of third parties and clients.	i. Incident reporting forms for the authorities designated in the applicable legislation on cybersecurity, by the infrastructure. ii. Inventory of communications and reportings.

1.8.SM8: Change management

Policies and processes shall be defined and implemented for change management through planning, assessment, approval, communication, implementation, and monitoring of changes in infrastructure.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Ensuring that any changes in the systems and processes of information technology (IT) infrastructure within Critical / Important Infrastructure are managed in a controlled and documented manner.	i. Change management policy (including description, date, responsibilities and anticipated impact, implementation plan, etc.). (Reviewe at least once (1) per year.) ii. Change management procedure (steps from proposal to approval and implementation). iii. Request for Change form ("RFC").

1.9.SM9: Business continuity management

Emergency plans and a clear strategy shall be established and implemented to ensure the continuity of communication networks and information systems.

Level	Security measures	Documentation/Verification of implementation
1	a. Establishment and implementation of a Business Continuity Plan ("BCP") to ensure the continuous operation of critical infrastructure processes in the event of cyber incidents, natural disasters, or operational disruptions. (Review at least once (1) per year and/or after any cybersecurity incident or following any major change in the infrastructure of CI/II).	i. The strategy policy for service continuity, including the conditions for activating the plan, recovery time, crisis-time communication, incident scenarios, action plan, testing rules, etc. ii. Business Impact Analysis (BIA), Identification of critical processes and determination of the Recovery Time/Point Objective *("*RTO*"* - *Recovery Time Objective / "*RPO*"* – *Recovery Time Objective)*. iii. Emergency contact list – information for contact points in case of crisis.
1	b. Use of data mirroring techniques through redundant configuration of independent disks (*"*RAID*"* -*Redundant Array of Independent Disks*).	i. Technical verification of the redundant configuration of independent disks ("RAID") (**1/5/6/10**) and the relevant records.
1	c. Implementation of a policy/procedure for performing backups . (At least once (1) per year and/or after any	i. Policy/procedure document for performing backups, including frequencies, types, data, and services.

	cybersecurity incident or after any major change in the CI/II infrastructure).	ii. Backup list performed and the reports of data recovery and integrity testing.
2	ç. Establishment of backup copies using techniques such as "*Backup Lock Retention*" or "*Tape Worm*".	i. Evidence of the use of techniques '*Backup Lock Retention"* or "Tape Worm".
2	d. Avoidance of single points of failure in the critical and important services of infrastructure.	i. Technical verification of single points of failure. ii. Record keeping for Service Redundancy.
2	dh. Implementation of infrastructure according to high availability ("HA") service schemes.	i. Document of infrastructure schemes according to the high-availability (HA) service at the technical support levels: L1, L2, L3, and the perimeter with digital firewall. ii. Verification and records.
2	e. Implementation of a secondary environment for the recovery and continuity of operation of information technology (IT) systems after a cyber incident ("DRS*"- Disaster Recovery Site*).	i. Strategy for BCP and detailed configurations. (Review at least once (1) a year and/or after any cybersecurity incident or after any major change in the infrastructure of CI/II). ii. Disaster Recovery Plan (*DRS),* Procedures for the recovery of Information Technology (IT) and infrastructure (Duties and responsibilities, list of key systems and assets). (To be reviewed at least once (1) per year and/or after every cybersecurity incident or after any major change in the CI/II infrastructure). iii. Test reports of the second environment for the recovery and

		continuity of the operation of information technology systems for disaster recovery (DRS). (At least once a year and/or after every cybersecurity incident or after every major change in the CI/II infrastructure). iv. Verification and record keeping.
2	*Optional:* ë. Implementation of Software Defined Networking ("SDN*")* so that critical services and applications can recover as quickly as possible and with minimal (or no) disruption to services in the event of disasters or incidents.f. Implementation of the "*Blockchain*" technology to decentralize data management while ensuring data protection and inviolability during recovery.	i. Strategy to ensure that critical services and applications (including those relying on Software Defined Network (SDN) technologies) and "*Blockchain*" to have the possibility of recovery as quickly as possible and with minimal interruption, in case of disasters or incidents. ii. Periodic testing of Software Defined Network (SDN) technology configurations. iii. Verification of the implementation of the technique "*Hashing*". iv. Backup policy for the technology "*Blockchain*". v. Monitoring of activity in "*Blockchain*".

1.10. SM10: Legal compliance management

A policy for monitoring compliance of standards with legal requirements shall be established and implemented

Level	**Security measures**	**Documentation/Verification of implementation**

1	a. Monitoring the compliance of standards with legal requirements.	i. Policy/Procedure for monitoring compliance with standards and legal requirements. ii. List of standards and legal requirements applicable to the infrastructure. iii. Review of policies and procedures for the Information Security Management System ("ISMS"), at a minimum 1 (one) time per year and/or after any cybersecurity incident or after any major change in the CI/II infrastructure.

1.11. SM11: Control and audit

Policies and procedures shall be established and implemented for conducting internal and external controls and audits, with the aim of monitoring compliance and continuously improving information security within the infrastructure.

Level	Security measures	Documentation/Verification of implementation
1	a. Policy/procedure for internal control and audit for information security and periodic review. (At least once (1) a year and/or after any cybersecurity incident or after any major change in the CI/II infrastructure).	i. Document of the policy/procedure for controls and audits (version, date, approval of the policy/procedure by senior management staff).
1	b. Conducting internal or third-party checks/audits for the security of	i. Internal audit reports and deficiency remediation plan (date, methodology, results).

	information and critical infrastructure systems. (At least once (1) per year and/or after any cybersecurity incident or after any major change in the CI/II infrastructure).	ii. Audit reports conducted by third parties on information security. iii. List of corrective actions undertaken following audits and records of their implementation.

CHAPTER IV

TECHNICAL AND OPERATIONAL MEASURES

2. The technical and operational measures include:

2.1.SM1: Physical security

Appropriate physical and environmental security for information networks/systems and devices shall be established and implemented.

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of physical security measures and environmental controls.	i. Records of the implementation of physical security measures (locks, cabinets, electronic access control). ii. Audit logs for access to authorized areas and alerts for unauthorized entries. iii. Reports on the operation and maintenance of alarm systems and fire extinguishers.. iv. Ensure the division of physical spaces into segmented zones based on authorization levels, including the drafting of a detailed topology and a clear evacuation plan to guarantee

		physical security and access management.
1	b. Implementation of a policy on physical security measures and environmental controls.	i. The physical security and environmental controls policy document (version, date, approval, review).

2.2. SM2: Management for access authorization

Appropriate access controls and authorisations to communication networks and information systems shall be established and maintained.

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of policies for controlling and protecting access to networks and information systems. (Review at least once (1) per year and/or after any major change to the CI/II CII/IIS infrastructure).	i. Access policy document (roles, groups, rights, procedures for granting and revoking access). ii. Form for granting access rights. iii. Form for revoking access rights and handing over assets. iv. Records of the deletion of generic accounts and reports of periodic access controls.
1	b. The application of traffic filters in the case of remote access to systems, as well as the encryption of traffic with secure protocols.	i. Technical verification and records for the installation of filters and the encryption of traffic.
1	c. Control whether in the firewall it has configured authorized lists/blocked lists ("*Whitelist/Blacklist*") of Internet Protocol	i. Verification and record for the configurations in firewall.

	addresses (*IP)* allowed or blocked.	
1	ç. Use of policies for the management of random passwords for users and local administrators.	i. Policy document for password management and verification of the implementation of solutions for random password management for users and local administrators ("LAPS*"*- *Local Administrator Password Solution*) or similar technology.
2	d. Establishement and implementation of a technological solution for Identity and Access Management ("IAM*")* to guarantee the security, authorisation, and audit of user activities in critical systems.	i. Technical verification and record keeping.
2	dh. Implementation of a technological solution for the Privileged Access Management ("PAM*" –)*	i. Technical verification and record keeping.
2	e. Implementation of the security service with Network Access according to the zero trust principle ("ZTNA*"* - *Zero Trust Network Access*)	i. Technical verification and record keeping.

2.3. SM3: Cryptographic Devices

Ensure the sufficient use of encryption to prevent and/or minimize the impact of cybersecurity incidents on users within communication networks and information systems.

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of encryption policies including details regarding algorithms and cryptographic keys.	i. The encryption policy document, such as: algorithms: "*AES", "RSA", "ECC", "TLS", "IPSec", "SSH*", etc. ii. List of cryptographic keys (e.g., type, validity period, method of generation and storage).
2	b. Encryption of data (in transit and at rest).	i. List of encryption configurations for data and applications ("*on-prem*", "*hybrid*", "*cloud*"). ii. Technical verification and record keeping.

2.4. SM4: Detection of cybersecurity incidents

To establish and maintain capacities for the detection of cybersecurity incidents.

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of the automated system for the detection and management of information and security incidents/events ("SIEM" - Security Information and Event Management).	i. Technical verification and configuration records of the automated system for the detection and management of information and security incidents/events (SIEM) including the rules for alerting and filtering of traces and activities (log*s*) for incident detection.

2.5. SM5: Collection and processing of information on cyber threats

To establish and maintain a mechanism for monitoring, collecting and analyzing information related to security threats in communication networks and information systems.

Level	Security measures	Documentation/Verification of implementation
1	a. Continuous monitoring of external cyber threat intelligence sources.	i. Periodic reports from cyber threat intelligence monitoring tools. ii. List of sources used for collecting information on threats.
2	b. Implementation of the cyber threat intelligence program, in which the roles, responsibilities and procedures shall be included.	i. Document of the cyber threat intelligence program (including the structure of roles and responsibilities). ii. Procedure for the collection, processing, analysis, and dissemination of cyber threat information.

2.6. SM6: Monitoring and logging of cybersecurity incidents

To establish and maintain systems and functions for monitoring and logging security events in critical networks and information systems.

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of policies for monitoring and logging cybersecurity events.	i. Policy document for monitoring and logging traces and activities (log*s)*, including minimum requirements, retention periods, objectives, approval, and updates.
1	b. Placement of means for the collection of traces and	i. List of implemented tools for collection of traces and

	activities (log*s)* of critical systems.	activities/logs of log servers etc. ii. Technical verification and record keeping.

2.7. SM7: Protection of the integrity of communication networks

To establish and maintain the integrity of networks and information systems and to protect them against viruses, code injections and other malware that may alter the functionality of the systems.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Installation of devices to monitor, control, and restrict inbound and outbound traffic in computer networks using next generation firewall.	i. Technical verification for the configuration of the next generation firewall. ii. Technical verification and record keeping.
1	b. Monitoring, detection and analysis of suspicious behaviours on endpoints, such as computers, laptops, and servers. This system collects and analyzes data from endpoints to detect sophisticated threats.	i. Technical verification and records of traffic analyses.
1	c. Network segmentation into subnets at the microsegmentation level.	i. Technical verification and records of the network topology with documented segmentation into subnets.
1	ç. Placement of computers and servers in areas/ subnets / *VLAN* with access control	i. List of implemented Virtual Local Area Network (VLAN*)*

	list following the least privilege principle.	and subnets, including access control lists. ii. Technical verification and record keeping.
1	d. Isolation of the wireless network from the rest of the network.	i. Technical verification and records of the wireless network isolation configuration.
1	dh. Use of switch port security techniques to limit the number of unique device identification addresses connected to the network *(*MAC Address) to "1" for regular users and a limited number for information iechnology or cybersecurity experts.	i. Technical verification of the switch configuration implementing Port Security technique for the allowed MAC Address.
1	e. Implementation of hardening techniques and standards of all network devices.	i. Device hardening guide (*PC,* "server", "router*",* "firewall", etc.). ii. Technical verification and record keeping.
1	ë. Logical isolation of database and web services (e.g. various virtual local networks/VLAN).	i. List of virtual local area network (VLAN) and technical verification of configuration for logical isolation of database and web services. ii. Technical verification and record keeping.
1	f. Implementation of "DNSSEC" to prevent DNS Amplification and DNS Poisoning.	i. Technical verification and record keeping.

2	g. Implementation of protection against DoS/DDoS attacks.	i. Technical verification of the configuration of DoS/DDoS protection mechanisms (e.g. "rate limiting", "WAF" - Web Application Firewall, "anti-DDoS" tools.
2	gj. Implementation of a solution/system for the control of the endpoint security baseline ("NAC" - Network Access Control).	i. Procedure for determining minimum security baseline. ii. Technical verification and record keeping.

2.8. SM8: User access management

To implement policies for password management and access control according to the Discretionary Access Control ("DAC") models", Mandatory Access Control ("MAC") and Role-Based Access Control ("RBAC"). The *Active Directory* (*AD)* service shall be used for managing privileges and restricting unauthorized access to devices.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Implementation of policies for user passwords management.	i. Password management policy document (complexity, expiration period, periodic changes).
1	b. Access control models for user access (Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC).	i. Technical documentation of configurations and rules implemented in the system and verification.
1	c. Management of user access and privileges through the "AD" service.	i. Technical verification and evidence of "AD" implementation (group

		structures, privileges, restrictions).
1	ç. Ensuring and protection of data and restriction of unauthorized access to information.	i. Verification of implementation of *Clean Desk* policy / procedure and the policy/ procedure for automatic screen lock after a period of inactivity ("*idle*").
2	d. Implementation of 2 (two) Factor Authentication ("2FA") systems at the application /web/ mail/ device level for all users of the critical system.	i. Verification and record keeping.

2.9. SM9: Administrator Activity and Authentication

Access for administrators shall be ensured by implementing Multi-factor Authentication (MFA) at the applications, web, email, and devices. Platforms for Data Loss Prevention (DLP) shall be used for the prevention of unauthorized leakage of information.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Implementation of Multi-Factor Authentication (MFA) at the application/web/mail/device level for administrators.	i. Verification and record keeping of the implementation of the Multi-Factor Authentication (MFA) method.
2	b. Use of the Data Loss Prevention (DLP) method for identifying and preventing the unauthorized leakage of sensitive data outside the infrastructure.	i. Verification of the implementation of Data Loss Prevention (DLP) method to prevent leakage of sensitive data.

2.10. SM10: Application security

Ensure the protection of applications by conducting security testing for Vulnerability Assessment ("VA") and Penetration Testing and addressing the identified issues.

Level	Security measures	Documentation/Verification of implementation
1	a. Conducting tests for the security assessment of information technology applications and networks for Vulnerability Assessment (VA) and the drafting of the plan for addressing the identified issues. (At least once (1) per year and/or after every cybersecurity incident or after any major change in the CII/III infrastructure.)	i. Vulnerability Assessment report and remediation plan.
1	b. Control whether web services operate by implementing the secure "https" protocol.	i. Technical verification and record keeping (e.g. visual records of configurations through "screenshot", logs and the detailed documentation of technical parameters).
1	c. Configuration of *anti-spoofing:* DMARC/SPF/DKIM in the email system.	i. Technical verification and record keeping (e.g. record of the implementation of anti-spoofing in the email system).
1	ç. Conducting software development testing (*staging*) in a dedicated area separated from the production area , if the	i. Verification of record keeping of the environment dedicated to software testing, separated from the production environment.

	infrastructure has a development department.	
2	d. Implementation of a solution for filtering, monitoring, and blocking malicious internet traffic, with a digital firewall for Web Application Security (WAF).	i. Technical verification and record keeping (e.g. visual records of configurations through *screenshot*, log events and detailed documentation of the technical parameters.).
2	dh. Implementation of "Reverse Proxy" on a server positioned between clients and "backend servers" and acts as an intermediary to process requests from clients and forward them to backend servers.	i. Verification of "Reverse Proxy"implementation on web servers (e.g. visual records of configurations through screenshot, logs and the detailed documentation of the technical parameters.).
2	e. Conducting tests for the assessment of the security of applications and networks (*Penetration Test – Black, Gray, White*) and drafting a plan to address identified issues. (At least once (1) per year and/or after any cybersecurity incident or after any major change in the CII/III infrastructure).	i. Test report of the types: "*black*", "*grey*", "*white*", for the assessment of the security of applications and networks (*penetration test*) and the remediation plan.

2.11. SM11: Software Production Security

The software production security for critical or important infrastructure shall include the practices and measures that enable the design, development, testing, and implementation of highly secure software, to protect infrastructure from cyberattacks**.**

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of a security procedure for the design and development of the software. (To be reviewed at least once (1) per year)	i. Documentation of the security procedure for the software design and/or development. ii. The procedure shall be approved by senior management staff and reviewed periodically.
1	b. Control and monitor access of software developers and users.	i. Include in the procedure specifics such as the method of authentication, authorization, encryption for software developers. ii. To clearly define the rights and accesses for software users.
1	c. Preservation of the history of changes/configurations/approval of software source code development .	i. Technical verification and record keeping (e.g. visual record of configurations through "*screenshot*", log files and detailed documentation of technical parameters).
1	ç. Risk and security analysis of the software before it goes into production.	i. Risk and security analysis reports of the software before going into production, including dependence on third-party libraries.
1	d. Handling and documenting cybersecurity incidents in software development.	i. Audit reports and logs of software development incidents.
1	dh. Monitoring the source code repository of the software.	i. Monitoring reports of the software source code repository.

1	e. Encryption of the source code at rest and in transit.	i. Technical verification and record keeping (e.g. record of encrypted code at rest and in transit).
1	ë. Implementation of the encrypted connection of the application with the database (*"connection string").*	i. Technical verification and record keeping (e.g. record of the encryption of the application's connection to the database).
1	f. Performing source code backup and testing the integrity of the backup.	i. Technical verification and record keeping (e.g.existence of source code backups and successful recovery tests).
2	g. Automation through "pipeline" ("CI/CD" – Continuous Integration / Continuous Delivery / Deployment) continuous integration / development/ continuous implementation of the process of software development, testing and publishing.	i. Technical verification and record keeping (e.g. visual record of configurations and functioning of CI/CD through "screenshot", logs and detailed documentation of technical parameters).
2	gj. Implementation of security measures for microservices, including the isolation of sources, continuous monitoring and the application of access controls.	i. Technical verification and record keeping (e.g. visual record keeping of configurations through "screenshot", logs and detailed documentation of technical parameters).

2.12. SM12: Security of Operational Technology (OT) systems

Ensure the protection of operational technology systems by applying the principle of least privilege access, network segmentation, and encryption of critical protocols. Measures shall be implemented for access control, real-time monitoring, and protection of devices against

cyberattacks and malware.

Level	Security measures	Documentation/Verification of implementation
1	a. Implementation of the principle of least privilege access by implementing Role-Based Access Control (RBAC) for users, Access Control List ("ACL") for traffic filtering , as well disabling unnecessary services in critical operational technology (OT) systems	i. Technical verification and record keeping.
1	b. Implementation of TLS/SSL, VPN for protocols (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	i. Technical verification and record keeping.
1	c. Implementation of the "Hot" and "Cold" backups techniques, for data protection.	i. Technical verification and record keeping.
1	ç. Implementation of a remote access management solution based on the *Zero Trust Network Access (ZTNA)* principle.	i. Technical verification and record keeping.
1	d. Controlled *patch* and configuration management with prior testing in test environments.	i. Technical verification and record keeping.

1	dh. Implementation of a software control solution in the "*production area"*, using techniques such as "Application Whitelisting*"*, either manually or automatically, to allow only authorised applications to execute.	i. Technical verification and record keeping.
1	e. Implementation of endpoint protection, including mechanisms for detection, response, or isolation of the attack at the signature and behaviour level.	i. Technical verification and record keeping.
1	ë. Implementation of the hardening techniques to operational technology equipment (PLC, RTU, HMI, SCADA, BMS, etc.)	i. Technical verification and record keeping.
1	f. Separation of information technology infrastructure from operational technology (providing specific services for each infrastructure, such as "Active Directory", "Antivirus", "NextGen Firewall", and SIEM that are dedicated to operational technology.	i. Technical verification and record keeping.
2	g. Implementation of real-time monitoring of operational actions in operational technology systems, as well as the registration, analysis, and notification of events based on their functions and	i. Technical verification and record keeping.

	importance for critical operations.	

2.13. SM13: Security of *Internet of Things*(“*IoT”)* systems.

To draft and implement procedures for the security of “*IoT” devices* including the use of mechanisms that guarantee the integrity and confidentiality of the systems. Secure updates shall be implemented and the protection of authentication keys on “IoT” devices shall be ensured.

Level	**Security measures**	**Documentation/Verification of implementation**
1	a. Drafting, approval, implementation and periodic review of procedures for the security of “IoT” devices and systems.	i. Procedure for the security of “IoT” devices and systems.
1	b. Security of “IoT” devices: • Determination of the minimum requirements for the hardware devices. • Use of mechanisms that guarantee integrity (e.g. *tamper proof*) and confidentiality (e.g. *Trusted Platform Module*). • Application of secure updates/upgrades of operating systems and “firmware".	i. Technical verification and record keeping (e.g. visual record keeping of configurations through screenshot, logs and detailed documentation of technical parameters).

	• Ensuring the security of authentication keys. • Conducting traffic analysis at the behavioral level (where applicable).	
2	c. Ensuring the integrity and confidentiality of data transmitted between "*IoT" devices:* • Use of authentication certificates that provide security (devices with Hub or" "*IoT"" Central*). • Ensuring secure communication (TLS 1.2 or higher). • Securing "*IoT" data* in transit and at rest. • Clear definition of access controls ("*IoT hub*" and "*IoT" Central* application). • Implementation of monitoring the security of "*IoT" solutions.*	i. Technical verification and record keeping (e.g. visual records of configurations through "screenshot", logs and detailed documentation of technical parameters).

2.14. SM14: Security in Cloud services

Security in "*Cloud"* services shall include the measures and policies that ensure the protection of data and infrastructure services, including strong authentication, data encryption, and activity monitoring. These measures shall be intended to guarantee the integrity, availability, and confidentiality of the systems used in "*Cloud*", as well as compliance with technical requirements and Service Level Agreement ("SLA*"*) established with the service providers.

Level	Security measures	Documentation/Verification of implementation
1	a. Establishment of a governance policy/procedure for "*Cloud"* services.	i. "*Cloud*" security policy/procedure.
1	b. Inclusion of technical, organizational, and security requirements in Service Level Agreements (SLA) with "*Cloud*" service providers.	i. The document of Service Level Agreement (SLA) which includes key performance indicators, monitoring metrics, security and recovery.
1	c. Implementation of strong authentication, such as Multi-Factor Authentication (MFA) for access to the "*Cloud*" administration platform and services".	i. Verification and records of "*Cloud*" authentication implementation.
1	ç. Implementation of an encryption mechanism for data at rest and in transit.	i. Technical verification and record keeping.
1	d. Regular establishment of the backup for critical and essential "*Cloud*" services.	i. Technical verification and record keeping.
1	dh. Implementation of log activation and monitoring of "*Cloud*" infrastructure activities.	i. Technical verification and record keeping.
2	e. Implementation of a network security architecture that combines network and information technology	i. Technical verification of the Secure Access Service Edge (SASE) solution.

	security functions into a unified "Cloud-based platform". U of Secure Access Service Edge ("SASE").	ii. Technical verification and record-keeping of the use of the Secure Access Service Edge (SASE) by the users.

CHAPTER V

CATEGORISATION OF DEADLINES FOR CORRECTIVE MEASURES

1. Based on Article 43 of Law No. 25/2024 "On Cybersecurity", in cases where the NCSA identifies deficiencies in the implementation of security measures, it shall determine a reasonable deadline within which operators of critical and important information infrastructure take the relevant corrective measures.
2. Deadlines for addressing identified deficiencies related to security measures shall be determined based on the level of risk for each deficiency or finding.
3. The risk assessment levels and deadlines for the implementation of corrective measures are as follows:

Risk Value	Risk level	Processing Time
[1-3]	Very low	No remediation required
[4-6]	Low	No remediation required
[7-11]	Medium	Must be remediated within 12 months
[12-19]	High	Must be remediated within 6 months
[20-25]	Very high	Must be remediated within 3 months

4. The National Cyber Security Authority (NCSA) may decide to extend the deadlines for the fulfillment of corrective measures by operators of Critical Information Infrastructures (CII) and operators of Important Information Infrastructures (III). This decision shall be taken only in exceptional cases, based on a documented assessment of the specific circumstances, upon a reasoned request from the respective infrastructure or at the initiative of NCSA itself.
5. Operators shall be required to notify the NCSA of the corrective measures undertaken within the specified deadline, as well as to submit the supporting documentation for these measures.