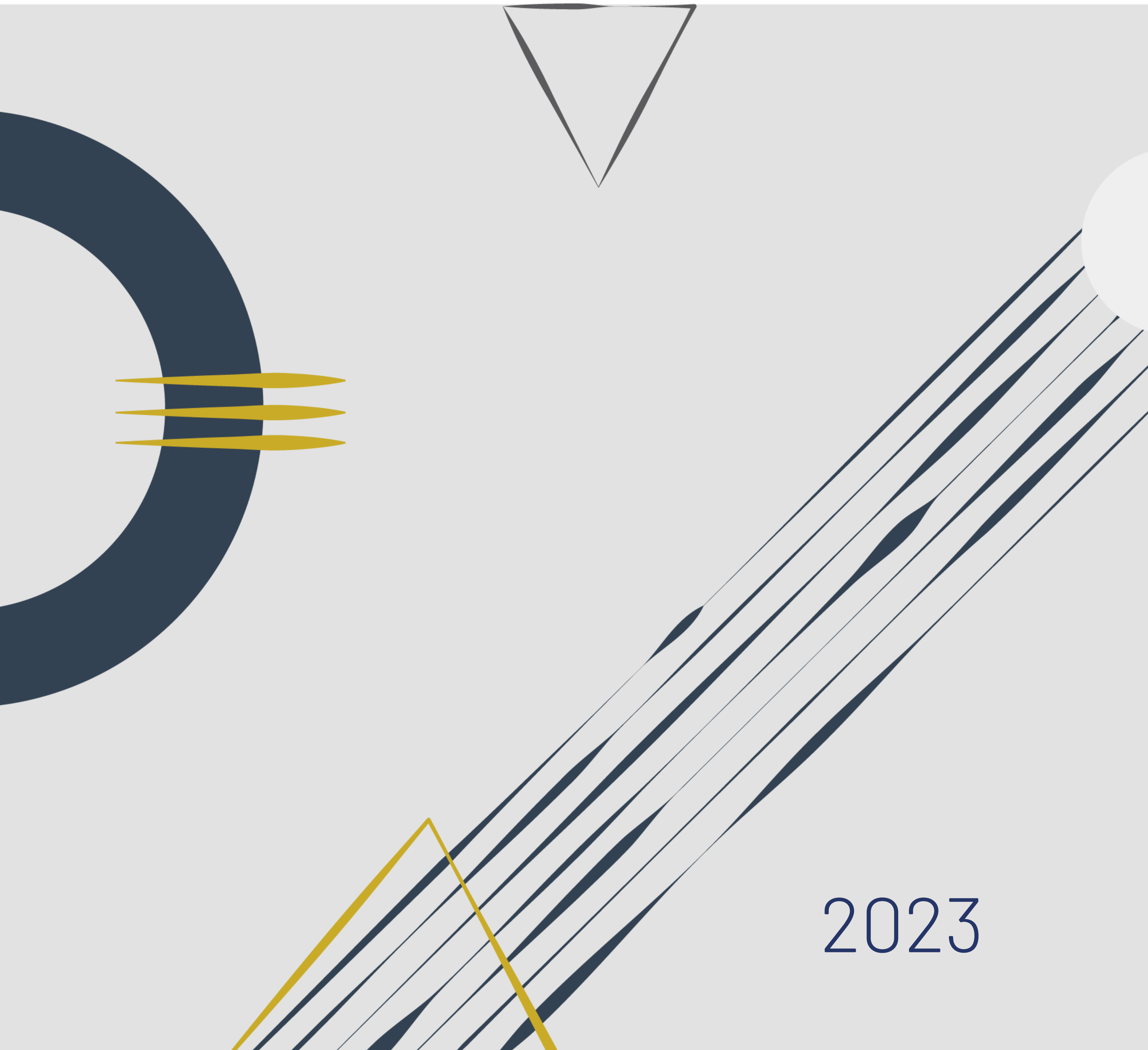
FORO
NACIONAL DE
CIBERSEGURIDAD

GOOD GOVERNANCE CODE ON CYBERSECURITY



2023

Traducción al inglés ofrecida por ISMS Forum

Catálogo de publicaciones de la Administración General del Estado

https://cpage.mpr.gob.es

Edita:

GOBIERNO
DE ESPAÑA

MINISTERIO
DE LA PRESIDENCIA, RELACIONES CON LAS CORTES
Y MEMORIA DEMOCRÁTICA

NIPO (edición online): 089-23-013-9
Fecha de edición: junio 2023

GOOD GOVERNANCE CODE ON CYBERSECURITY

Experts participating in these Working Groups have acted in their personal capacities. Therefore, their opinions and recommendations do not stand for or hold their organisations accountable.

These papers are the result of a collective reflection exercise; however, their conclusions and proposals does not necessarily represent the opinion of all the participants, which do not necessarily share all them.

ACKNOWLEDGMENTS

Civil society coordinator:

Gianluca D'Antonio (Presidente de ISMS Forum)

Institutional coordinator:

Andrés J. Ruiz Vázquez (Departamento de Seguridad Nacional)

Authors and contributors:

Raúl Amigorena Eguiluz

Roberto Baratta Martínez

Mariano J. Benito Gómez

Juan Fco. Cornago Baratech

Ángel Domínguez Fernández-Burgos

Javier García Quintela

Daniel Largacha Lamela

Idoia Mateo Murillo

Francisco del Olmo Fons

Luis Paredes Hernández

Julia Perea Velasco

Olga Ramírez Sánchez

Antonio Ramos García

Jesús Sánchez López

Alejandro Viana Lara

María Elisa Vivancos Cerezo

CONTENTS

1. INTRODUCTION

In April 2019, the **National Security Council** approved the National Cybersecurity Strategy, the text of which highlights public-private cooperation as a key component to achieve the goals established in cybersecurity. The Strategy also foresees the National Cybersecurity Forum, an area within the National Security System composed of representatives of civil society, independent experts, the private sector, academic institutions, associations and non-profit organisations, among others, with the aim to strengthen and create public-private synergies.

Cybersecurity has become the strategic foundation on which the digital revolution experienced by all sectors of society, including public administrations, companies and citizens, is based. It will only be possible to continue to progress safely in this transformation if cybersecurity is the basis.

The regulatory framework for cybersecurity has evolved over the last few years, both at a national and European level, seeking to improve the cybersecurity of new sectors whose obligations have been increased. Many of the regulatory developments and changes in this area have been prompted by the increasingly frequent and costly negative effects borne by organisations, either as a result of cyber-attacks or inadequate internal management of cybersecurity risks.

In Spain, the new **National Cybersecurity Framework**, set down in Royal Decree 311/2022[1], explicitly mentions the need to follow a process of continuous and adaptive improvement of cybersecurity, which is an increasingly relevant part of the **country's sustainability model**, because of the impact it can have, not only on the organisation itself, but also on its employees, suppliers, customers and stakeholders who may be affected by the organization's activities. Also, **Royal Decree 43/2021**[2] requires the appointment of an **information security officer** in the organisation who reports directly to senior management and maintains appropriate independence from those in charge of networks and information systems.

[1] Royal Decree 311/2022, of 3 May, regulating the National Cyber-security Scheme.

[2] Royal Decree 43/2021, of 26 January, implementing Royal Decree-Act 12/2018, of 7 September, on the security of networks and information systems

At European level, Directive EU 2022/2555, known as **NIS 2**, on measures for a high common level of cybersecurity across the Union, includes specific cybersecurity governance measures. Among these, it establishes that the management bodies of organisations shall **approve cybersecurity risk management measures and supervise their implementation**.

The **National Cybersecurity Forum**, at its plenary session on 8 October 2021, approved the lines of work for the 2021 - 2022 period for each of the working groups comprised in the Forum. Specifically, the **incorporation of cybersecurity into the good corporate governance of organisations** was the line of work approved to be elaborated by **Working Group 1 on Cybersecurity Culture**.

Management bodies are in charge of the organisation's leadership and the monitoring of their correct functioning, including supervising the management and control of **corporate risks**, which ever more frequently and more intensely include those of a cybernetic nature.

Accordingly, and along the lines approved at the National Cybersecurity Forum, Working Group 1 began the task of **compiling the fundamental principles and associated recommendations that the management bodies of an organisation,** regardless of its size or sector, can follow in order to ensure suitable governance of its cybersecurity.

This Code of Good Governance is the final result of the work of the aforementioned Group, made up of experts in cybersecurity, as well as the analysis of various existing regulations and standards, examined from a practical and current perspective, to improve corporate governance in the field of cybersecurity.

2. GOAL

The new challenges arising from the materialisation of threats in cyberspace have generated a significant increase in cyber attacks, both in terms of volume and in terms of frequency and/or sophistication. Facing new cybersecurity challenges requires policies of continuous review and improvement, together with the optimisation of cybersecurity controls and measures, applied both to the protection of the value and functioning of organisations and to the protection of the citizens' data they hold.

This Code of good governance is neither a definition of a new standard of controls, nor an implementation manual. On the contrary, the goal of the Code is to propose to organisations practices aimed at supporting a **cybersecurity governance model** that facilitates the management of the security of networks and information systems, as well as contributing to improve the decision-making process in this field by the organisations' governing bodies and, in particular, by the management body.

With this general goal in mind, a number of specific goals are set out below:

- **Goal I. Integrate the guiding principles of cybersecurity governance into a single code of good governance.**

  Group together, in a specific and succinct manner, the main activities that an organisation must carry out to govern its corporate cybersecurity in a suitable and mature manner.

  Have in place a common approach for the guiding principles, security measures and audit procedures, as well as elements to monitor compliance with current or future cybersecurity standards that may be implemented.

- **Goal II. Create a document to assist the organisation's management body and management team.**

  Identify the major issues related to cybersecurity management and/or risks that need to be addressed by an organisation, the sessions in which these issues are to be addressed and their periodicity.

- **Goal III. Train and raise awareness among organisations' governing bodies and management teams on their role and responsibility in the field of cybersecurity.**

  Serve as a reference for managers of organisations and their governance bodies to understand their responsibilities and functions in the proper management of corporate cybersecurity.

- **Goal IV. Provide a comprehensive view of cybersecurity monitoring and reporting responsibilities.**

  Explicitly define the cybersecurity monitoring and reporting responsibilities and provide guidance on which significant events or incidents should be reported to management, governance bodies and/or supervisory bodies.

3. SCOPE

This Good governance code on cibersecurity **provides general recommendations**, organised in Principles so that it may be used by any organisation seeking to achieve an adequate governance of cybersecurity, regardless of its size, sector, activity or even degree of maturity in the field.

The effective implementation of the Principles and Recommendations included in this Code by an organisation could de facto be interpreted as a **sign of maturity in cybersecurity** and contribute to better risk management and protection of its goals and of the stakeholders that may be affected by the activities of the organisation.

This Code **may also be used by the organisation as a guide for compliance with reporting obligations** that may be required by various supervisory bodies.

4. STRUCTURE

The Code presents a **principles' approach** defined as the set of values, experiences and standards that guide and regulate the governance of cybersecurity.

These principles may be considered as **supporting the vision, mission and strategic goals** of cybersecurity risk management and should be observed for the improvement of the decision-making process by the bodies responsible for any organisation, according to the Principle of proportionality, irrespective of its size or activity.

The principles are drawn up in the form of recommendations that are fundamental for their implementation.

They are organised in three major blocks:

- **Strategy and organisation**

  This details the most important principles on which management bodies must build the cybersecurity strategy and organisation. These principles are directly related to the management of cybersecurity.

- **Management**

  A set of fundamental activities, controls and decisions that organisations must undertake to ensure that they have suitable cybersecurity maturity, including the prevention, detection, response to and recovery from incidents. These principles should be implemented by the organisation's management from the cybersecurity or information security unit.

- **Supervision**

  This details the minimum elements that need to be validated by the organisation's governance bodies, as well as the basic requirements that the information to be received must meet in order to perform this validation. It specifies how continuous supervision should be carried out by the organisations' management and the cybersecurity or information security unit.

5. PRINCIPLES AND RECOMMENDATIONS

Principle 1: Proportionality

The recommendations included in this Code will be applied to organisations under the principle of proportionality, taking into account their own complexity, size, the risks to which they are subject, the resources they have available and other applicable circumstances.

5.1 Strategy and organisation

Principle 2: Strategic alignment and foresight

Cybersecurity, as a discipline that helps organisations achieve their goals, **needs to be aligned with the organisation's mission and vision**.

Recommendation 1: The management body shall formally recognise, in a publicly visible document, the principles and commitments to cybersecurity as a fundamental element to protect the business assets, for the purpose of achieving its goals and fulfilling its mission.

Recommendation 2: Cybersecurity shall be one of the declared areas of the organisation's risk management and control policy.

Recommendation 3: The organisation, taking into consideration the operational needs of the business and the risks that might affect achieving its goals, shall define short-, medium- and long-term plans that ensure the future vision and continuous improvement of cybersecurity, enabling it to reduce its exposure to risk within the defined tolerance levels.

Recommendation 4: Decisions on cybersecurity will be made according to the actual risk of the materialisation of threats to the organisation. A system for monitoring the efficiency and compliance with the defined security goals shall likewise be implemented.

Principle 3: Responsibility and organisation

Cybersecurity is a complex and cross-cutting discipline that affects all the activities of an organisation, so it requires suitable leadership and a structure that, in order to be properly implemented and managed, must in turn be made up of professionals with appropriate training and experience.

Recommendation 5: The organization shall aim to have at least one member of the management body with experience in cybersecurity management to support and validate the objectives prior to their approval by the management team.

Recommendation 6: The organisation shall have a unit that assumes the function of defining, driving and controlling cybersecurity, that participates in cybersecurity decision-making and strategy, and that ensures appropriate reporting of cybersecurity-related risks at the proper levels, as well as the necessary mechanisms to mitigate and control those risks.

This unit shall have sufficient material and human capacities and resources to achieve its goals, and shall report functionally to the management body, to one or more of its specialised committees, or to any other body or member of the organisation's senior management, provided that due independence is maintained with respect to those responsible for the network and information systems.

Recommendation 7: The head of this unit, the Chief Information Security Officer (hereinafter, CISO), shall be a person with the appropriate knowledge, experience and skills to perform this function, and shall have sufficient decision-making capacity and influence in the organisation.

Recommendation 8: There shall be a formally constituted cybersecurity committee in which, in addition to the CISO, an appropriate number of areas of the organisation will be represented in order to adopt any important resolution for information security that may substantially affect the organisation's activities.

Recommendation 9: Organisations, depending on their complexity and exposure to cyber risk, should take cybersecurity into consideration in at least one of their crisis committees.

Recommendation 10: The management body shall assign the executive supervision of cybersecurity management to one of its specialised committees (e.g. risk committee, audit committee).

Principle 4: Ethics and compliance

Cybersecurity governance shall include not only compliance with applicable regulations, but also **best practices in security and the ethical use of the organisation's resources**.

Recommendation 11: The management body shall understand the implications of best practices, among others, in the management of cybersecurity risks, both within its organization and in each of the markets in which it operates and in its relationship with the different stakeholders.

5.2 Management

Principle 5: Management model

Cybersecurity is a cross-cutting matter for the entire organisation and its business processes. Cybersecurity management should be guided by best practices and be suited to each organisation.

Recommendation 12: The organisation shall rely on recognised national, european or international standards, suited to its needs, in order to better monitor the evolution of its maturity.

Principle 6: Resourcing

Organisations should bear in mind that **the cybersecurity function requires constant and suitable resources** allocated to its maintenance and improvement.

Recommendation 13: The management body shall ensure that the unit in charge of cybersecurity management, as well as other units with responsibility to achieve the established goals, have sufficient material and human capacities to be able to carry out the assigned functions effectively and efficiently.

Principle 7: Managing incidents and resilience

One of the purposes sought by cybersecurity is to ensure the continuity of operational capability for the purposes of the organisation and the stakeholders that may be affected by its activities. This is known as **operational resilience** and as a result it is necessary to develop capabilities to contain and/or recover from cyber incidents.

Recommendation 14: It will be defined when an incident is considered significant, depending on the impact, the type of organization, its sector and the regulations to which it may be subject in the markets in which it operates.

Recommendation 15: The operating groups in charge of its management (both at technical, tactical and strategic level) shall be identified in order to minimise the impact on the business, and to ensure regulatory compliance and suitable internal/external communication.

Recommendation 16: Capabilities shall be available that allow the organisation to be resilient to ensure continuity of operations and full recovery of services within an appropriate timeframe, which shall be determined in the business continuity plan.

Principle 8: Training and awareness

All **the staff in the organisation need to have sufficient cybersecurity know-how** to deal with and mitigate the risk to which they are exposed[3].

> **Recommendation 17:** Management and the management body shall promote cybersecurity training, awareness and culture throughout the organisation in order to educate its staff on best practices and habits to prevent and mitigate cybersecurity risks.

Principle 9: Innovation and continuous improvement

Cybersecurity needs to adapt and improve in keeping with new and constant developments in technology and cyber threats.

> **Recommendation 18:** Cybersecurity management will be constantly improving and evolving to guarantee a suitable defence against threats.

5.3 Supervision

Principle 10: Cyber intelligence

Anticipation is a key element in protecting against any risk not only the organisation itself, but also the stakeholders who may be affected by its activities, so the organisation needs to rely on cyber intelligence as a basis to prepare for the management of cyber threats.

[3] People are the main asset available to organisations for suitable cybersecurity protection. At the same time, the main risks in this area often arise from incidents which, whether actively or passively, are generated by people

Recommendation 19: The cybersecurity committee shall inform management and the management body of cyber threats that might affect the organisation's goals. For this purpose, at least the main actors and the major and most recent cyber threats shall be taken into account, considering their potential impact on the organisation's operations.

Principle 11: Periodic reporting

Regular reporting of the organisation's cybersecurity situation to the organisation's governance bodies is among governance best practices according to international standards, and in some cases it is an obligation.

Recommendation 20: The management body shall regularly monitor cybersecurity by including this topic on the agenda of its meetings and/or those of its specialised committees where applicable (audit, risk, sustainability or other specific committees for the treatment of cybersecurity risk), for which it will require regular reporting of cybersecurity management to the executive responsible (Chief Information Security Officer - CISO). This reporting should take place periodically, and it is a best practice to report at least twice a year.

Recommendation 21: The periodic reporting should at least include the status of cybersecurity, the evolution of the degree of maturity and cyber risk, the evolution of threats, the allocation of resources for network and information systems security, significant incidents managed, if any, the status of security of supply chain operations dependent on third parties, as well as any relevant cybersecurity resolutions taken by the management team that may materially affect the organisation's activities. The Chief Information Security Officer - CISO - shall also report, if applicable, any obstacle or hindrance that might restrict the proper performance of their activity.

Recommendation 22: When a matter that may affect cybersecurity is on the agenda of the management body meetings, the cybersecurity implications of the matter must be discussed, for instance: major digital transformation initiatives, implementation of new technologies and major investments in technology assets, mergers and acquisitions, expansion of facilities, and major upgrades.

Principle 12: Continuity

Cybersecurity is part of an organisation's continuity strategy, and its testing it is essential to be properly prepared for cyber incidents.

Recommendation 23: The management body shall require the performance of comprehensive periodic tests in order to check the resilience mechanisms of the organization as part of the cybersecurity plans

In this context:

- Testing the business continuity plan as well as simulations and preparation exercises for crisis management committees should be conducted.
- In general terms, companies should systematically conduct effective drills and tests of the various protection, response and recovery measures.
- These exercises should involve the entire organisation, particularly focusing on the company's critical processes, also involving the supply chain.

Recommendation 24: The management body shall make sure that management supports the establishment, implementation, testing and continuous improvement of cyber resilience mechanisms.

Principle 13: Risk management

The proper management, assessment and communication of cybersecurity risk is a **key component of corporate risk management for any organisation**.

Recommendation 25: Independent assessments, with respect to the cybersecurity unit, shall be conducted at least once a year to enable the management body to obtain an additional and complementary view of the proper status of the cybersecurity risk management programme for the organisation's critical processes, including the supply chain.

6. GLOSSARY

A glossary is included below for a better understanding of the concepts covered in this Code:

Information asset: Any information or system related to the processing of information of value to the organisation. It can be business processes, data, applications, computer equipment, personnel, carriers of information, ancillary equipment or facilities. This information is susceptible to being attacked, whether deliberately or accidentally, with consequences for the organisation.

Cyber threat: A threat to systems and services present in cyberspace or reachable through cyberspace.

Cyber attack: A deliberate attempt by a cybercriminal to gain unauthorised access to a computer system by using various techniques and vulnerabilities in order to carry out activities for malicious purposes, such as theft of information, extortion of the owner or simply damaging the system.

Cyber intelligence: The discipline that allows processed information about the intent, opportunity and capability of malicious actors to be used in order to anticipate the most appropriate cybersecurity measures.

Cybersecurity: The ability of network and information systems to withstand, at a given level of reliability, any action compromising the availability, authenticity, integrity or confidentiality of the stored, transmitted or processed data, or the corresponding services offered by or accessible through such network and information systems. It comprises the combination of people, policies, processes and technologies employed by an organisation to protect its assets against cyber threats in order to achieve its goals and fulfil its mission.

Organisation: This term refers not only to the company itself but also to all the other entities within its group.

Cyber risk: An unfavourable circumstance that may occur and when it happens it has negative consequences on the assets, causing their unavailability, incorrect operation or loss of value. If this unfavourable circumstance occurs at the same time as a vulnerability or weakness in the systems, it can result in a security incident.

FORO
NACIONAL DE
CIBERSEGURIDAD

2023