TLP:CLEAR

IMC_02 – Dictionary of Cyberresilience Improvement Indicators (CII)

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

February 2023

IMC_02 – dictionary-indicators version 2.8

INDEX

FIGURES INDEX

No se encuentran elementos de tabla de ilustraciones.

TABLE INDEX

1. DOCUMENT OBJECT

This dictionary describes the Cyber resilience Improvement Indicators (CII) for organizations and companies of industrial sectors and industrial critical infrastructures with respect to the fields of IT (Information Technology) and OT (Operation Technology).

These indicators can be used to define maturity consultation surveys —for each company, sector or group of companies— which determine the levels of resilience (for the objectives anticipate, resist, recover and evolve) corresponding to the provision of its essential services.

All indicators are valued according to the criteria indicated in the methodology assessment described in the document: IMC_01 - Methodology for Assessing Cyber resilience Improvement Indicators (CII).

2. INDICATORS

In this section is described, in independent tables, each of the Cyber resilience improvement indicators.

- The indicators are identified with a code (X-XX-OEN-NN) consisting of:
- X: The letter that corresponds to the goal according to the methodology.
- XX: The two letters that indicate the functional domain according to the methodology.
- OEN: The letters OE (specific objective, from Spanish Objective Specific) followed by a number that identifies each of the specific objectives.
- NN: The number that identifies each metric.

For the definition of "essential service[1]", It is taken as a reference the Ley 8/2011 (Spanish Act 8/2011), of April 28th, by which establishes measures for the protection of critical infrastructures.

Each table includes the following fields: identification, characterization, collection and analysis.

The **identification** field contains the following subfields:

- the indicator code, as described above;
- the goal to which it belongs;
- the functional domain in which it is been assessed;
- the indicator's objective;
- the indicator's description;
- the question issued and
- the correlation subfield that includes the guidelines, standards and rules on which each indicator is based.

The **characterization** field establishes and describes the **scale** of levels on which the organization identifies its compliance status for each indicator: L0, L1, L2, L3, L4 or L5.

The field of **collection** details the **method of collection** of the information for the indicator, and the **responsible** in charge of carrying it.

Finally, the table includes the field of **analysis**, with two subfields:

- **Objective measure**: where the optimum level that the organization must reach is established.
- Indicator with two elements: positive values and corrective measures. In the first one, the justification on which the organization can be considered at a high level is indicated. In the second element, the measures to be taken by the organization to increase the level within the scale with respect to the indicator.

2.1. Anticipate

The tabs for the metrics corresponding to the Anticipate goal are detailed below.

[1] Service that is necessary for the maintenance of basic social functions, health, safety, social and economic welfare of citizens, or the effective functioning of State Institutions and Public Administrations.

2.1.1. Cybersecurity Policy (CP)

The general objective of this functional domain is to have a cybersecurity policy that establishes the requirements of cyberresilience, contemplates the risks of cybersecurity, assigns responsibilities and is communicated to the entire organization. Its specific objectives are:

- To establish and to communicate the mission, objectives and priority activities to the entire organization.
- To establish responsibilities in the field of cybersecurity.
- To identify the critical functions of the organization and establish the requirements of cyber resilience.
- To have a continuity and recovery strategy.
- To collaborate with other organizations in the field of cybersecurity.

In addition, the following indicators correspond to it:

FIELD	INFORMATION
ID	
Code	**A-PC-OG1-01**
Goal	ANTICIPATE
Functional domain	CYBERSECURITY POLICY
Indicator objective	Establish, update and maintain a Cybersecurity policy.
Description	Establish the formal rules to which the organization's assets (employees, processes and technology) must be subject, in terms of information security. That policy must be approved by the Management.
Question asked	Has a cybersecurity policy been established within the organization?
Correlation	ISO/IEC 27001:2022 [5.1], [6.1.3] NIST SP 800-53 R5 [PL-01-00] ENS [Article 12] y Annex II sección 3.1 Minimum content guide PSO (2.1, 4.2.1) NIS Transposition (Cap. 1, 2 y Art.6)
CHARACTERIZATION	
Scale	**L0 -** No cybersecurity policy has been established. **L1 -** The establishment of a cybersecurity policy has begun. **L2 -** A policy has been established, but it is not formal (it has not been documented or approved by the Management).

	L3 - A Cybersecurity policy has been documented and has been approved by the Management and is kept up to date. **L4 -** The Cybersecurity policy is managed, updated and maintained regularly. **L5 -** Actions are applied to measure the level of compliance with the Cybersecurity policy.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has established a cybersecurity policy that allows the protection of information assets in a correct way.
	Corrective actions	Establish, formalize and review the Cybersecurity policy, to ensure correct adaptation to the organization's context, while arbitrating elements to measure its level of compliance (for example, through security audits).

Table 1 - Metric A-PC-OG1-01: Establish, update and maintain a Cybersecurity policy.

CAMPO	INFORMACIÓN
ID	
Code	**A-PC-OE3-02**
Goal	ANTICIPATE
Functional domain	CYBERSECURITY POLICY
Indicator objective	Establish Cyber resilience requirements to support essential services.
Description	Cyber resilience requirements are established for the essential service. It is about knowing to what extent cyberresilience is conceived as something different and specific within cybersecurity. To measure cyberresilience, at least one critical essential service must be identified. This indicator measures the degree of commitment of the organization to the definition of specific cyberresilience objectives (for the essential service identified as having the greatest impact) and the requirements to fulfil them. In the event that there are several essential services identified, a survey can be made for each one. Different surveys may also be carried out for the OT and IT areas. If the essential service belongs to the OT scope, the cyberresilience requirements should include, for example, the secured remote accesses from the Internet to elements such as PLC, HMI, RTU, etc., that support the essential service.
Question asked	Have the cyberresilience requirements been established for an essential service (choosing the one whose interruption or alteration causes the greatest impact)?
Correlation	ISO/IEC 27001:2022 [A.5.1], [A.5.8] NIST SP 800-53 R5 [PM-07-00], [SA-02-00], [SA-08-13] ENS [org.1] [Article 11] Minimum content guide PSO (3.1,3.3) NIS Transposition (Art.6 y 7)
CHARACTERIZATION	

Scale	**L0** - No cyberresilience requirements have been established. **L1** - The identification of cyberresilience has started. **L2** - Cyber resilience requirements have been established, but they have not been documented. **L3** - Cyber resilience requirements have been documented and are kept up to date. **L4** - Cyber resilience requirements are managed, updated and verified. **L5** - Improvement actions are applied in the definition of cyberresilience requirements.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has identified and documented the cyberresilience requirements for the identified essential service, that these requirements are exact and up to date. These requirements should allow managing risks, managing vulnerabilities, managing incidents, managing service continuity, and managing configurations and changes, reducing the impact or alteration of identified essential services.
	Corrective actions	• Identify, document and review the cyberresilience requirements of the identified essential service. • Update the documentation associated with the cybersecurity policy.

Table 2 - Metric A-PC-OE3-02: Establish Cyberresilience requirements to support essential services.

CAMPO	INFORMACIÓN
ID	
Code	**A-PC-OE5-01**
Goal	ANTICIPATE
Functional domain	CYBERSECURITY POLICY
Indicator objective	Collaborate with public or private entities on cyberresilience.
Description	Establish formal agreements for mutual aid, cooperation or exchange of information with public or private entities in the field of cyberresilience, such as, for example, incident response centres or CERT, INCIBE-CERT, cybersecurity consulting companies, suppliers and other companies in the sector. Formalization means that a document is approved by the Management.
Question asked	Has a formal agreement for mutual aid, cooperation or information exchange been established with other public or private entities in the area of cyberresilience?
Correlation	ISO/IEC 27001:2022 [A.5.1], [A.5.5], [A.5.6] NIST SP 800-53 R5 [PM-07-00], [AT-05-00], [PM-15-00] ENS [org.1] Minimum content guide PSO (2.2.4) NIS Transposition (Art.4, 5 y 9)
CHARACTERIZATION	
Scale	**L0 -** No mutual aid, cooperation or information exchange agreement has been established with public or private entities. **L1** - The establishment of mutual aid, cooperation or mutual information exchange agreements with public or private entities has begun. **L2** - Agreements have been established with public or private entities, but they are not formal (they have not been documented or approved by the management). **L3** - The agreements established with public or private entities have been documented, have been approved by the management and are kept up to date. **L4** - Formally established agreements are managed, updated and verified. **L5** - Improvement actions are applied in formally established agreements with public or private entities.
OBTAINING	
Collection method	Manual

Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has established and regularly updates agreements for mutual aid, collaboration or the exchange of cyberresistance information with private or public entities, to guarantee the collaboration or support of external entities, if necessary, in the event of a cyberattack that may lead to the unavailability of essential services. This exchange of information improves anticipation in incident management, vulnerability management, and essential service continuity.
	Corrective actions	Establish, formalize and review mutual aid, cooperation or information exchange agreements with private or public entities, to guarantee mutual collaboration in the event of a cyberattack.

Table 3 - Metric A-PC-OE5-01: Collaborate with public or private entities on cyberresilience.

2.1.2. Risk Management (RM)

The overall objective of this functional domain is to identify, document, and manage the risks of assets throughout their life cycle, to ensure the sustained productivity of essential services.

Its specific objectives are:

- Identify, document and manage assets throughout their life cycle, to ensure the sustained productivity of essential services.
- Establish, implement and maintain a formal and documented impact analysis (BIA) process.
- Develop a strategy to identify, analyse and mitigate risks.
- Identify risks and risk tolerance levels.
- Analyse the risks and assign them a treatment mechanism.
- Control risks on assets and services.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**A-GR-OE1-03**
Goal	ANTICIPATE
Functional domain	RISK MANAGEMENT
Indicator objective	Establish, implement and maintain a formal and documented impact analysis (BIA) process on the processes and activities that support the essential service.
Description	Identify the impact of the interruption or alteration of the provision of the essential service in your processes and activities, evaluating which of them are more critical. It is about knowing if an impact analysis (BIA) is carried out on the essential service, which analyses the consequences of a provision interruption or alteration, in order to identify which are the critical processes and activities that support this service to prioritize your recovery. It must be ensured that the treatment of risks is prioritized according to their criticality for the organization or for the society (people affected and their economic, environmental, public and social impact).
Question asked	Has the impact of the interruption or alteration of the essential service on the processes and activities that support it been identified? And, have you assessed which of these processes and activities are most critical based on this impact?
Correlation	ISO/IEC 31000:2018 NIST SP 800-53 R5 [RA-02-00], [RA-03-00], [PM-09-00], [PM-11-00], [RA-09-00]

	ENS [op.pl.1] Minimum content guide PSO (4.1, 4.4) Minimum content guide PPE (4.2, 4.3) NIS Transposition (Art.6)	
CHARACTERIZATION		
Scale	**L0** - The impact analysis on the essential service of the interruption or alteration of the processes and activities that support it has not been started. **L1** - The analysis of the impact on the essential service of the interruption or alteration of the processes and activities that support it has begun. **L2** - The analysis of the impact on the provision of the essential service of the interruption or alteration of the processes and activities that support it has been established, evaluating which of them are more critical, but it has not been documented. **L3** - The impact analysis on the essential service of the interruption or alteration of the processes and activities that support it has been documented and is kept up to date. **L4** - The analysis of the impact on the essential service of the interruption or alteration of the processes and activities that support it is managed, updated and verified. **L5** - Improvement actions are applied in the impact analysis in the essential service of the interruption or alteration of the processes and activities that support it.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has identified and prioritized the possible impacts of the interruption or alteration of the processes and activities that support the essential service, that is, it has implemented an impact analysis (BIA) for this service.
	Corrective actions	• Identify the possible impact that an interruption of the different processes and activities that support essential services would cause. • Categorize these impacts to prioritize their treatment.

Table 4 - Metric A-GR-OE1-03: Establish, implement and maintain a formal and documented impact analysis (BIA) process on the processes and activities that support the essential service.

CAMPO	INFORMACIÓN
ID	
Code	**A-GR-OE1-04**
Goal	ANTICIPATE
Functional domain	RISK MANAGEMENT
Indicator objective	Estimate the Maximum Tolerable Time to Fall (BAT) or time that an essential service may be down before unacceptable effects occur.
Description	This is a business parameter that indicates the maximum duration of an interruption or alteration in the provision of the essential service that is considered tolerable. This data is generally subjective but can be supported by quantitative indicators of business impact (unserved customers, decreased sales...) of the interruption. Internal procedures, guidelines and reference standards or qualitative factors based on intuition can be used as estimation criteria for these values.
Question asked	Has the maximum acceptable duration of an essential service interruption or alteration been estimated?
Correlation	ISO/IEC 31000:2018 NIST SP 800-53 R5 [RA-02-00], [RA-03-00], [PM-09-00], [PM-11-00], [RA-09-00] ENS [op.pl.1], [op.cont.1]* Minimum content guide PPE (4.2) NIS Transposition (Art.6)
CHARACTERIZATION	
Scale	**L0 -** The maximum duration of an interruption or alteration in the provision of essential service that is considered tolerable has not been estimated. **L1** - The estimation of the maximum duration of an interruption or alteration of the provision of the essential service that is considered tolerable has begun. **L2** - How to estimate the maximum duration of an interruption or alteration in the provision of essential service that is considered tolerable has been determined, but it has not been documented. **L3** - The procedure for estimating the maximum duration of an interruption or alteration in the provision of essential services that is considered tolerable and is kept up-to-date has been documented.

	L4 - The procedure for estimating the maximum duration of an interruption or alteration in the provision of the essential service that is considered tolerable is managed, updated and verified. **L5** - Improvement actions are applied in the procedure to estimate the maximum duration of an interruption or alteration in the provision of the essential service that is considered tolerable.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has estimated the maximum tolerable period of an interruption for essential service. This estimate is based on objective criteria and is periodically reviewed.
	Corrective actions	• Establish criteria and procedures to estimate the maximum tolerable interruption periods for each process and activity that supports the essential service for which we are conducting the survey. • Document, review and manage the procedure to estimate maximum tolerable interruption time for essential service.

Table 5 - Metric A-GR-OE1-04: Estimate the Maximum Tolerable Time to Fall (BAT) or time that an essential service may be down before unacceptable effects occur.

CAMPO	INFORMACIÓN
ID	
Code	**A-GR-OG1-03**
Goal	ANTICIPATE
Functional domain	RISK MANAGEMENT
Indicator objective	There is a specific procedure to implement risk management activities.
Description	Risk management is one of the pillars to know in detail the essential service and its internal functioning, as well as the consequences for the organization of an eventual interruption. The risk management procedure should treat the following elements: • Asset inventory. • Set of threats each asset is exposed to. • Set of vulnerabilities associated to each asset. • Set of security measures implemented. With this information, we are in a position to calculate the risk. For each asset-threat pair, we will estimate the probability that the threat will materialize and the business impact this would produce. The risk calculation can be performed using both quantitative and qualitative criteria and allows prioritizing on which risks the corresponding controls will be applied.
Question asked	Have procedures been established to manage the risk associated to the essential service?
Correlation	ISO/IEC 27005:2022 ISO/IEC 31000:2018 NIST SP 800-53 R5 [RA-02-00], [RA-03-00], [PM-09-00], [PM-11-00], [RA-09-00] ENS [op.pl.1] Minimum content guide PPE (4.2) NIS Transposition (Art.6)
CHARACTERIZATION	

Scale	**L0 -** Risk management related to the provision of the essential service is not carried out. **L1 -** Risk management related to the provision of the essential service has been started. **L2 -** Risk management related to the provision of essential services has been established but has not been documented. **L3 -** Risk management related to the provision of the essential service has been documented and is kept up to date. **L4 -** Risk management related to the provision of the essential service is managed, updated and verified. **L5 -** Improvement actions are applied in risk management related to the provision of the essential service.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization manages the risk related to the provision of the essential service as a process of continuous improvement.
	Corrective actions	Establish a risk management procedure related to the provision of the essential service based on references such as CCN-STIC 882 of Risk Analysis for Local Entities, or the Light Risk Analysis Model of Cybersecurity in Industrial Control Systems (ARLI-CIB) by INCIBE-CERT

Table 6 - Metric A-GR-OG1-03: Establish, implement and maintain a specific procedure for implementing risk management activities.

CAMPO	INFORMACIÓN
ID	
Code	**A-GR-OE5-03**
Goal	ANTICIPATE
Functional domain	RISK MANAGEMENT
Indicator objective	Establish and implement an essential service risk mitigation plan.
Description	It is important to understand that the goal of risk mitigation is to reduce the risk exposure of the essential service with the intention of taking it to the limits of the acceptable thresholds defined in each organization. It is about documenting the short, medium and long-term security controls, actions or initiatives that need to be implemented in order to mitigate the risks the essential service is exposed to. If the essential service belongs to the OT scope, it is about taking into account the thresholds for the risks on assets related to the OT infrastructures, for example the controls to face the difficulty of modifying default configurations or the lack of encryption and other Residual inherent risk of SCADA systems.
Question asked	Has an essential service risk mitigation plan been established and implemented?
Correlation	ISO/IEC 31000:2018 NIST SP 800-53 R5 [RA-02-00], [RA-03-00], [PM-09-00], [PM-11-00], [RA-09-00] ENS [op.pl.1] Minimum content guide PSO (4.1, 4.4) NIS Transposition (Art.6)
CHARACTERIZATION	
Scale	**L0 -** An essential service risk mitigation plan has not been established or implemented. **L1** - The establishment and implementation of an essential service risk mitigation plan has begun. **L2** - An essential service risk mitigation plan has been established and implemented, but it has not been documented. **L3** - The establishment and implementation of an essential service risk mitigation plan has been documented. This information is kept up to date. **L4** - The establishment and implementation of an essential service risk mitigation plan is managed, updated and verified. **L5** - Improvement actions are applied in the establishment and implementation of a risk mitigation plan for the essential service.

OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has defined and implemented the essential service risk mitigation plan to prevent the risk from exceeding its tolerance threshold.
	Corrective actions	• Establish and implement an essential service risk mitigation plan. • Document, manage and update risk tolerance thresholds for the essential service for which we are conducting the survey.

Table 7 - Metric A-GR-OE5-03: Establish and implement an essential service risk mitigation plan.

CAMPO	INFORMACIÓN
ID	
Code	**A-GR-OE6-01**
Goal	ANTICIPATE
Functional domain	RISK MANAGEMENT
Indicator objective	Prepare, document and maintain an inventory of the assets that support the essential service.
Description	The asset inventory is the first element of the chain in a security management system. An asset inventory includes: • the people who operate and monitor the services; • the information that is fed and produced by the services; • the technology that supports the services; • the facilities in which the services are carried out. In short, all those elements that have value for the organization and the provision of its essential service, and therefore need to be protected from potential risks. Location, process or processes in which it intervenes, cost of its replacement and responsible will be recorded for each asset. The purpose of this inventory is to identify the threats to these assets and their vulnerabilities, in order to analyse and manage the risks that could be derived for the essential service they support.

Question asked	Is an inventory of assets directly supporting the essential service developed, documented and maintained?	
Correlation	ISO/IEC 27001:2022 [A.5.9] NIST SP 800-53 R5 [CM-08-00] ENS [op.exp.1] Minimum content guide PSO (3.2 y 4.2) Minimum content guide PPE (3.2)	
CHARACTERIZATION		
Scale	**L0** - The assets inventory that support the essential service is not carried out. **L1** - The assets inventory that support the essential service has begun, but it is incomplete. **L2** - The assets inventory that support the essential service has been prepared, but the process is not documented. **L3** - The process for inventorying the assets that support the essential service has been developed and documented. **L4** - The assets inventory that support the essential service is periodically reviewed. **L5** - Improvement actions are applied to the process to inventory the assets that support the essential service.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has prepared, documented and maintains an inventory of the critical assets for the provision of the essential service.
	Corrective actions	Prepare, document and periodically review an asset inventory process that allows the information on the assets that support the essential service to be updated, among others: name, description, identifier, code, type, owner, responsible, location and valuation of the asset.

Table 8 - Metric A-GR-OE6-01: Prepare, document and maintain an inventory of the assets that support the essential service.

CAMPO	INFORMACIÓN
ID	
Code	**A-GR-OE6-02**
Goal	ANTICIPATE
Functional domain	RISK MANAGEMENT
Indicator objective	Back up and preserve the most sensitive classification information assets.
Description	A backup is a copy of the original data that is made in order to have a means of recovering it in case of loss. Backups are useful in different events and uses: recovering computer systems and data from a disaster; restoring data that may have been accidentally deleted, corrupted, infected by a computer virus or other causes; saving historical information, etc. Allowing relocation to locations other than that of the original data. Periodic checks to ensure that the process of restoring these copies is carried out correctly are essential to prevent failures in data restoration, for example.
Question asked	Is a procedure followed to periodically check that the restoration of backups is performed correctly?
Correlation	ISO/IEC 27001:2022 [A.8.13] NIST SP 800-53 R5 [CP-09-00] ENS [mp.info.6] [mp.per.4], [mp.info.1]*, [mp.info.2] Minimum content guide PPE (4.2.2)
CHARACTERIZATION	
Scale	**L0** - No procedure is followed to check the correct restoration of backups on a regular basis. **L1** - A procedure for verifying the correct restoration of backups on a periodic basis has been initiated. **L2** - A procedure for verifying the correct restoration of backups on a periodic basis has been implemented, but has not been documented. **L3** - A procedure for verifying the correct restoration of backups on a periodic basis has been implemented and documented. **L4** - The procedure for checking the correct restoration of backups on a periodic basis and the procedures for their preservation are periodically reviewed. **L5** - Improvement actions are implemented on the process for checking the correct restoration of backups on a regular basis and the procedures for their preservation.

OBTAINING		
Collection method	Manual A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values trending towards L5 indicate that there is an improved process for checking the periodicity of backup restoration.
	Corrective actions	• In the case of delegating backup to third-party cloud systems, ensure that they comply with the organization's security policies for sensitive classified information, e.g. encryption of information and access control. • Document processes, including where backups are stored. • Review retention procedures to adapt them to the different copy media according to their characteristics and those of the copies they house. • Periodically check that the procedure for retrieving copies of information is useful and effective..

Table 9 - Metric A-GR-OE6-02: Periodically check that the restoration of backups is carried out correctly.

2.1.3. Cybersecurity Training (CT)

The overall objective of this functional domain is to promote the knowledge and development of skills and knowledge of people in support of their roles in achieving and maintaining operational cyberresilience and protection. Its specific objectives are:

- Establish training programs in Cybersecurity.
- Carry out training activities.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**A-FO-OG1-03**
Goal	ANTICIPATE
Functional domain	CYBERSECURITY TRAINING
Indicator objective	Define and implement a specific procedure to implement the training activities.
Description	Define and implement a cyberresilience training plan for personnel involved in essential service. It is about knowing if knowledge and skill development is promoted among users related, directly or indirectly, to the provision of essential services, in support of their functions for the achievement and maintenance of cyberresilience. The training plan may contemplate any training initiative or training in cyberresilience, aimed at these users, including their participation in cyber exercises.
Question asked	Has a cyberresilience training plan for staff involved in essential service been defined and implemented?
Correlation	ISO/IEC 27001:2022 [A.6.3] NIST SP 800-53 R5 [AT-01-00], [AT-03-00], [PM-13-00], [PM-14-00] ENS [mp.per.4] Minimum content guide PSO (2.2.2) NIS Transposition (Art.6, 7)
CHARACTERIZATION	

Scale	**L0 -** A cyberresilience training plan has not been established. **L1** - The definition of a training plan has begun. **L2** - A training plan has been established, but it has not been documented. **L3** - A training plan and associated activities have been documented. This plan is kept up to date. **L4** - The training plan and associated activities are managed and verified. **L5** - Improvement actions are applied in the training plan and in the associated activities.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization carries out training activities or cyber exercises aimed at educating and training the organization's personnel in cyberresilience. The training plan should be directed at the organization's employees and, where relevant, third-party contractors and users.

	Corrective actions	• Plan, dedicate resources, inform staff and carry out training activities in cyberresilience or cyber exercises aimed at training the organization's staff in this area. • Identify the needs and gaps in the capacities of the personnel responsible for cybersecurity • Evaluate the number of users (internal and external) who have successfully completed the periodic training sessions according to what is established in the plan. • Evaluate the effectiveness of training plans. • These plans are periodically updated to adapt them to changes in the workforce or processes, when new equipment and technologies are incorporated, and to keep abreast of the evolution of threats.

Table 10 - Metric A-FO-OG1-03: Define and implement a specific procedure to implement the training activities.

CAMPO	INFORMACIÓN
ID	
Code	**A-FO-OE1-02**
Goal	ANTICIPATE
Functional domain	CYBERSECURITY TRAINING
Indicator objective	Identify Cybersecurity training needs for essential services.
Description	In order to determine the organization Cybersecurity training needs, an analysis must assess the activities of the employees (risks to which they are exposed, competencies that need to be developed in their day-to-day activities, certifications or regulations that must be achieved or maintained to ensure the proper functioning of the essential service) and integrate them into corporate training plans.
Question asked	Have Cybersecurity training needs for essential services been identified?
Correlation	ISO/IEC 27001:2022 [A.6.3] NIST SP 800-53 R5 [AT-01-00], [AT-03-00], [PM-13-00], [PM-14-00] ENS [mp.per.4]

	Minimum content guide PSO (2.2.2) NIS Transposition (Art.6, 7)	
CHARACTERIZATION		
Scale	**L0** -Cybersecurity training needs for essential services have not been identified. **L1** - Cybersecurity training needs for essential services have been identified. **L2** - Cybersecurity training needs for essential services have been identified, but they have not been documented. **L3** - Cybersecurity training needs for essential services have been documented. And they are kept up to date. **L4** - Cybersecurity training needs are managed and verified for essential services. **L5** - Improvement actions are applied in the identification of Cybersecurity training needs for essential services.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has identified Cybersecurity training needs for essential services and maintains them in a cycle of constant improvement.
	Corrective actions	• Allocate time and dedicate resources to identify the organization's Cybersecurity training needs. • Periodically update cybersecurity training needs to adapt them to the level of security required, new threats and the different professional profiles of the company.

Table 11 - Metric A-FO-OE1-02: Identify Cybersecurity training needs for essential services.

CAMPO	INFORMACIÓN
ID	
Code	**A-FO-OE3-01**
Goal	ANTICIPATE
Functional domain	CYBERSECURITY TRAINING
Indicator objective	Carry out cyberresilience awareness activities.
Description	Define and implement a cyberresilience awareness plan. It is about knowing if a culture of cyberresilience is promoted within the organization to reach all staff. This plan incorporates any initiative to raise awareness on cyberresilience.
Question asked	Has a cyberresilience awareness plan for all staff involved in essential service been defined and implemented?
Correlation	ISO/IEC 27001:2022 [A.6.3] NIST SP 800-53 R5 [AT-01-00], [PM-16-00], [AT-02-00], [PM-15-00] ENS [mp.per.3] Minimum content guide PSO (2.2.2) NIS Transposition (Art.6, 7)
CHARACTERIZATION	
Scale	**L0** - A cyberresilience awareness plan has not been established. **L1** - The definition of an awareness plan has been started. **L2** - An awareness plan has been established, but it has not been documented. **L3** - An awareness plan and associated activities have been documented. This plan is kept up to date. **L4** - The awareness plan and associated awareness activities are managed and verified. **L5** - Improvement actions are applied in the awareness plan and associated awareness activities.
OBTAINING	
Collection method	Manual
Responsible	CSO o CISO
ANALYSIS	
Objective Measure	L5

Indicator	**Positive values**	Values tending to L5 indicate that the organization carries out awareness-raising activities aimed at sensitizing the organization's staff to cyberresilience.
	Corrective actions	• Incorporate the awareness plan as part of the company's security strategy. • Allocate time and dedicate resources to inform all personnel of the security risks that they can avoid and the processes that must be activated in the event of an incident. Carry out cyberresilience awareness activities aimed at sensitizing the organization's staff in this matter. • Periodically update these plans to adapt them to the necessary security level, new threats and the different professional profiles of the company.

Table 12 - Metric A-FO-OE3-01: Carry out cyberresilience awareness activities.

2.2. Resist

The tabs for the metrics corresponding to the Resist goal are detailed below.

2.2.1. Vulnerability Management (VM)

The general objective of this functional domain is to identify, analyse and manage vulnerabilities in the operating environment of an essential service. Its specific objectives are:

- To prepare to carry out vulnerability analysis and resolution activities.
- To establish and maintain a vulnerability identification and analysis process.
- To manage exposure to identified vulnerabilities.
- To analyse the root causes of vulnerabilities.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OG1-03**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Prepare, implement and maintain a specific procedure for vulnerability management.
Description	Vulnerability management is a continuous process of any information system that consists of identifying, evaluating and correcting vulnerabilities in any system in the organization, be it *software or hardware* that support the provision of essential

	service. It goes beyond vulnerability assessment, as it categorizes assets and classifies vulnerabilities according to their level of risk. If the essential service belongs to an OT environment, it is about managing those vulnerabilities that may affect the components that comprise it (PLC, RTU, HMI, SCADA, Controller, etc.).	
Question asked	Has a specific procedure for vulnerability management been developed, implemented and is maintained within the organization?	
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [CA-08-00], [RA-05-00], [SA-11-00], [SI-02-00], [SI-03-00] ENS [op.pl.1] [mp.sw.2], [op.exp.3], Article 8*, 21	
CHARACTERIZATION		
Scale	**L0** - There is no specific procedure for vulnerability management. **L1** - The definition of a specific procedure for vulnerability management has been started, but it is incomplete and has not been formalized. **L2** - A specific procedure for vulnerability management has been established, is complete but is not updated. **L3** - A specific procedure for vulnerability management has been documented. This procedure is kept up to date. **L4** - The specific procedure for vulnerability management is managed and verified. **L5** - Improvement actions are applied in the specific procedure for vulnerability management.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values close to L5 indicate that the organization is actively reviewing the specific procedure to implement vulnerability management.

	Corrective actions	• Identify and establish a list of sources of information about vulnerabilities for assets: manufacturers, CERTs, distribution lists, newsgroups, among them. • Establish in the procedure a section for the active discovery of vulnerabilities, their prioritization and evaluation of the impact on assets. • Incorporate vulnerability analysis and resolution activities into the procedure. • Establish those responsible for the vulnerability management procedure.

Table 13 - Metric T-GV-OG1-03: Prepare, implement and maintain a specific procedure for vulnerability management.

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OE1-02**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Use tools or mechanisms to identify vulnerabilities in assets.
Description	Vulnerability identification tools or mechanisms are applications designed to perform assisted or automatic analysis of the organization technological assets. Although these applications may not be able to detect the vulnerability with complete precision, they are capable of detecting certain elements that could trigger a vulnerability, making it easier for researchers and engineers. It is about proactively discovering, using these tools, the vulnerabilities that affect the provision of essential services, and whether they are used regularly.
Question asked	Are tools or mechanisms to identify vulnerabilities in assets used?
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [CA-08-00], [RA-05-00], [SA-11-00], [SI-02-00], [SI-03-00] ENS [op.pl.1] [mp.sw.2]
CHARACTERIZATION	

Scale	**L0** - No tools or mechanisms to identify vulnerabilities in assets are used. **L1** - The use of vulnerability identification tools or mechanisms has been started in the assets. **L2** - A procedure has been established for the use of vulnerability identification tools or mechanisms in assets. **L3** - The procedure has been documented and tools or mechanisms to identify vulnerabilities in assets are used. **L4** - The procedure for using tools or mechanisms to identify vulnerabilities in assets is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for using tools or mechanisms to identify vulnerabilities in assets.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values close to L5 indicate that the organization is actively reviewing vulnerabilities that affect the essential service, through the use of a known set of tools or mechanisms to identify vulnerabilities in assets.
	Corrective actions	• Identify and establish a list of vulnerability analysis tools. • Document and review a list of the vulnerability scanning tools used.

Table 14 - Metric T-GV-OE1-02: Use tools or mechanisms to identify vulnerabilities in assets.

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OE2-04**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Categorize and prioritize vulnerabilities.
Description	Vulnerability categorization is probably the most important step in a vulnerability management process and also the most difficult and risky step. During this stage, the different vulnerabilities identified must be classified, determining the probability of exploitation and the consequences that they could generate. This makes it easier to prioritize your remediation. It is convenient for clarity to apply well-known criteria, such as CVE.
Question asked	Are the vulnerabilities that affect the provision of the essential service for their management categorized and prioritized?
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [RA-02-00], [SA-10-00], [SA-11-00], [SI-02-00] ENS [op.pl.1] [mp.sw.2], [op.exp.3], Article 8*, 21 Minimum content guide PSO (2.1)
CHARACTERIZATION	
Scale	**L0** - Vulnerabilities are not categorized or prioritized. **L1** - The categorization and prioritization of vulnerabilities has begun. **L2** - A procedure has been established for the categorization and prioritization of vulnerabilities, but it is not documented. **L3** - The vulnerability categorization and prioritization procedure has been documented and is kept up to date. **L4** - The categorization and prioritization of vulnerabilities is managed, updated and verified. **L5** - Actions to improve vulnerability categorization and prioritization are applied.
OBTAINING	
Collection method	Manual. A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.
Responsible	CSO o CISO

ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the vulnerabilities are categorized, and their remediation is regularly prioritized.
	Corrective actions	• Categorize and prioritize vulnerabilities to report them to those responsible. • Document and update a vulnerability categorization and prioritization procedure.

Table 15 - Metric T-GV-OE2-04: Categorize and prioritize vulnerabilities.

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OE2-06**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Establish and maintain an updated vulnerability repository.
Description	Maintain an updated repository of those vulnerabilities that affect the provision of essential services. That repository must contain updated information on the life cycle of vulnerabilities, with specific information on each of them, including the measures required to tackle them.
Question asked	Is an updated repository of vulnerabilities affecting the provision of essential service established and maintained?
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [RA-05-00], [SA-10-00], [SA-11-00], [SC-38]-00, [SI-02-00], [SI-03-00] Minimum content guide PPE (4.4.2) ENS [op.pl.1] [mp.sw.2]
CHARACTERIZATION	

Scale	**L0** - A vulnerability repository with information about vulnerabilities has not been established. **L1** - The development of a repository of vulnerabilities with information about them and their resolution has begun. **L2** - A repository of vulnerabilities has been established with information about them and their resolution. **L3** - A repository of vulnerabilities has been documented with information about them and their resolution. **L4** - A vulnerability repository is managed, updated and verified with information about vulnerabilities and their resolution. **L5** - Improvement actions are applied in the vulnerability repository with information about them and their resolution.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization maintains an updated repository of all known vulnerabilities, storing information about them and their resolution.
	Corrective actions	Establish a repository of vulnerabilities with information on their life cycle. Such repository must contain basic information such as: • Unique identifier for internal reference of the vulnerability in the organization. • Description of the vulnerability. • Date of entry into the repository. • References to the source of the vulnerability. • Importance of vulnerability to the organization (critical, moderate, etc.) • People or teams assigned to analyse and solve it. • Record of resolution actions taken to decrease or eliminate vulnerability.

Table 16 - Metric T-GV-OE2-06: Establish and maintain an updated vulnerability repository.

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OE3-01**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Develop and maintain a procedure for managing patches and updating technological assets.
Description	Updates, whether security or functionality, to computer systems should be guided by a patch management process that adequately identifies the life cycle and indicates its periodicity. In the TO environment, patch management in industrial systems should also address the possibility that certain manufacturers may not have a recurring patch release implemented to address security issues. This can lead to determining other measures to protect industrial assets (isolation or active monitoring of the environment).
Question asked	Has a procedure for managing patches and updating technology assets been developed and maintained?
Correlation	ISO/IEC 27001:2022 [A.7.13], [A.8.8], [A.8.32] NIST SP 800-53 R5 [CM-08-00], [SI-02-00], [SI-03-00] [SI-08-00] ENS [op.exp.4] [op.exp.5] Minimum content guide PPE (4.4.2) NIS Transposition (Art.6)
CHARACTERIZATION	
Scale	**L0** - No procedure has been developed for the management of patches and updating of technological assets. **L1** - The definition of a procedure for managing patches and updating technology assets has been started, but it is incomplete and has not been formalized. **L2** - A procedure for managing patches and updating technology assets has been established, is complete but is not updated. **L3** - A procedure for managing patches and updating technology assets has been documented. This plan is kept up to date. **L4** - The procedure for managing patches and updating technological assets is managed and verified. **L5** - Improvement actions are applied in the procedure for managing patches and updating technological assets.
OBTAINING	
Collection method	Manual

Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization includes in its processes the management of patches and updating of technological assets. As a result of this procedure, the impact of applying or not an update on a certain system can be objectively assessed.
	Corrective actions	Establish a procedure for managing patches and updating technological assets, which may include activities: • Identification of assets and base *software* as well as the level of patches of each one in the inventory. • Availability: review the current patch list and identify which one affects each asset in the process. • Applicability: check if the specific update is suitable for the assets of our process. • Acquisition: obtain the update files from a reliable source as well as check the veracity of the patch. • Validation: ensuring that the update does not adversely impact the process. • Deployment: During the validation process, a deployment package has to be created for the entire infrastructure.

Table 17 - Metric T-GV-OE3-01: Develop and maintain a procedure for managing patches and updating technological assets.

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OE3-04**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Monitor the status of those unresolved vulnerabilities that affect the provision of essential service.
Description	There are multiple reasons why a vulnerability may not be corrected: forgetfulness, lack of patch, affect non-critical systems or non-critical priority. This indicator tries to find out if periodic monitoring is performed and if vulnerabilities that have not been resolved are reported. For example, you can measure the time between vulnerability detection and when it is definitively resolved.
Question asked	Is the status of unresolved vulnerabilities that affect the provision of essential service monitored?
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [RA-05-00], [SA-10-00], [SA-11-00], [SI-02-00], [SI-03-00] ENS [op.pl.1] [mp.sw.2], [op.exp.3] Minimum content guide PSO (1.4) Minimum content guide PPE (1.4, 2.4) NIS Transposition (Art.8, 10, 11, 12)
CHARACTERIZATION	
Scale	**L0** - The status of unresolved vulnerabilities is not monitored. **L1** - Monitoring of unresolved vulnerabilities has started. **L2** - A procedure for monitoring unsolved vulnerabilities has been established but is not documented. **L3** - The procedure for monitoring unresolved vulnerabilities has been documented and is kept up to date. **L4** - The procedure for monitoring unresolved vulnerabilities is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for monitoring unresolved vulnerabilities.
OBTAINING	
Collection method	Manual. A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.
Responsible	CSO o CISO

ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that unresolved vulnerabilities are regularly monitored and reported.
	Corrective actions	• Monitor unsolved vulnerabilities and report them to those responsible. Measure the time it takes to report and resolve vulnerabilities. • Document and update a procedure for unresolved vulnerabilities.

Table 18 - Metric T-GV-OE3-04: Monitor the status of those unresolved vulnerabilities that affect the provision of essential service.

CAMPO	INFORMACIÓN
ID	
Code	**T-GV-OE4-01**
Goal	RESIST
Functional domain	VULNERABILITY MANAGEMENT
Indicator objective	Identify and analyse the root causes of vulnerabilities.
Description	Not all vulnerabilities are failures reported by the manufacturer, many are due to bad configurations or unsuccessful installations (network architecture for example) and others also due to their administration and use. The latter would indicate lack of training or specific policies for the installation and maintenance of this equipment or infrastructure. Determining the source of vulnerabilities can be very helpful in improving the protection of systems that assist in the provision of essential service. This involves developing procedures that trace the root cause of the vulnerability on those most critical systems. In this case, measures will have to be applied to carry out an adequate audit.
Question asked	Are the causes of vulnerabilities investigated and analysed?
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [RA-05-00], [SA-10-00], [SA-11-00], [SI-02-00], [SI-03-00], [IR-06-00] ENS [op.pl.1] [mp.sw.2], [op.exp.3] NIS Transposition (Annex 2)
CHARACTERIZATION	

Scale	**L0** - It is not considered to define any procedure to investigate the origin of the vulnerabilities. **L1** - The procedure to investigate the origin of the vulnerabilities has been started. **L2** - A procedure has been established to investigate the origin of the vulnerabilities, but it has not been documented. **L3** - The procedure to investigate the origin of vulnerabilities is documented and updated. **L4** - The procedure to investigate the origin of vulnerabilities is managed, updated and verified. **L5** - Improvement actions are applied in the procedure to investigate the origin of the vulnerabilities.	
OBTAINING		
Collection method	Manual A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that there is an improved process to investigate the origin of vulnerabilities
	Corrective actions	• Establish a procedure to investigate the origin of vulnerabilities on the most critical systems. • In the case of vulnerabilities linked to faulty configurations, it is proposed to resolve the lack of training or specific policies for the installation and maintenance of this equipment or infrastructure.

Table 19 - Metric T-GV-OE4-01: Identify and analyse the root causes of vulnerabilities.

2.2.2. Continuous Supervision (CS)

The overall goal of this functional domain is to collect, collect, and distribute information about the behaviour and activities of systems and people to support the ongoing process of identifying and analyzing risks to the organization's assets and essential services that may affect negatively to the operation and provision of the same. Its specific objectives are:

- Monitor the organization's communication networks.
- Monitor the physical environment of the organization.
- Monitor the activity of the organization's staff.
- Monitor the activity of service providers external to the organization.
- Monitor unauthorized access to the organization.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**T-SC-OG1-03**
Goal	RESIST
Functional domain	CONTINUOUS SUPERVISION
Indicator objective	Establish and maintain a specific continuous monitoring procedure.
Description	It is about knowing if there is continuous monitoring (24x7) or if there is a continuous monitoring strategy for the provision of the essential service to detect potential cyberincidents.
Question asked	Is the provision of the essential service permanently monitored (24x7) to detect potential cyberincidents?
Correlation	ISO/IEC 27001:2022 [A.8.6] NIST SP 800-53 R5 [RA-05-00], [CA-07-00], [PM-06-00], [SI-04-00] ENS [op.mon] Minimum content guide PSO (2.2.3) Minimum content guide PPE (4.2.2)
CHARACTERIZATION	

Scale	**L0** - 24x7 monitoring of essential service provision is not performed. **L1** - 24x7 monitoring of essential service provision has started. **L2** - A 24x7 monitoring procedure for essential service provision has been established, but it has not been documented. **L3** - A 24x7 monitoring procedure for essential service provision has been documented and is kept up to date. **L4** - The procedure for 24x7 monitoring of essential service provision is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for 24x7 monitoring of essential service provision.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO o Physical Security Director	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization monitors (24x7) the essential service to detect potential cyberattacks.
	Corrective actions	• Establish a continuous monitoring procedure on the assets and processes that support essential services (communication networks, systems, accesses, physical environment, personnel activity, external service providers, etc.) to detect potential cyberattacks. • Identify those responsible for continuous monitoring and define their responsibilities.

Table 20 - Metric T-SC-OG1-03: Establish and maintain a specific continuous monitoring procedure.

CAMPO	INFORMACIÓN
ID	
Code	**T-SC-OE1-01**
Goal	RESIST
Functional domain	CONTINUOUS SUPERVISION
Indicator objective	Monitor the organization's communication networks to detect potential Cybersecurity events.
Description	An information security event is an identified occurrence of the state of a communications system, service, or network that indicates a possible violation of the information security policy or failure of controls, or a previously unknown situation that may be relevant for security. Monitor the communication networks that support the essential service to detect security events, such as unauthorized *malware* connections that can compromise the organization assets (people, processes, technology or facilities). You can use an intrusion detection system or a firewall.
Question asked	Are the communications networks that support the essential service monitored for unauthorized connections?
Correlation	ISO/IEC 27001:2022 [A.8.6], [A.8.30] NIST SP 800-53 R5 [RA-05-00], [CA-07-00], [PM-06-00], [SI-04-00] ENS [op.mon] Minimum content guide PPE (4.2.2)
CHARACTERIZATION	
Scale	**L0** - Monitoring of communication networks to detect unauthorized connections is not performed. **L1** - Monitoring of communication networks has begun to detect unauthorized connections. **L2** - A communication network monitoring procedure has been established to detect unauthorized connections, but it has not been documented. **L3** - A communication network monitoring procedure to detect unauthorized connections has been documented and is kept up to date. **L4** - The procedure for monitoring communication networks to detect unauthorized connections is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for monitoring communication networks to detect unauthorized connections.
OBTAINING	

Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization monitors communications networks to detect unauthorized connections.
	Corrective actions	Document, update, verify and improve a procedure for continuous monitoring of cybersecurity events that are registered in communication networks.

Table 21 - Metric T-SC-OE1-01: Monitor the organization's communication networks to detect potential Cybersecurity events.

CAMPO	INFORMACIÓN
ID	
Code	**T-SC-OE1-02**
Goal	RESIST
Functional domain	CONTINUOUS SUPERVISION
Indicator objective	Monitor the existence of unauthorized *software and hardware* in systems that support essential services.
Description	The existence of unauthorized *software or hardware* in the organization is largely due to employees who do not respect the procedures for obtaining the technology through corporate channels or are unaware of the consequences. For example: the use of unauthorized USB, non-corporate file sharing platforms, or installation of pirated *software*. Overseeing the system that supports the essential service for unauthorized *software* or *hardware* is crucial to fight these practices. For example, periodic system scan tools can be used to support essential service.
Question asked	Is the system that supports the essential service monitored for unauthorized *software or hardware*?
Correlation	ISO/IEC 27001:2022 [A.8.6], [A.8.30] NIST SP 800-53 R5 [RA-05-00], [CA-07-00], [PM-06-00], [SI-04-00] ENS [op.mon]
CHARACTERIZATION	

Scale	**L0 -** System monitoring is not performed to detect unauthorized *software or hardware*. **L1** - System monitoring has started to detect unauthorized *software or hardware*. **L2** - A system monitoring procedure has been established to detect unauthorized *software or hardware*, but it has not been documented. **L3** - A system monitoring procedure to detect unauthorized *software or hardware* has been documented and is kept up to date. **L4** - The procedure for monitoring the system to detect unauthorized *software or hardware* is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for monitoring the system to detect unauthorized *software or hardware.*	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values for L5 indicate that the organization monitors the systems that support essential services for unauthorized *software or hardware.*
	Corrective actions	• Document, update, verify, and improve a continuous monitoring procedure on systems that support essential services for unauthorized *software or hardware*. • Establish policies on the permitted and non-permitted use of *software and hardware*; and communicate them to employees. • Select the tools used to detect the use of unauthorized *software or hardware*.

Table 22 - Metric T-SC-OE1-02: Monitor the existence of unauthorized software and hardware in systems that support essential services.

CAMPO	INFORMACIÓN
ID	
Code	**T-SC-OE4-01**
Goal	RESIST
Functional domain	CONTINUOUS SUPERVISION
Indicator objective	Establish and maintain a procedure agreed with external providers (in the ANS) to report potential cybersecurity events that affect the essential service.
Description	External specialized services, for example from consulting providers, technology (cloud or hosting, among others) can support the provision of the organization essential service. In this type of situation, it is useless to have a high level of security demand in the organization itself, if the same level is not required to external providers. It is necessary to establish clauses in the Service Level Agreement (SLA) and in the contracts that help us to set the agreed level of quality and safety, as well as to determine the monitoring and control mechanisms necessary to react quickly in case the service provided may be compromised by the presence of cybersecurity events.
Question asked	Is there an agreed procedure with external providers to report potential cybersecurity events that affect the essential service?
Correlation	ISO/IEC 27001:2022 [A.8.8] NIST SP 800-53 R5 [[SA-09-00] ENS [op.pl.1] [mp.sw.2], [op.exp.3] [op.exp.9] [mp.s.4] Minimum content guide PPE (3.2, 3,3) NIS Transposition (Art.6, 8, 15-4)
CHARACTERIZATION	

Scale	**L0** - No agreed procedure has been established with external providers to report potential cybersecurity events that affect the essential service. **L1** - The establishment of an agreed procedure has been started with external providers to report potential cybersecurity events that affect the essential service. **L2** - An agreed procedure has been established with external providers to report potential cybersecurity events that affect the essential service. **L3** - The procedure agreed with external providers to report potential cybersecurity events that affect the essential service has been documented. **L4** - The procedure agreed with external providers is managed, updated and verified so that they report potential cybersecurity events that affect the essential service. **L5** - Improvement actions are applied in the definition of the procedure agreed with the external providers so that they report potential cybersecurity events that affect the essential service.	
OBTAINING		
Collection method	Manual A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that there is an improved process for external providers to report potential cybersecurity events that affect the essential service.
	Corrective actions	• Identify, document and keep updated an agreed procedure for external providers to report potential cybersecurity events affecting the essential service. • Implement improvement actions to reduce reporting times for cybersecurity events from external providers.

Table 23 - Metric T-SC-OE4-01: Establish and maintain a procedure agreed with external providers (in the ANS) to report potential cybersecurity events that affect the essential service.

2.3. Recover

The tabs for the metrics corresponding to the Retrieve goal are detailed below.

2.3.1. Incident Management (IM)

The overall objective of this functional domain is to establish processes to identify and analyse events, detect incidents, and determine an organization response. An information security event is an identified occurrence of the state of a communications system, service, or network that indicates a possible violation of the information security policy or failure of controls, or a previously unknown situation that may be relevant for security. The specific objectives are:

- To establish a process to detect, report, prioritize, and analyse events.
- To identify and analyse cyberincidents
- To establish a process to respond to and recover from cyberincidents.
- To analyse the information of cyberincidents.
- Coordination with other organizations in the response to cyberincidents.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE1-01**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Establish a procedure to detect, report and report events.
Description	There should be a procedure for event detection and notification to staff in charge of incident management. It is a matter of knowing if events, that is, unexpected or unwanted facts (for example, unauthorized access attempts, high response times, increased volume of files) are identified, in the infrastructures that support the essential service and if they are notified to those who will proceed to their immediate or subsequent analysis. For example, indicate if there are tools or services with automatic detection mechanisms for real-time events.
Question asked	Is event detection and notification to incident management personnel carried out?
Correlation	ISO/IEC 27001:2022 [A.6.8], [A.5.25] NIST SP 800-53 R5 [IR-04-00] ENS [op.exp.7] Minimum content guide PPE (4.2.2) NIS Transposition (Art.9, 10, 11, 12)

CHARACTERIZATION		
Scale	**L0** - No event detection and notification is performed. **L1** - Event detection and notification has started. **L2** - An event detection and notification procedure has been established, but it has not been documented. **L3** - An event detection and notification procedure has been documented and is kept up to date. **L4** - The procedure for event detection and notification is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for the detection and notification of events.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has an updated procedure to capture and analyse events, so that it can determine if the event will become (or has become) a cyberincident that requires the organization's action and notify those responsible opportune to proceed with its analysis.
	Corrective actions	Establish an event reporting procedure to detect events and provide reports to incident management personnel and concerned officials. Influence users in the Awareness Plan on the need to communicate to those responsible, as soon as possible, any anomaly or security event detected, teaching them to recognize anomalous situations that may initiate an incident (malfunction, slow processes, behaviours outside than normal, ...).

Table 24 - Metric R-GI-OE1-01: Establish a procedure to detect, report and report events.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE1-07**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Establish a process to detect, report, prioritize and analyze events.
Description	With regard to the management of events and incidents, ensuring the collection of evidence related to such an event can be very useful to assess what caused it, as well as to carry out actions to improve internal detection and action processes. In this case it will be necessary to apply measures that help us to guarantee the correct collection of evidence, in accordance with current legislation.
Question asked	Is there a process in place to ensure evidence of events in accordance with current legislation?
Correlation	ISO/IEC 27001:2022 [A.5.27], [A.5.28] NIST SP 800-53 R5 [IR-04-00], [IR-05-00] ENS [op.exp.7] [op.exp.9] Guía contenidos mínimos PSO (2.2.1, 2.2.4) Guía contenidos mínimos PPE (2.1, 2.3, 4.2.1, 4.2.2)
CHARACTERIZATION	
Scale	**L0** - No procedure is followed to ensure evidence of events in accordance with current legislation. **L1** - Implementation of a process to ensure evidence of events in accordance with current legislation has been initiated. **L2** - A process to ensure evidence of events in accordance with current legislation has been implemented but not documented. **L3** - A process to ensure evidence of events in accordance with current legislation has been implemented and documented. **L4** - The process for ensuring evidence of events in accordance with current legislation is periodically reviewed. **L5** - Improvement actions are applied on the process to ensure evidence of events according to the legislation in force.
OBTAINING	
Collection method	Manual
Responsible	CSO o CISO

ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has a process to ensure the collection of evidence of events in accordance with current legislation.
	Corrective actions	Implement a procedure to ensure the collection of evidence related to events in accordance with current legislation. Document, review and update the evidence collection procedure.

Table 25 - Metric R-GI-OE1-07: Follow a process to ensure evidence of events in accordance with current legislation.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE2-01**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Establish and maintain a procedure to classify and assess cyberincidents.
Description	Having a procedure to classify and assess cyberincidents, based on a predefined typing of them, will allow, in addition to improving incident management, to demonstrate the organization regulatory compliance. For example, data such as detection date, notification date, resolution date and closing date must be recorded for cyberincidents. Incident reporting can be mandatory or optional and must follow homogeneous criteria as indicated in the National Incident Reporting and Management Guide (see References section of the Dictionary of Indicators).
Question asked	Is there a procedure for the classification and evaluation of cyberincidents, based on a predefined typing of them?
Correlation	ISO/IEC 27001:2022 [A.6.8], [A.5.25] NIST SP 800-53 R5 [IR-04-00] ENS [op.exp.7] Minimum content guide PPE (4.2.2) NIS Transposition (Annex 2)
CHARACTERIZATION	

Scale	**L0** - There is no procedure to classify and evaluate cyberincidents according to their typing. **L1** - The establishment of a procedure to classify and evaluate cyberincidents based on a defined typing has begun. **L2** - A procedure has been established to classify and evaluate cyberincidents based on their typing, but they have not been documented. **L3** - A procedure for classifying and evaluating cyberincidents based on their typing has been documented and is kept up to date. **L4** - The procedure for classifying and evaluating cyberincidents based on their classification is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for the classification and evaluation of cyberincidents based on their classification.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization classifies and evaluates cyberincidents according to an established process, using a defined incident classification, to obtain metrics to support regulatory compliance.
	Corrective actions	Establish a procedure for the classification and assessment of cyberincidents using a predefined typing, such as that proposed by the ICT Security Guide CCN-STIC 817 or The National Cyber Incident Notification and Management Guide (see References section).

Table 26 - Metric R-GI-OE2-01: Establish and maintain a procedure to classify and assess cyberincidents.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE2-02**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Document and transmit the criteria to identify and recognize cyberincidents.
Description	It is a matter of knowing if the criteria that facilitate the identification and recognition of a cyberincident for their reporting have been documented and transmitted to the members of the organization staff.
Question asked	Have criteria been established to identify and recognize cyberincidents, and are they accessible and known to all staff?
Correlation	ISO/IEC 27001:2022 [A.6.8], [A.5.25] NIST SP 800-53 R5 [IR-04-00] ENS [op.exp.7] Minimum content guide PPE (4.2.2) NIS Transposition (Annex 2)
CHARACTERIZATION	
Scale	**L0** - The criteria for the identification and recognition of cyberincidents have not been established. **L1** - The definition of the criteria for the identification and recognition of cyberincidents has begun. **L2** - Criteria for the identification and recognition of cyberincidents have been established, but they have not been documented or transmitted to all members of the organization. **L3** - The criteria for the identification and recognition of cyberincidents have been documented, have been transmitted to all members of the organization and are kept up to date. **L4** - The identification and recognition criteria for cyberincidents are managed, updated and verified. **L5** - Improvement actions are applied in the definition of the criteria for the identification and recognition of cyberincidents.
OBTAINING	
Collection method	Manual
Responsible	CSO o CISO
ANALYSIS	

Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has defined and documented the criteria for identification and recognition of cyberincidents and this information is available to all personnel who may need it.
	Corrective actions	Define and document the criteria for identification and recognition of cyberincidents and make this information available to all personnel.

Table 27 - Metric R-GI-OE2-02: Document and transmit the criteria to identify and recognize cyberincidents.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE2-03**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Analyse cyberincidents to determine an appropriate response.
Description	It is a question of knowing if an incident analysis procedure is followed to identify the actions necessary for its resolution, in the shortest possible time. For example, answering the following questions: • What happened? • Who does it affect (users / customers / suppliers)? • What should I tell them? • Who do I notify to? • Does it have legal or contractual repercussions? • Or do we have the affected services and systems under control?
Question asked	Are cyberincidents analysed to determine the most appropriate response in the shortest possible time?
Correlation	ISO/IEC 27001:2022 [A.6.8], [A.5.25] NIST SP 800-53 R5 [CA-02-00], [IR-04-00], [IR-05-00], [IR-06-00], [PE-06-00] ENS [op.exp.7] Minimum content guide PSO (2.2.3,4.1,4.4) Minimum content guide PPE (1.1,4.2, 4.4) NIS Transposition (Annex 2, 3, 4)

CHARACTERIZATION		
Scale	**L0** - A cyberincident analysis is not performed to determine the most appropriate response. **L1** - Cyber incident analysis has begun to determine the most appropriate response. **L2** - A cyberincident analysis procedure has been established to determine the most appropriate response, but it has not been documented. **L3** - A cyberincident analysis procedure has been documented and updated to determine the most appropriate response. **L4** - The cyberincident analysis procedure is managed, updated and verified to determine the most appropriate response. **L5** - Improvement actions are applied in the cyberincident analysis procedure to determine the most appropriate response.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has a standardized cyberincident analysis procedure to formulate a response in the shortest possible time.
	Corrective actions	Establish a cyberincident analysis procedure with which to correctly define the type of incident and prepare the most appropriate response in the shortest possible time. It should also help to determine if the incident has legal repercussions and to whom to report it. In the case of security breaches of personal data, the reference entity is the AEPD.

Table 28 - Metric R-GI-OE2-03: Analyse cyberincidents to determine an appropriate response.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE3-01**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Establish an incident response structure for escalation to those responsible for its resolution.
Description	Establish an organizational structure for responding to cyberincidents, as well as a formal protocol to escalate cyberincidents to those responsible. For example, indicate if there is documentation specifying who should be notified.
Question asked	Is there a cyberincident response structure that allows it to be escalated to those responsible for its resolution?
Correlation	ISO/IEC 27001:2022 [A.5.26] NIST SP 800-53 R5 [IR-04-00], [IR-09-00], [IR-08-00] ENS [op.exp.7] Minimum content guide PSO (1.5) NIS Transposition (Art.4, 8)
CHARACTERIZATION	
Scale	**L0** - There is no cyberincident response structure. **L1** - The definition of a cyberincident response structure has been started. **L2** - A cyberincident response structure has been established, but it has not been documented. **L3** - A cyberincident response structure has been documented and is kept up to date. **L4** - The cyberincident response structure is managed, updated and verified. **L5** - Improvement actions are applied in the design of the cyberincident response structure.
OBTAINING	
Collection method	Manual
Responsible	CSO o CISO
ANALYSIS	
Objective Measure	L5

Indicator	**Positive values**	Values tending to L5 indicate that there is a complete and clear scaling structure that facilitates greater coordination, internal and external, to respond to cyberincidents.
	Corrective actions	• Establish an incident response structure and escalation protocol to ensure that incidents are addressed as quickly as possible by those responsible, as failure to do so will impede the organization's diligent response, thus increasing the impact of the cyberincident. • Send periodic communications to users insisting on the need to communicate any anomaly or security event detected as soon as possible, teaching them to recognize anomalous situations that may initiate an incident (malfunction, slow processes, unusual behaviours, etc.). • Offer communication channels to users to report incident detection.

Table 29 - Metric R-GI-OE3-01: Establish an incident response structure for escalation to those responsible for its resolution.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE3-05**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Control cyberincidents until their resolution.
Description	Cyberincident control allows you to properly manage potential security events. Depending on the type of incident, it will be assigned and escalated to the appropriate people to ensure, as far as possible, its correct analysis, resolution, notification and closure. Obtaining indicators such as the time it takes to resolve the cyberincident is, in addition, vital to ensure legal compliance in the event that the cyberincident is related to personal data.
Question asked	Is a measurement of the average time from the opening of a cyber incident until it is considered closed?
Correlation	ISO/IEC 27001:2022 [A.6.8], [A.5.25] NIST SP 800-53 R5 [IR-01-00], [IR-04-00], [IR-05-00], [IR-06-00], [IR-08-00] ENS [op.exp.7] [op.exp.9]

	NIS Transposition (Art.8)	
CHARACTERIZATION		
Scale	**L0** - The average time from when a cyber incident is opened until it is considered closed is not estimated. **L1** - The establishment of a procedure to measure the average time from when a cyber incident is opened until it is considered closed has been initiated. **L2** - A procedure has been established to measure the average time from when a cyber incident is opened until it is considered closed, but has not been documented. **L3** - The procedure for measuring the average time from when a cyber incident is opened until it is considered closed is documented and updated. **L4** - The procedure for measuring the average time from when a cyber incident is opened until it is considered closed is managed, updated and verified. **L5** - Improvement actions are implemented in the procedure for defining and measuring the average time from when a cyber incident is opened until it is considered closed.	
OBTAINING		
Collection method	Manual A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values close to L5 indicate that there is an improved procedure for monitoring cyber-incidents until they are resolved, allowing measurement of the average time from opening to closure. It is desirable to increase vigilance and control especially if these detection activities depend on third parties.
	Corrective actions	• Establish and improve the process by measuring the times between which events are detected and their resolution. • Record the lessons learned for each type of event.

Table 30 - Metric R-GI-OE3-05: Measure the average time from when a cyber incident is opened until it is considered closed.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE3-06**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Establish a process to estimate the response and recovery capacity of cyberincidents.
Description	Estimate with effectiveness indicators the response and recovery capacity to a cyberincident, that is, the ability to detect attacks and threats, minimize the loss or destruction of technological or information assets, mitigate the harmful exploitation of infrastructural weaknesses and recover the services as soon as possible. Among other factors, the average time to respond to different incidents or the use of resources (hours of technicians) can be measured. One way to measure the time to resolve incidents is to record the moment in which a cyberattack is detected and when it is deactivated and assess the average elapsed time for each type of incident. If a cyberincident has never been experienced, It can be considered, for example, the times obtained in the recovery of systems in the tests of the continuity plan carried out. Standardized metrics and indicators can be followed, as indicated in the CCN-STIC 817 ICT Security Guide (see References section of the Dictionary of Indicators).
Question asked	Is there an estimation of the response and recovery capacity for a cyberincident?
Correlation	ISO/IEC 27001:2022 [A.5.26] NIST SP 800-53 R5 [IR-04-00], [IR-09-00], [IR-08-00] ENS [op.exp.7] Minimum content guide PPE (4.2) NIS Transposition (Art.5, Annex 2, 3, 4)
CHARACTERIZATION	

Scale	**L0** - The ability to respond and recover from a cyberincident is not estimated. **L1** - The definition of a procedure to estimate the response and recovery capacity to a cyberincident has been started. **L2** - A procedure has been established to measure the response and recovery capacity for a cyberincident, but it has not been documented. **L3** - The procedure to estimate the response and recovery capacity for a cyberincident has been documented and updated. **L4** - The procedure to estimate the response and recovery capacity for a cyberincident is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for the definition and estimation of the response and recovery capacity before a cyberincident.	
OBTAINING		
Collection method	Manual A personal or telephone interview is recommended in order to interpret the results with a higher level of detail.	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the number of hours between the occurrence of a cyberincident and resolution has been estimated.
	Corrective actions	• Establish a procedure to estimate the average response time to a cyberincident and the use of resources in technical hours in its resolution. • Document, update and verify the procedure to estimate the average resolution time.

Table 31 - Metric R-GI-OE3-06: Establish a process to estimate the response and recovery capacity of cyberincidents.

CAMPO	INFORMACIÓN
ID	
Code	**R-GI-OE4-01**
Goal	RECOVER
Functional domain	INCIDENT MANAGEMENT
Indicator objective	Investigate the causes of cyberincidents.
Description	Regarding the response to incidents, determining the causes of cyberincidents can be very useful to assess what has caused it; determining and refining responsibilities; and learning lessons. This can be done by relying on procedures that trace the root cause of the cyberincident. In this case, measures will have to be applied to carry out an adequate investigation: establishment of the investigation device, isolation of the system, temporal planning of the analysis and reporting of the findings to assess the risks and facilitate decision-making.
Question asked	Are the causes of cyberincidents investigated?
Correlation	ISO/IEC 27001:2022 [A.5.27] NIST SP 800-53 R5 [IR-04-00], [IR-09-00], [IR-08-00] ENS [op.exp.7], [op.exp.8] Minimum content guide PPE (4.2) NIS Transposition (Art.8)
CHARACTERIZATION	
Scale	**L0** - The origin of the cyberincidents will not be investigated. **L1** - A procedure to investigate the origin of cyberincidents has been started. **L2** - The procedure to investigate the origin of cyberincidents has been established, but it has not been documented. **L3** - The procedure to investigate the origin of cyberincidents is documented and updated. **L4** - The procedure to investigate the origin of cyberincidents is managed, updated and verified. **L5** - Improvement actions are applied in the procedure to investigate the origin of cyberincidents.
OBTAINING	
Collection method	Manual A personal or telephone interview is recommended, in order to interpret the results with a higher level of detail.
Responsible	CSO o CISO

ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that there is a procedure to investigate the causes of cyberincidents.
	Corrective actions	• Establish a procedure for the investigation of cyberincidents, using for example guides such as the CCN-STIC 817 ICT Security Guide. • Document, review and verify the procedure to investigate the causes of cyberincidents.

Table 32 - Metric R-GI-OE4-01: Investigate the causes of cyberincidents.

2.3.2. Service Continuity Management (SCM)

The overall objective of this functional domain is to establish processes to identify and analyse events, detect incidents, and determine an organization response. Its specific objectives are:

- Develop continuity plans for essential services.
- Review continuity plans.
- Test continuity plans.
- Execute and review continuity plans.
- Establish processes to manage an adequate level of controls that ensure the protection of essential services and critical assets that depend on the actions of external entities.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE1-01**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Develop a Continuity Plan to guarantee the provision of the essential service.
Description	It is about knowing if the provision of the essential service is backed by a Continuity Plan, if it follows a discipline of periodic updating and if it is also updated when new risks or changes in the organizational or operational environment are known.
Question asked	Has a Continuity Plan been defined to guarantee the permanent provision of the essential service?

Correlation	ISO/IEC 27001:2022 [A.5.29] NIST SP 800-53 R5 [CP-01-00], [CP-02-00], [CP-13-00], [PM-11-00] ENS [op.cont.2] Minimum content guide PPE (2.3) NIS Transposition (Art.6)	
CHARACTERIZATION		
Scale	**L0** - There is no Continuity Plan to guarantee the provision of the essential service. **L1** - The development of a Continuity Plan has begun to guarantee the provision of essential services. **L2** - The actions of the Continuity Plan for the provision of the essential service have been established, but they have not been documented. **L3** - The Essential Service Continuity Plan has been documented and is kept up to date. **L4** - The Continuity Plan for the continuity of the essential service is managed, updated and reviewed. **L5** - Improvement actions are applied in the Continuity Plan of the essential service.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization develops the Continuity Plan of the essential service, that is, that it contemplates the protection, dependencies or replacements of the essential assets that intervene in the provision of such service (people, information, technology and facilities).

	Corrective actions	• Review if the essential services continuity plans contemplate the critical assets involved (people, information, technology, facilities) in the essential service. • Verify that the continuity plans take into account aspects such as the relocation of activities and resources, the existence of alternative processes or redundancy, the replacement of resources and activities and temporary contingency solutions. • Adapt the Continuity Plans to established standards (for example, ISO 22313). • Develop, update and verify the actions of the Continuity Plan of the essential service for which we are doing the survey. • Make Continuity Plans available to all involved and keep versions. • Continuity plans are reviewed to ensure that there are no conflicts with other plans.

Table 33 - Metric R-CS-OE1-01: Develop a Continuity Plan to guarantee the provision of the essential service.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE1-06**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Define the RTOs in the Continuity Plan.
Description	The RTO is the time defined within the service level in which a business process must be recovered after a disaster or loss in order to avoid consequences due to the break in service continuity. The RTO establishes the temporal technical limits of the entire business continuity management strategy. The RTO (Recovery Time Objective) must be less than the MTD (Maximum Tolerable Downtime). It must be ensured that the RTO is not only documented but is used to ensure continuity of service. In addition, it is verified that the RTO complies with the essential service continuity requirements. This data is generally determined by technical personnel.
Question asked	Do continuity plans document the Recovery Time Objective (RTO) for essential service?
Correlation	ISO/IEC 27001:2022 [A.5.29]

	NIST SP 800-53 R5 [CP-01-00], [CP-02-00], [CP-13-00], [PM-11-00] ENS [op.cont.1] Minimum content guide PPE (4.2) NIS Transposition (Art.6)	
CHARACTERIZATION		
Scale	**L0 -** The RTO has not been defined nor has it been identified as necessary for the continuity of the provision of the essential service. **L1** - The need to establish the RTO for the provision of the essential service has been identified and its definition has begun. **L2** - A procedure has been established to define the RTO for the continuity of essential service provision, but it has not been documented. **L3** - A procedure to define the RTO in all continuity plans for the provision of essential service has been documented and is updated. **L4** - The procedure to define the RTO in the continuity plans for the provision of the essential service is managed, updated and reviewed. **L5** - Improvement actions are applied in the procedure to define the RTO documented in the continuity plans for the provision of the essential service.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization documents the objective recovery times (RTO) of the essential service in its continuity plan.

	Corrective actions	Identify RTOs for continuity of essential service. For this, the sum of: • detection and decision time; • the time to restore damaged or inactive computers / servers; • the time to locate the appropriate and safe backup and restore it; • the time required to resume operation. To assess the RTO, the balance with costs must be taken into account, since if it is very low, it will imply higher costs by having faster contingency equipment / services. In addition, a minimum RTO review period and system changes that require review must be specified. This information can be expanded in the CCN-STIC 803 ICT Security Guide.

Table 34 - Metric R-CS-OE1-06: Define the RTOs in the Continuity Plan.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE3-01**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Test continuity plans to ensure they meet recovery goals.
Description	It is about knowing if there are test protocols for the essential service continuity Plan and if it is regularly verified in order to: • Determine the feasibility, completeness and precision of the Continuity Plan with respect to the essential service. • Gather information on the degree of preparation of the organization. If the essential service is based on an Industrial Control System (SCI), which does not allow the completion of a complete shutdown for the execution of tests of the Continuity Plan, the implementation of partial or phased shutdowns may be considered; conducting tests on a replica of it; or even its simulation.
Question asked	Has the Continuity Plan for the provision of essential service been tested?
Correlation	ISO/IEC 27001:2022 [A.5.29] NIST SP 800-53 R5 [CP-03-00], [CP-04-00]

	ENS [op.cont.3] Minimum content guide PPE (2.3) NIS Transposition (Art.6)	
CHARACTERIZATION		
Scale	**L0** - The Continuity Plan is not tested for any essential service. **L1** - The definition of the Continuity Plan tests for essential service has begun. **L2** - Periodic tests of the Continuity Plan for essential service have been established, but they have not been documented. **L3** - All essential service continuity plan test plans have been documented and are kept up to date. **L4** - Test plans for the essential service Continuity Plan are managed, updated and reviewed. **L5** - Improvement actions are applied in the Continuity Plan as a result of the tests.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization tests the Continuity Plan of the essential service for which we are conducting the survey.
	Corrective actions	• Establish a test procedure for the Continuity Plan of the identified essential service. • Test continuity plans to ensure they meet recovery goals. • Establish a schedule for testing continuity plans and a frequency for their repetition. • Test the procedures for restoring backup copies of sensitive information. • Evaluate the continuity capacity of service providers external to the organization, if they exist. • Evaluate the ability to deploy redundant resources, locate resources, and restore copies.

Table 35 - Metric R-CS-OE3-01: Test continuity plans to ensure they meet recovery goals.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE3-03**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Evaluate the organization's response from the interruption of essential service to its recovery to a minimum acceptable level.
Description	This response can be measured by calculating the time required between the moment an interruption in the provision of the essential service occurs and the moment it becomes available again with a minimum acceptable level of functionality. This minimum acceptable level can be set as a percentage, for example when 70% of the activity has been recovered. This response can be measured by calculating the time required between the time an interruption in the provision of the essential service occurs and the moment it becomes available again with a minimum acceptable level of functionality. This minimum acceptable level can be set as a percentage, for example when 70% of the activity has been recovered.
Question asked	Is the organization response evaluated from the interruption of essential service to its recovery to a minimum acceptable level?
Correlation	ISO/IEC 27001:2022 [A.5.29] NIST SP 800-53 R5 [CP-01-00], [CP-02-00], [CP-13-00], [PM-11-00] ENS [op.cont.1] Minimum content guide PPE (4.2) NIS Transposition (Art.5, Annex 2, 3, 4)
CHARACTERIZATION	

Scale	**L0** - The organization response is not measured from the interruption of the essential service until it is restored to a minimum level of functionality. **L1** - The definition of the procedure has been started to measure the organization response from the interruption of the essential service until it is restored to a minimum level of functionality. **L2** - The procedure to measure the organization response from the interruption of the essential service until it is restored to a minimum level of functionality has been established, but it has not been documented. **L3** - The procedure for measuring the organization response from the interruption of the essential service until it is restored to a minimum level of functionality and is kept up-to-date has been documented. **L4** - The procedure to measure the organization response from the interruption of the essential service until it is restored to a minimum level of functionality is managed, updated and verified. **L5** - Improvement actions are applied in the procedure to measure the organization response from the interruption of the essential service until it is restored to a minimum level of functionality.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that a procedure is available, updated and improved to estimate the number of hours between an interruption in the provision of the service and it is available with a minimum level of functionality.
	Corrective actions	Establish the necessary mechanisms (technological, logistical and physical) to assess the time necessary for the essential service to be available again at a minimum level after the interruption event. This can be done, for example, by relying on essential service interruption simulation exercises.

Table 36 - Metric R-CS-OE3-03: Evaluate the organization's response from the interruption of essential service to its recovery to a minimum acceptable level.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE4-04**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Evaluate the organization's response from the interruption of essential service to its full recovery and normal operation.
Description	Evaluate the organization response to an interruption in the provision of essential service until it recovers its usual full functionality.
Question asked	Is the organization response assessed from the interruption of essential service to its full recovery and normal operation?
Correlation	ISO/IEC 27001:2022 [A.5.29] NIST SP 800-53 R5 [CP-01-00], [CP-02-00], [CP-13-00], [PM-11-00] ENS [op.cont.1] Minimum content guide PPE (4.2) NIS Transposition (Art.5, Annex 2, 3, 4)
CHARACTERIZATION	
Scale	**L0** - The organization response to an interruption in the provision of essential service has not been measured until it returns to its normal full functionality. **L1** - The definition of the procedure to measure the organization response to an interruption in the provision of the essential service has begun until it returns to its usual full functionality. **L2** - A procedure has been established to measure the organization response to an interruption in the provision of the essential service until it recovers its normal full functionality, but it has not been documented. **L3** - The procedure to assess the organization response to an interruption in the provision of the essential service until it recovers its usual full functionality has been documented. It is kept up to date. **L4** - The procedure to assess the organization response to an interruption in the provision of essential service is managed, updated and verified until it returns to its usual full functionality. **L5** - Improvement actions are applied in the procedure to assess the organization response to an interruption in the provision of the essential service until it recovers its usual full functionality.
OBTAINING	

Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that there is a procedure, updated and optimized for evaluating the organization's response to an interruption in the provision of the essential service until it recovers its normal full functionality.
	Corrective actions	Establish the necessary mechanisms (technological, logistical and physical) that allow evaluating how the normality of the essential service has been recovered so that it becomes fully available again in the shortest possible time after the interruption event. A constructive way is to record times when milestones are occurring: interruption, minimal service recovery, and full service recovery.

Table 37 - Metric R-CS-OE4-04: Evaluate the organization's response from the interruption of essential service to its full recovery and normal operation.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE5-02**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Identify and prioritize external dependencies related to the provision of essential services.
Description	Identify and prioritize external dependencies (third party dependencies) so as to ensure that the organization directs its cyberresilience efforts primarily towards those that contribute most, and most directly, to the provision of the essential service. Determining the impact on the organization of the dependencies of public services or basic supplies. For example, emergency or health services, providers of physical security, logical security, technological operators, hosting services, cloud services, etc.
Question asked	Are external dependencies related to essential service provision identified and prioritized?
Correlation	ISO/IEC 27001:2022 [A.5.19], [A.5.20], [A.5.21]

	NIST SP 800-53 R5 [PL-08-00] ENS [op.ext.1] Minimum content guide PSO (3.4,4.3) Minimum content guide PPE (3.2,3.3)	
CHARACTERIZATION		
Scale	**L0** - External dependencies related to the provision of essential services are not identified or prioritized. **L1** - The identification and prioritization of external dependencies related to the provision of essential services has begun. **L2** - External dependencies related to essential service provision are identified and assigned priorities, but they have not been documented. **L3** - A procedure to identify and assign priorities to external dependencies related to the provision of essential services has been documented and is kept up to date. **L4** - The procedure to identify and assign priorities to external dependencies related to the provision of the essential service is managed, updated and reviewed. **L5** - Improvement actions are applied in the procedure to identify and assign priorities to external dependencies related to the provision of the essential service.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has a prioritized list of all external dependencies that affect the essential service and that list is updated.
	Corrective actions	Establish criteria to identify and prioritize external dependencies. Keep the criteria and priorities documented, updated and periodically review them.

Table 38 - Metric R-CS-OE5-02: Identify and prioritize external dependencies related to the provision of essential services.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE6-01**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Identify and manage the risks associated with external dependencies.
Description	Identify and adequately manage the risks associated with external dependencies that contribute, directly or indirectly, to the provision of the essential service. Prioritize and update the identified risks.
Question asked	Are the risks associated with external dependencies related to the provision of the essential service properly identified and managed?
Correlation	ISO/IEC 27001:2022 [A.5.19], [A.5.20], [A.5.21] NIST SP 800-53 R5 [SA-21-00], [SC-38-00] ENS [op.ext.1] Minimum content guide PSO (3.4,4.3) Minimum content guide PPE (3.2,3.3)
CHARACTERIZATION	
Scale	**L0** - Risk management associated with external dependencies has not carried out. **L1** - Risk management associated with external dependencies has been started. **L2** - Risk management associated with external dependencies has been established, but it has not been documented. **L3** - The risk management associated with external dependencies has been documented and is kept up to date. **L4** - The risks associated with external dependencies are managed, updated and verified. **L5** - Improvement actions are applied in risk management associated with external dependencies.
OBTAINING	
Collection method	Manual
Responsible	CSO o CISO
ANALYSIS	
Objective Measure	L5

Indicator	**Positive values**	Values tending to L5 indicate that the organization has identified the risks associated with external dependencies and that this list has been prioritized and is updated.
	Corrective actions	Identify and evaluate the risks due to external dependencies so that they can be managed effectively and thus maintain the resilience of the essential service provided by the organization.

Table 39 - Metric R-CS-OE6-01: Identify and manage the risks associated with external dependencies.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE7-04**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Establish specific cyberresilience agreements with those third parties that are involved in the provision of the essential service.
Description	"It is a matter of knowing whether, for each external agency (for each third party that contributes directly or indirectly to the provision of the essential service), the organization has established and documented a detailed set of requirements that it must meet in order to provide support and improve the resilience of the organization operations. Additionally, it is a matter of knowing if that requirements have been included as part of the clauses that make up the outsourced service provision agreements, or Service Level Agreements (SLA), reached with such entities. For example: the Maximum Tolerable Downtime of the server infrastructure or the penalties in the event of non-compliance.
Question asked	Are cyberresilience requirements included in agreements with those third parties that contribute, directly or indirectly, to the provision of the essential service?
Correlation	ISO/IEC 27001:2022 [A.5.19], [A.5.20], [A.5.21] NIST SP 800-53 R5 [RS-05-00], [SA-08-00] ENS [op.ext.1] Minimum content guide PPE (2.3,3.2) NIS Transposition (Art. 6)
CHARACTERIZATION	

Scale	**L0 -** Cyber resilience requirements are not included in service level agreements with providers (external dependencies). **L1** - The inclusion of cyberresilience requirements in agreements with external agencies has begun. **L2** - Cyber resilience requirements have been established in relations with external dependencies, but they have not been documented. **L3** - Cyber resilience requirements have been documented in agreements with external agencies and are kept up to date. **L4** - Cyber resilience requirements are managed, updated and verified in agreements with external agencies. **L5** - Actions to improve cyberresilience are applied in agreements with external agencies.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization verifies and updates cyberresilience requirements in all agreements with external entities that contract services that support the essential service.
	Corrective actions	Define, update and review cyberresilience requirements in Service Level Agreements (ANS) with external entities, so that: • are required by the organization; • include detailed and complete specifications of what must be fulfilled by the external entity; • include the required performance standards; • are updated when appropriate and periodically, so that they reflect the necessary changes during the term of the relationship.

Table 40 - Metric R-CS-OE7-04: Establish specific cyberresilience agreements with those third parties that are involved in the provision of the essential service.

CAMPO	INFORMACIÓN
ID	
Code	**R-CS-OE8-01**
Goal	RECOVER
Functional domain	SERVICE CONTINUITY MANAGEMENT
Indicator objective	Supervise and manage the operation of external dependencies.
Description	Supervise and manage the operation of external dependencies that support the provision of the essential service in accordance with the cyberresilience requirements agreed with the organization. It is a matter of knowing whether there is a regular supervision of the operations of third parties that contribute, directly or indirectly, to the provision of the essential service, so that compliance with the cyberresilience requirements agreed between the parties is verified. Additionally, this will make possible to know whether the operational problems regarding the provision of outsourced services are solved. Supervise and manage the operation of external dependencies that support the provision of the essential service in accordance with the cyberresilience requirements agreed with the organization.
Question asked	For those third parties that participate, directly or indirectly, in the provision of the essential service, are their operations supervised and managed in accordance with the cyberresilience requirements agreed with the organization?
Correlation	ISO/IEC 27001:2022 [A.5.22] NIST SP 800-53 R5 [CA-02-00], [SA-03-00], [SA-09-00], [SR-06-00], [SA-08-00] ENS [op.ext.2] Minimum content guide PPE (2.3,3.2) NIS Transposition (Art. 6)
CHARACTERIZATION	

Scale	**L0** - There is no supervision and management of the operation of the external dependencies. **L1** - The supervision and management of the operation of the external dependencies has begun. **L2** - A procedure has been established for the supervision and management of the operation of the external dependencies, but they have not been documented. **L3** - The procedure for the supervision and management of the operation of the external dependencies has been documented and is kept up to date. **L4** - The procedure for the supervision and management of the operation of the external dependencies is monitored and verified. **L5** - Improvement actions are applied in the procedure to supervise and manage the operation of external dependencies.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization periodically monitors the operation of the external dependencies that support the essential service to verify that they comply with the established cyberresilience requirements.
	Corrective actions	Establish a procedure, which will be updated and improved, to periodically monitor the operation of the dependencies outside the essential service and analyse deviations from the established cyberresilience requirements to understand the potential impact on the organization.

Table 41 - Metric R-CS-OE8-01: Supervise and manage the operation of external dependencies.

2.4. Evolve

The tabs for the metrics corresponding to the Evolve goal are detailed below.

2.4.1. Configuration and Change Management (CCM)

The general objective of this functional domain is to establish processes that guarantee the integrity of the assets that support essential services, so that changes in such assets affect the organization as little as possible. Its specific objectives are:

- To manage the life cycle of critical assets that support essential services.
- To manage the integrity of information and technological assets.
- To establish asset configuration baselines.

In addition, the following indicator corresponds to it:

CAMPO	INFORMACIÓN
ID	
Code	**E-CC-OE2-01**
Goal	EVOLVE
Functional domain	CONFIGURATION AND CHANGE MANAGEMENT
Indicator objective	Manage the configuration of information and technological assets.
Description	Establish a procedure for managing the configuration of the components and computer or technological equipment associated with the system that provides the essential service in a way that facilitates its acceptable restoration, after a cyberincident with serious consequences. Additionally, the management of changes in those components and equipment must be guaranteed, so that potential negative impacts on the provision of essential service due to such changes are prevented.
Question asked	Is a configuration management procedure followed for the equipment associated with the system that makes it possible to provide the essential service?
Correlation	ISO/IEC 27001:2022 [A.8.32] NIST SP 800-53 R5 [CM-01-00], [CM-02-00], [CM-03-00], [CM-06-00], [CM-09-00], [SA-05-00], [SA-10-00] ENS [op.exp.2] Minimum content guide PPE (4.2.3)
CHARACTERIZATION	

Scale	**L0** - There is no configuration management procedure for computer and technological equipment. **L1** - The establishment of a procedure for managing the configuration of computer and technological equipment has begun. **L2** - The procedure for managing the configuration of computer and technological equipment has been established, but it has not been documented. **L3** - The procedure for managing the configuration of computer and technological equipment has been documented, and it is kept up to date. **L4** - The procedure for managing the configuration of computer and technological equipment is managed, updated and reviewed. **L5** - Improvement actions are applied in the procedure for managing the configuration of computer and technological equipment.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization carries out the configuration management of the computer and technological equipment that supports the essential services. This provides a level of control to avoid altering the support it provides to essential services. The procedure must guarantee the restoration of the service, in an acceptable way, after a cyberincident with serious consequences.

	Corrective actions	• Establish a configuration management procedure for the technological assets that support the essential service. • Identify and inform those responsible for managing change. • Evaluate the cyberresilience requirements caused by the changes made to the assets that support essential services (information, technology, facilities). • Implement mechanisms to detect changes in technological assets, whether at the level of policies and procedures, technical (change management *software*), or physical (inspections and audits).

Table 42 - Metric E-CC-OE2-01: Manage the configuration of information and technological assets.

CAMPO	INFORMACIÓN
ID	
Code	**E-CC-OE2-06**
Goal	EVOLVE
Functional domain	CONFIGURATION AND CHANGE MANAGEMENT
Indicator objective	Test changes in technology assets before going into production.
Description	Changes applied to systems within the development life cycle should be controlled through the use of formal change control procedures. The production phase is one of the most important, since it supports the operation of assets that intervene in the provision of the essential service. Technical review of applications before changes to the operating platform is extremely important to ensure essential service degradations or interruptions. Whenever a change affecting production assets is identified (integration of a new component, modification of configuration, or removal of an asset), the test suite should be designed and run to ensure that there is no adverse impact on the operations or security of the organization, before making the change. Changes applied to systems within the development life cycle should be controlled through the use of formal change control procedures. The production phase is one of the most important, since it supports the operation of assets that intervene in the provision of the essential service. Technical review of applications before changes to the operating platform is extremely important to ensure essential service degradations or interruptions.
Question asked	Are changes in technology assets tested before going into production?

Correlation	ISO/IEC 27001:2022 [A.8.32], [A.8.31], [A.8.29]* NIST SP 800-53 R5 [CM-01-00], [CM-02-00], [CM-03-00], [CM-06-00], [CM-09-00], [SA-05-00], [SA-10-00] ENS [op.pl.3], [op.exp.3], [op.exp.4] [op.exp.5] Minimum content guide PPE (4.2.3)	
CHARACTERIZATION		
Scale	**L0** - There is no procedure to test changes in technology assets before going into production. **L1** - The establishment of a procedure to test the changes in technological assets has begun before going into production. **L2** - The procedure to test the changes in the technological assets before going to production has been established, but it has not been documented. **L3** - The procedure for testing changes in technology assets before going into production has been documented and is kept up to date. **L4** - The procedure to test changes in technological assets is managed, updated and reviewed before going into production. **L5** - Improvement actions are applied in the procedure to test the changes in technological assets before going into production.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization carries out a procedure to test the changes in technological assets before going into production. This provides a level of control to avoid altering the support it provides to essential services. The procedure must ensure that the system works perfectly in the presence of new asset changes.

	Corrective actions	• Establish a procedure to test changes in technology assets before going into production. • Establish a pre-production environment similar to that of production where validate the integration of changes and the stability of the environment. • Identify and document the relevant tests (performance, consumption, security, etc.) and those responsible for executing them.

Table 43 - Metric E-CC-OE2-06: Test the changes in technological assets before going into production.

2.4.2. Communication (CM)

The general objective of this functional domain is to establish processes that guarantee communication between managers involved in the operation of essential services, both internal and external to the organization. Its specific objectives are:

- Establish communication mechanisms, internal and external to the organization.
- Guarantee the availability of the media.
- Communicate the continuity strategy to the entire organization.
- Communicate problems, weaknesses, and changes.

In addition, the following indicators correspond to it:

CAMPO	INFORMACIÓN
ID	
Code	**E-CM-OE1-02**
Goal	EVOLVE
Functional domain	COMMUNICATION
Indicator objective	Establish communication mechanisms external to the organization regarding cyberresilience.
Description	Define and establish external communication mechanisms in the area of cyberresilience with, among others: customers, suppliers, the media, State Security Forces and Bodies, emergency services, etc. It should be assessed whether these mechanisms are effective and whether they are used regularly.
Question asked	Have effective external communication mechanisms been defined and established for cyberresilience? For example, with clients, suppliers, the media, the State Security Forces and Bodies or emergency services.
Correlation	NIST SP 800-53 R5 [IR-07-00], [SA-09-00] Minimum content guide PSO (2.2.1, 2.2.4) Minimum content guide PPE (2.1, 2.3, 4.2.1

CHARACTERIZATION		
Scale	**L0** - No communication is established with external entities regarding cyberresilience. **L1** - Communication with external entities in the area of cyberresilience has begun. **L2** - Communication mechanisms have been established with external entities in the area of cyberresilience, but they have not been documented. **L3** - The communication mechanisms with external entities in cyberresilience have been documented in a procedure and are kept up to date. **L4** - The procedure for communication with external entities in the area of cyberresilience is managed, updated and verified. **L5** - Improvement actions are applied in the procedure for communication with external entities in the area of cyberresilience.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization establishes procedures, updates and improves them, to manage the mechanisms regarding external communication formally and regularly with, among others: clients, suppliers, the media, State Forces and Bodies, services emergency etc.
	Corrective actions	• Establish effective external communication mechanisms through the authorized channels. • Create good practices to communicate cyberincidents.

Table 44 - Metric E-CM-OE1-02: Establish communication mechanisms external to the organization regarding cyberresilience.

CAMPO	INFORMACIÓN
ID	
Code	**E-CM-OE2-02**
Goal	EVOLVE
Functional domain	COMMUNICATION
Indicator objective	Guarantee the availability of internal or external communication channels required by the essential service.
Description	The objective is to guarantee that, in the event of an interruption, the mechanisms necessary to establish the appropriate communications with the actors that are necessary to recover the provision of the essential service exist and function. This involves verifying, for example, that the incident can be communicated to whom it may concern for resolution. In any case, there will be alternative communication channels in the event that the usual ones fail, offering the same communication protection guarantees as the usual channel; and guarantee a maximum time of entry into operation. The objective is to guarantee that, in the event of an interruption, the necessary mechanisms to establish the appropriate communications with the actors that are necessary to recover the provision of the essential service exist and function.
Question asked	Has the availability of internal or external communication channels required by the essential service been verified?
Correlation	NIST SP 800-53 R5 [CP-02-02], [CP-08-00], [SC-01-00] ENS [op.cont.4] Minimum content guide PSO (2.2.1, 2.2.4) Minimum content guide PPE (2.1, 4.2.1)
CHARACTERIZATION	

Scale	**L0** - The availability of the internal or external communication channels required by the essential service is not verified. **L1** - The tests for the availability of the internal or external communication channels required by the essential service have been started. **L2** - A procedure has been established to verify the availability of internal or external communication channels required by the essential service, but it has not been documented. **L3** - A procedure to verify the availability of internal or external communication channels required by the essential service has been documented and is kept up to date. **L4** - The procedure to verify the availability of internal or external communication channels required by the essential service is managed, updated and verified. **L5** - Improvement actions are applied in the procedure to verify the availability of internal or external communication channels required by the essential service.	
OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization has a procedure for verify the availability of internal or external communication channels required by the essential service. For example, it is verified that the cyberincident can be communicated to whom it may concern in the event of interruption of the normal operation of essential services.
	Corrective actions	• Establish a procedure to verify that the cyberincident can be communicated to whom it may concern in case of interruption of the normal operation of the essential service for which we are conducting the survey. • Test the communication capabilities to be used in the event of interruption of the normal operation of essential services. • Verify that the potential or real problems and the detected weaknesses are communicated in a timely manner to avoid their further occurrence.

Table 45 - Metric E-CM-OE2-02 Guarantee the availability of internal or external communication channels required by the essential service.

CAMPO	INFORMACIÓN
ID	
Code	**E-CM-OE3-02**
Goal	EVOLVE
Functional domain	COMMUNICATION
Indicator objective	Communicate the continuity strategy to the entire organization.
Description	It is about knowing if the delegations of authority and assignments of responsibility (both internal and external) that have been established within the framework of the cyberresilience program have been carried out with the required publicity and transparency, so that all the personnel involved in the program knows its particular role and recognizes who is the authority in each moment.
Question asked	Does the essential service continuity plan include the allocation of the respective delegations of authority and communicate these responsibilities to all those involved (both internal and external)?
Correlation	ISO/IEC 27001:2022 [A.5.29] NIST SP 800-53 R5 [CP-02-03], [CP-03-00] ENS [op.cont.2] Minimum content guide PSO (2.2.1) Minimum content guide PPE (4.2, 4.2.2)
CHARACTERIZATION	
Scale	**L0 -** The responsibilities involved are not assigned and communicated to the personnel involved in the continuity plans. **L1** - The assignment and communication of responsibilities to the personnel involved in the continuity plans has begun. **L2** - A procedure has been established to assign and communicate responsibilities to the personnel involved in the continuity plans, but they have not been documented. **L3** - The procedure for assigning and communicating responsibilities to the personnel involved in the continuity plans has been documented and is kept up to date. **L4** - The procedure for assigning and communicating responsibilities to the personnel involved in the continuity plans is managed, updated and verified. **L5** - Improvement actions are applied in the procedure to assign and communicate the responsibilities to the personnel involved in the continuity plans.

OBTAINING		
Collection method	Manual	
Responsible	CSO o CISO	
ANALYSIS		
Objective Measure	L5	
Indicator	**Positive values**	Values tending to L5 indicate that the organization guarantees the assignment and communication of responsibilities and authorities within the Continuity Plan to all the personnel involved, both internal and suppliers involved, with the aim of knowing their roles and responsibilities.
	Corrective actions	• Establish, verify and improve a procedure for the assignment and communication of responsibilities and authorities within the Continuity Plan to all the personnel involved. • Guarantee the communication of responsibilities and authorities within the continuity plan to all the personnel involved, who know their roles and responsibilities. • Guarantee that the continuity strategy is communicated and understood within the organization, as well as the importance of complying with such strategy. • Check that changes or variations of legal requirements are communicated to employees and other interested parties.

Table 46 - Metric E-CM-OE3-02: Communicate the continuity strategy to the entire organization.

3. ACRONYMS

- BIA: *Business Impact Analysis*.
- CISO: *Chief Information Security Officer*.
- CSO: *Chief Security Officer*.
- CVSS: *Common Vulnerability Score System*.
- ENS: Esquema Nacional Seguridad.
- ISO: *International Organization for Standardization*.
- MTD: *Maximum Tolerable Downtime*.
- NIST: *National Institute of Standards and Technology*.
- PPE: Planes de Protección Específicos.
- PSO: Planes de Seguridad del Operador.
- RPO: Punto objetivo de recuperación, del inglés *Recovery Point Objetive.*
- RTO: Tiempo objetivo de recuperación, del inglés *Recovery Time Objetive*.

4. REFERENCES

- CNPIC. Good Practice Guide - Specific Protection Plan (PPE)
  https://cnpic.interior.gob.es/opencms/pdf/publicaciones/guias-y-metodologias/2.GUIA-BUENAS-PRATICAS-PPE.pdf
- CCN (2020). CCN-STIC 817 ICT Security Guide
  https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
- CCN (2017). CCN-STIC 803 ICT Security Guide
  https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html
- INCIBE (2020). National Guide for Notification and Management of Cyber Incidents
  https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf
- NIST. Special Publication 800-53 Rev.4
  https://nvd.nist.gov/800-53
- NIST. Special Publication 800-53A Rev.5
  https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final
- AENOR (2017). UNE-EN ISO: 27001:2017 Information technology. Security techniques. Information Security Management Systems.
  https://www.iso.org/isoiec-27001-information-security.html
  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058428
- ISO (2018). ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management
  https://www.aenor.com/normas-y-libros/buscador-de-normas/ISO?c=075281
- AENOR (2018). UNE ISO: 31000:2018 Risk management. Guidelines
  https://www.iso.org/iso-31000-risk-management.html
  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0059900
- ISO (2015). ISO/TS 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)
  https://www.aenor.com/normas-y-libros/buscador-de-normas/iso?c=050054
- España. BOE. Cybersecurity Law Code
  https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad
  It includes (among others):
  - Spain (2017). **National Security Strategy**.
  - Law 8/2011, of 28 April, establishing measures for the **protection of the critical infrastructures**.
  - Real Decree 3/2010, of 8 of January, regulating the **National Security Scheme** in the field of Electronic Administration.
  - Resolution of September 8, 2015, of the Secretary of State for Security, approving the new minimum contents of the **Operator Security Plans and the Specific Protection Plans**.
  - Real Decree-Law 12/2018, of 7 September, on the **security of the networks and information systems**.
- UE (2016). Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of networks and information systems within the Union

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA&toc=OJ:L:2016:194:TOC

- España (2020). National Guide for Notification and Management of Cyber Incidents https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf
- MITRE (2023). MITRE Launches Cyber Resiliency Engineering Framework Navigator. https://www.mitre.org/news-insights/news-release/mitre-launches-cyber-resiliency-engineering-framework-navigator
- MITRE. (s.f). Navigator. https://crefnavigator.mitre.org/navigator