yes

CELSIA

La energía que quieres

Política

de Ciberseguridad

Version:	3
Approval date:	11/01/2021
Responsible process:	Technology
Approved by:	steering Committee

Cybersecurity Policy

1. Statement

Establish all those organizational, technical, physical and legal measures aimed at the identification, protection, detection, response and recovery of critical cyber assets in such a way that compliance with the laws, regulations and regulations in force that are applicable to the organization is achieved, against unauthorized access, disclosure, duplication, operation interruption, modification, destruction, loss, theft, or misuse, which may occur intentionally or accidentally, seeking to guarantee the reliability, confidentiality, integrity, and availability of technologies of operation, to ensure the sustainability and security of the businesses.

Through this policy, CELSIA's cybersecurity objectives are disseminated, which are achieved with the application of cybersecurity controls, to manage an acceptable level of cyber risk.

Technology is responsible for carrying out the awareness, communication, training and socialization actions of the cybersecurity policy and cybersecurity processes where the following objectives are included at least:

- *Identification and documentation of the current situation.*
- *Establishment of cyber security procedures.*
- *Design of security architectures applicable to cyber assets.*
- *Definition and implementation of legal, technical, organizational and physical controls.*
- *Implementation of a cycle of continuous improvement of cybersecurity management.*

The principles of the policy are part of CELSIA's culture, which is why a commitment on the part of CELSIA's Steering Committee is ensured for the dissemination, consolidation and compliance with this policy.

2. Scope

This policy is applicable to all collaborators, suppliers, contractors, third parties, who physically or remotely enter the security perimeters and access critical cyber assets owned by CELSIA and its subsidiaries.

This policy must be reviewed at least once a year or when necessary.

3. Policy guidelines

Organization for the cybersecurity

This policy establishes a cybersecurity governance model that provides guidance and direction for cybersecurity management, as well as the necessary resources to carry out tasks related to cybersecurity management, projects, and operation.

Cybersecurity will be supported by a Security Operations Center, which will have the necessary capabilities for the identification, operation and response to cybersecurity incidents, will be assigned the pertinent responsibilities in said matter and will report directly to the Cybersecurity Leader.

Government Model

CELSIA has defined the following organizational structure with instances, roles and responsibilities, in order to ensure proper compliance with this policy:

Board of Directors and Senior Management: *Responsible for the adoption and adequate implementation of the cybersecurity policy, the establishment of an organizational structure that provides guidance and direction for the management of cybersecurity, granting the necessary resources for the implementation of measures in favor of the cybersecurity, and exercise the appropriate leadership in front of its collaborators to reduce cybersecurity risks.*

Cybersecurity Committee: *Responsible for the definition, management and operation of the cybersecurity program, including the established cybersecurity policies and guidelines applicable to the organization.*

The Cybersecurity Committee must establish management and control criteria that allow the most appropriate protection mechanisms for CELSIA's critical cyber assets to be implemented, applying the principles of confidentiality, integrity and availability, authenticity, authorization, traceability and non-repudiation.

Responsible for critical assets and cyber assets: *Celsia is the owner of the critical assets and cyber assets, their possession and management is delegated to Generation, Transmission and Distribution, Human Talent and Organizational Solutions who are responsible for the critical assets and cyber assets assigned to them, as well as the classification, control and monitoring of their use and management . For this reason, they must be aware of the risks to which the critical assets and cyber assets in their charge are exposed, so that they exercise the appropriate leadership towards their collaborators to reduce them.*

Technology: *Responsible for managing the necessary measures to mitigate the risks associated with cybersecurity and will report any associated event to the cybersecurity committee.*

Audit: *Responsible for evaluating compliance with the cybersecurity policy, contributing to the identification of new risks and associated controls to strengthen cybersecurity.*

Users: *Any collaborator, supplier, contractor, or other authorized person who uses critical assets and cyber assets of the organization in the execution of their daily work activities.*

Classification and control of cyber assets

Critical cyber assets must be identified and prioritized according to cyber risks and cyber security exposures in an updated inventory; with the aim of avoiding financial, operational and/or image losses for the organization.

Treatment and Management of cyber risk

Generation, Transmission and Distribution, Human Talent and Organizational Solutions are responsible for analyzing, prioritizing and treating cyber risks based on business objectives and aligned with the risk management policy.

In projects or new acquisitions, the identification of critical assets and critical cyber assets, risks, vulnerabilities and the level of cyber security management in the operation must be carried out to establish a cyber security plan.

Physical and Environmental Security

Resource Protection, you must document, implement and maintain a physical security program for the protection of critical cyber assets.

All critical cyber assets defined in an electronic security perimeter must reside within a physical security perimeter and be in areas physically protected from unauthorized access, damage, or interference.

Control of access to cyber assets

Generation, Transmission and Distribution, Human Talent and Organizational Solutions in accordance with the classification of critical cyber assets, must implement the applicable cybersecurity measures as the case may be, in order to avoid adulteration, loss of continuity of operation, leakage, consultation unauthorized or fraudulent use or access.

Access control to critical cyber assets must be based on the principle of least privilege, which implies that access will not be granted unless explicitly authorized.

Electronic security perimeters within which critical cyber assets reside and their access points must be identified, protected and traceable.

Cybersecurity incident management

All collaborators, consultants, contractors, third parties must report any vulnerability that they have observed or that they suspect exists in the systems or services that support the operation through the Services Help Desk.

The Security Operations Center will report incidents with an impact on critical cyber assets to the Cybersecurity Leader so that they can be evaluated and reported to the Operations Center Leader in accordance with the organization's incident procedure.

Critical cyber assets recovery plan

Generation, Transmission and Distribution, Human Talent and Organizational Solutions must implement recovery plans for critical cyber assets and that said plans correspond to the techniques and practices established for business continuity.

exceptions

Exceptions to any compliance with the policy must be approved by the Technology and Cybersecurity Leader, which may require authorization from the Human Talent and Organizational Solutions Leader and the CELSIA Leader. All exceptions to the policy must be formally documented, logged, and reviewed.

Breach of the cybersecurity policy

Violations of the cybersecurity policy or its guidelines by employees will trigger treatment measures for cybersecurity incidents generated and could be subject to disciplinary actions by Human Resources.

4. Definitions

For the purposes of this document, the following concepts are defined:

- ***Critical asset** : Installations, systems or electrical equipment that, if destroyed, degraded or made unavailable, affects the reliability or operability of the electrical system. In accordance with the recommendations of the CNO Technology Committee for the definition of critical assets that compromise the safety of the SIN operation.*

- ***Cyberactive :** Programmable electronic device and elements of communications networks including hardware, software, data and information. As well as those elements with routable communication protocols, which allow access to it locally or remotely.*

- ***cyber asset :** Device for the reliable operation of critical assets that meets the following attributes:*

- *The cyber asset uses a routable protocol to communicate outside the electronic security perimeter, or,*
- *The cyber asset uses a routable protocol with a control center, or,*
- *The cyberactive is accessible by dialing.*

- ***Confidentiality:** property that determines that information is not available or disclosed to unauthorized individuals, entities or processes.*

- ***Disaster or contingency:** interruption of the ability to access information and process it through computers or other means necessary for the normal operation of a business.*

- ***Availability:** property that the information is accessible and usable by request of an authorized entity.*

- ***Cybersecurity event:** The identified presence of a condition of a system, service, or network, indicating a potential breach of cybersecurity policy or failure of safeguards, or a previously unknown situation that may be relevant to security.*

- ***Cybersecurity Guidelines:** are approved products, procedures and metrics, which define in detail how security policies will be implemented for a particular environment, taking into account the strengths and weaknesses of the available security features. They must be reflected in a document that describes the implementation of a guide for a specific component of hardware, software or infrastructure.*

- ***Integrity:** property of safeguarding the accuracy and completeness of assets.*

- ***Vulnerability:** weakness of an asset or group of assets, which can be exploited by one or more threats.*

5. Annexes

- *TEC-N-1 Cybersecurity policy guidelines.*

Change control

Version	Date	Version Justification
1	02/15/2019	Creation of the document.
2	12/18/2020	The reference standard is updated; agreement number 1241 by the Cybersecurity Guide of the National Operation Council.
3	11/01/2021	Reference standards that were used as the basis for the policy are excluded. Change of name of the vice presidency Human Administrative Management and Technology for Human Talent and Organizational Solutions. Change in the policy documentation format.