IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 October 2022, accepted 16 November 2022, date of publication 18 November 2022,
date of current version 28 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223440

RESEARCH ARTICLE

CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels

MANUEL DOMÍNGUEZ-DORADO[1], JAVIER CARMONA-MURILLO[2], DAVID CORTÉS-POLO[3], AND FRANCISCO J. RODRÍGUEZ-PÉREZ[2]

[1]Department of Information Systems and Digital Toolkit, Public Business Entity Red.es., 28020 Madrid, Spain
[2]Department of Computing and Telematics Engineering, Universidad de Extremadura, 10003 Cáceres, Spain
[3]Department of Signal Theory and Communications and Telematics Systems and Computing, Rey Juan Carlos University, Móstoles, 28933 Madrid, Spain

Corresponding author: Manuel Domínguez-Dorado (manuel.dominguez@red.es)

This work was supported in part by Project TED2021-131699B-I00 and Project MCIN/AEI/10.13039/501100011033; in part by the European Union NextGenerationEU''/The Recovery, Transformation and Resilience Plan (PRTR); and in part by the Regional Government of Extremadura, Spain, under Grant GR21097.

ABSTRACT Currently different reference models are used to manage cybersecurity, although practically none are applicable ''as is'' to lower levels as they do not detail specific procedural aspects for them. However, they urge organizations to develop a methodological foundation to manage cybersecurity at those levels. Although they allow organizations to adhere to a recognized standard at the strategic level, this advantage vanishes when organizations must define specific low-level procedures, allowing the appearance of inconsistency at tactical and operational levels between departments of the same organization or between organizations. The design of these elements with the required holism and homogeneity is difficult, and this is why generic processes focused on getting certified regarding a standard are usually originated, but they are insufficient to obtain effective cybersecurity because they are not focused on dealing with real cyber threats. Because of the great responsibility of lower levels to achieve effective cybersecurity, this lack of methodological definition makes it difficult to adapt cybersecurity to the highly dynamic cyber context with the required holism and strategic alignment. Our proposal provides CyberTOMP, a process for managing cybersecurity at lower levels, as well as a set of methodological elements that support it. The novelty of these contributions is that they complement the strategic standard selected by the organization, providing it with a set of procedural elements ready to be used out of the box, contributing those aspects required by high-level frameworks to manage cybersecurity at lower levels, for which there is no alternative with a managerial approach.

INDEX TERMS Business asset, cybersecurity management, cybersecurity metrics, cyber threats, CyberTOMP, holistic cybersecurity, strategic alignment, tactical and operational cybersecurity, unity of action.

I. INTRODUCTION

Currently, various approaches to the security aspects of the digital world coexist. These strategies correspond to different organizations' digital evolution stages from decades ago to the present. Over time, the organizations' degree of digitization has increased, causing their most relevant assets at those moments to have been affected by a different threat context and, therefore, have required a specific risk analysis and a particular way of dealing with them. Depending on the specific stage, we can use an information technologies *(IT)* security approach [1], [2], an information security approach [3], [4], [5] or a cybersecurity approach [6], [7] among the main ones.

A. EVOLUTION TOWARDS A CYBERSECURITY APPROACH

Around the decades of the fifties and sixties, under an IT security approach, the most important organizations asset was the technology itself; this was a time when the cost of the first

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

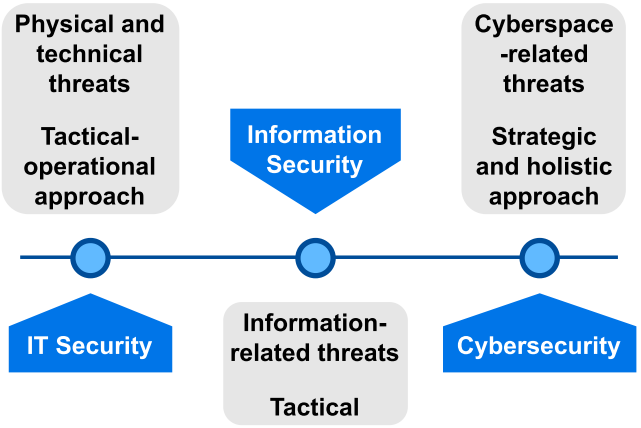


FIGURE 1. From IT security to Cybersecurity. Moving from a single-departmental approach to an organization-wide approach.

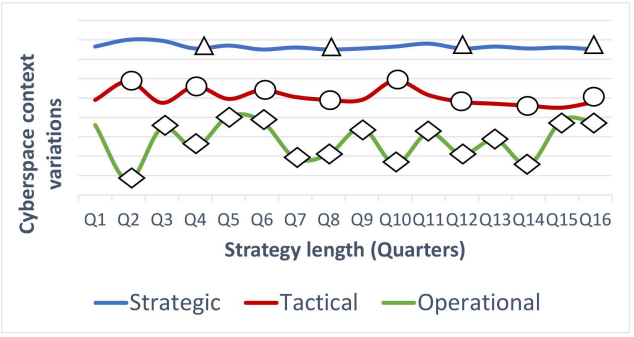


FIGURE 2. Cybersecurity checkpoints agenda at different levels during a four-years strategy. The tactical and operational levels must deal with the greatest variations of the cyber threats context. These variations are often hidden to higher levels due to the observation of variables that do not correctly reflect variations in the short and medium term.

mainframes constituted a large investment. The associated risks were mainly circumscribed to the technical and physical spheres and were addressed by most technical departments within the organizations. As information systems evolved, the value provided by the information increased, transforming it into a highly valued asset and forcing organizations to adapt their strategies towards an information security approach. Different departments that owned that information began to be involved in managing and handling the risks associated with it. They started to understand the threats that could affect the information and, by extension, the normal development of their own activities.

This paradigm has been prevailing for many years and is still used as the main approach in many organizations today. However, with the irruption of cyberspace, the information security approach has become insufficient. Cyberspace, understood as a set of interconnected information systems through communication networks in which people and entities interact and accomplish their activities, has unique characteristics: high dynamism; it is a common playing field where each organization controls only part of it; it has a high dependency on third parties; it requires the focus to be placed not so much or not only on information, but also on the continuity of business processes/assets; there is a need for cyber resilience, etc.

Parallel to the massive adoption of cyberspace, a set of specific threats has emerged that can potentially affect the capability of organizations to develop their activities, interact with third parties, and even preserve their image, reputation, and the trust vested in them. To deal with this evolution (fig. 1), with an increasing cyber threat context, the only approach to properly manage the current cyber risks and cyber threats is cybersecurity, mistakenly understood as information security synonymous on many occasions [8], [9]. This is not only because of cyberspace features but also because the greater digital dependency of organizations on cyberspace has brought to light new vital organizational assets, affected by cyber threats, which cannot be analyzed easily by employing an information security approach [10]: reputation, trust placed by third parties, people's physical integrity, supply chains, the organization's capabilities, Internet of Things *(IoT)* specific threats [11], etc.

Cybersecurity requires unity of action from the whole organization, leadership from strategic levels [12] and a high degree of holism [13], from its conception to its practical application, focusing on business assets [14]. It demands a proactive attitude that takes into account the response and recovery from cyber incidents as well as business continuity [15], aspects that must be managed throughout the entire life cycle, carefully considering the critical success factors to achieve effective cybersecurity [16].

B. RESPONSIBILITY OF TACTICAL AND OPERATIONAL LEVELS IN CYBERSECURITY

The main standards and reference models used for cybersecurity provide guidelines for its evaluation, although this is a high-level evaluation. This implies that variations in the state of cybersecurity can only be measured at the strategic level in the medium/long term. In scopes other than cybersecurity, assessing within such periodicity might be acceptable if the context is not very changing and significant corrective or adaptive actions are not frequently required. Under these circumstances, high-level assessments and corrections may be sufficient to maintain the state of the organization aligned with strategic goals.

However, this does not occur in the field of cybersecurity. Cyberspace and its associated cyber threat context evolve very dynamically, intensely, and frequently. For this reason, most corrective or adaptive actions, as well as the measurement of their effects, must be carried out in the medium/short term, that is, at tactical and operational levels within the organization. Thus, a large part of the responsibility for preserving the cybersecurity state aligned with an organization's cybersecurity strategy falls on them, who are also responsible for maintaining the unity of action and the holistic approach required by cybersecurity. Accomplishing these requirements from lower levels that are distributed

throughout the organization in several departments and areas that usually operate as silos and have different chains of command is very difficult.

Regrettably, the aforementioned standards and frameworks do not supply these levels, out of the box, with detailed methodological elements to help them manage and evaluate cybersecurity; neither do they provide standardized mechanisms to maintain the strategic alignment nor to quickly detect new cyber threats and nimbly apply the necessary actions to deal with them (fig. 2). Consequently, it cannot be taken for granted that these levels have the necessary mechanisms to carry out this work for the mere fact that the organization has adhered to a high-level standard in the strategic sphere.

C. CONTRIBUTIONS OF OUR WORK

From the current state-of-the-art, which we detail in later sections, needs are identified in the frameworks commonly used to manage cybersecurity. They are defined at a strategic, level and almost all urge organizations to develop a methodological base to be used in cybersecurity management at lower levels so that the cybersecurity strategy can be broken down and transferred correctly to the whole organization. As explained in the previous paragraphs, and we will expand on it in the article, we understand that the responsibility of these levels in the management of cybersecurity is relevant, but it encounters a series of challenges derived, on the one hand, from these aspects not covered by high-level frameworks and on the other hand by the structural rigidity of many organizations. Using any of the existing high-level frameworks, organizations can adhere to a widely recognized standard at the strategic level. But by having to define their own cybersecurity management process and procedures for the lower levels of the organization, this advantage, in a way, vanishes, inducing inconsistency between different organizations or even within different departments and functional areas of the same organization at tactical and operational levels.

Defining these elements is not always simple; it is almost never homogeneous and seldom consider cyber threats, but simply organizational aspects. On more occasions than is recommended, the difficulty in developing methodological elements for the tactical and operational levels leads to generic processes and procedures that are sufficient to obtain a certification with respect to the selected strategic framework, but insufficient to obtain effective cybersecurity.

Our work provides CyberTOMP as a means of managing cybersecurity at the tactical and operational levels, as well as a set of methodological elements, knowledge bases and concepts on which it is based. They are designed to complement the standard selected by the organization in the strategic sphere, providing it with a set of processes and procedures ready to be used out of the box. They contribute aspects required by the methodological guidelines of the high-level framework and by the organization to manage cybersecurity at tactical and operational level, levels for which there is no alternative with a managerial approach. Our proposal constitutes a procedural and methodological solution and not a technical one. Specifically, our proposal supplies lower levels with:

- Mechanisms to manage cybersecurity at tactical and operational levels, regardless of the higher-level standard or framework adopted by the organization, are thus a complement and not a disruptive element.
- A set of techniques and metrics focused on business assets to quantitatively and homogeneously assess cybersecurity, at different levels and degrees of aggregation.
- A homogeneous set of expected cybersecurity outcomes that arises from the analysis and combination of well-recognized international sources.
- The capability to maintain alignment with the cybersecurity strategy, under a holistic approach, from the tactical and operational levels, engaging all functional areas involved in the process.
- Procedures to incorporate the dynamic variations of the real cyber threats context, in an agile way, into cybersecurity daily grinds.

D. ORGANIZATION OF THIS DOCUMENT

The remainder of this work is organized as follows: in section II, the aspects found in the current state of the art that must be overcome to achieve effective cybersecurity management at low levels of the organization, are identified; in section III the methodological elements, knowledge bases and concepts developed in our proposal as support for the practical application of cybersecurity management at tactical and operational levels, are described; the section IV defines and describes in detail the CyberTOMP, our core contribution that, based on the rest of the elements detailed in section III, allows the organization to manage cybersecurity at tactical and operational levels; in this section recommendations and guidelines for its practical application are proposed as well.

II. STATE OF THE ART AND PROBLEM STATEMENT

From a theoretical perspective, the adoption of a cybersecurity approach does not have apparent complexity. However, based on the current standards commonly used for cybersecurity at a strategic level, there are different aspects that hinder its practical adoption in organizations when it is applied from lower levels, especially considering the differentiating characteristics of cybersecurity with respect to previous approaches and the need to change the way it is addressed [17]. In the following subsections we identify the current problems that our proposal addresses.

A. LACK OF HIGH-LEVEL STANDARDS THAT PROVIDE PROCEDURAL ELEMENTS FOR TACTICAL AND OPERATIONAL LEVELS

There are many frameworks and standards that can be useful, in certain cases, to manage cybersecurity [18], which sometimes makes it difficult to choose one and implement it in organizations [19]. A large number of them, such

as Capability Maturiry Model Integration *(CMMI)* [20], [21], [22] or Information Technology Infrastructure Library *(ITIL)* [23], [24] are generic and applicable to multiple spheres. When applied to cybersecurity, they can contribute to managing it. Some even contain elements related to security in the digital field [25]. However, they are, in no case, specific models for cybersecurity, so their advantages are very limited in this regard [26], in addition to being defined at a very high level [27].

Other frameworks and standards are focused on information security management, not on cybersecurity, for instance, the ISO 27000 family of standards [28], [29], the Model of Indicators for the Improvement of Cyber Resilience *(IMC)* [30], [31] or even the Spanish National Security Scheme *(ENS)* [32], [33], [34], [35]. They are commonly used to address cybersecurity, although they are based on or bear a clear perspective of information security and do not properly cover the specific aspects of the cybernetic context; therefore, they do not allow, *per se*, meeting the requirements of a cybersecurity model.

To conclude, there are other works, such as the one developed by MITRE in the Adversarial Tactics, Techniques and Common Knowledge matrix *(ATT&CK©)* [36], [37] (used in various works on threat intelligence [38], [39]), the Critical Security Controls for Effective Cyber Defense *(CSC)* [40], [41] from the Center for Internet Security *(CIS)*, even with its shortcomings [42], the Open Web Application Security Project *(OWASP)* Top 10 project [43], [44], the Community Defense Model *(CDM)* [45] from the CIS, that aligns the CSC to cover the threats documented by MITRE, helping to implement the mitigations that it proposes [46] or those known as nine D's of cybersecurity described in [47] (so called because they are recommendations that all begin with this letter). All of them are sets of recommendations, good practices and specific tools for cybersecurity, which are very useful but disconnected from a comprehensive framework that covers all organizations' levels.

Among the analyzed models, the Framework for Improving Critical Infrastructure Cybersecurity [48], [49], from the National Institute of Standards and Technology *(NIST)* stands out. It is a complete framework for cybersecurity that is accompanied by the SP-800 series of guides [50] (where guide SP-800-53 [51] can be especially highlighted), which provides the organization with high levels of cyber resilience under a cybersecurity approach. This framework in conjunction with the Cybersecurity Maturity Model *(CMM)* [52], [53] also allows the evaluation of third parties that must be part of the organization's supply chain. There are other less common models as, for example, the one developed in [54], [55] which focuses on the managerial aspects of cybersecurity to protect critical infrastructure. It is defined at a very high level of abstraction and does not provide procedural elements for direct application. However, it provides a modern view that cybersecurity is not only related to technical domains but also involves the whole organization.

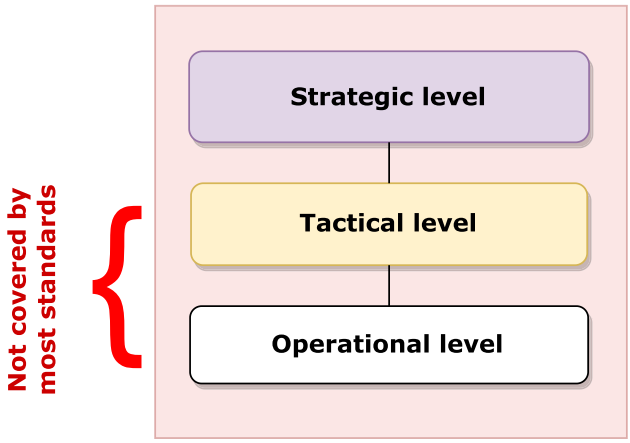


FIGURE 3. It is necessary to provide the tactical and operational levels with homogeneous methodological tools for cybersecurity management.

There are published works that focus on cybersecurity very applied to specific and particular cases. A deeper literature review and an analysis of the body of knowledge in the field of cybersecurity can be found in [56], [57], [58], [59], [60], and [61], for general cases and also specific ones. They generally follow technical approaches that do not address organizational cybersecurity from a procedural perspective. But it is also important to study the problem from the managerial point of view within the current standards and new contributions such as the one we will describe in this paper.

Nevertheless, none of these frameworks or initiatives, and even the NIST framework, includes a detailed methodological description of how cybersecurity should be managed at the organization's tactical/operational levels. This means that none of them are applicable without being complemented, since cybersecurity must be administered on many occasions from these levels (fig. 3). It is the responsibility of each organization to design the set of processes and procedures indicated by these frameworks for their lower levels.

By not including specific standardized guidelines, the tactical/operational application of these models can be completely different between organizations, between areas within the same organization, or it cannot even take place.

There are several factors why an organization could choose to use them even though they are not fully defined options to address cybersecurity at all levels of the organization: because they are certifiable standards that allow positioning against competitors, because they are widespread and finding workers trained in them is easier, because they are required by third parties to access contracts, or because they are mandatory rules according to the legal framework surrounding the organization. For these reasons, replacing these frameworks in the organization is not always an option, but they should be complemented to provide them with what they lack. They should be provided with methodological elements that apply at the

lowest levels to address the deficiencies in this area. Hence, it is necessary to provide tactical and operational levels with homogeneous cybersecurity management mechanisms that allow them to adapt to the cyber threat context and maintain alignment with the strategic cybersecurity objectives.

In [62], a use case in Portugal for the implementation of information security actions in a group of SMEs was explained in detail. Some aspects of this work are similar to those adopted in our proposal: a set of information security controls from a recognized standard, which have been grouped into different groups of controls to respond to different needs. Subsequently, the characterization of each control depends on the type of organization and other aspects.

However, this very well-prepared work has, in our opinion, some limitations. It is based on the ISO 27001 standard, a standard for information security and not for cybersecurity. At the procedural level, it does not detail the elements of management, processes and procedures used at tactical and operational levels to coordinate the efforts of the organization's workforce. This is most likely because their destination is small and medium-sized companies, where this distinction between levels makes perhaps less sense.

Paraphrasing the conclusions of the authors of this work: *However, ISO-27001:2013 is a single tool for achieving the project goal and it can be seen as a limitation in this study. In that sense, other best practices and frameworks should be addressed, implemented, and compared.*

In our work, we present a wider solution based on several standards and initiatives specific to cybersecurity and not information security. It also contributes the required processes, procedures and metrics to be used out of the box that can be applied to tactical and operational levels.

B. LACK OF MECHANISMS TO PROVIDE HOLISM FROM LOWER LEVELS

Cybersecurity requires something that, until now, none of the previous approaches related to digital security required [63]: a holistic approach, promotion from the strategic levels to the whole organization, unity of action to address cybersecurity risks, and proactive mindset and focus on cyber incident response and recovery tasks.

Since a large part of the initiative in cybersecurity must be driven at tactical and operational levels, the interdepartmental coordination required to provide a holistic approach must also be addressed from these levels.

Notwithstanding, the areas or units that compose these levels do not have direct visibility, communication, and coordination between them, and usually work under different chains of command in isolated silos. Habitual conflict escalation mechanisms are useful for inter-area communication in specific situations, but not for managing the daily grinds at lower levels. Under these circumstances, it is difficult for lower levels to achieve the coordination, unity of action, and holistic and proactive vision required by cybersecurity (fig. 4).

This situation is amplified when the organization is more distributed in silos. In any event, this communication is

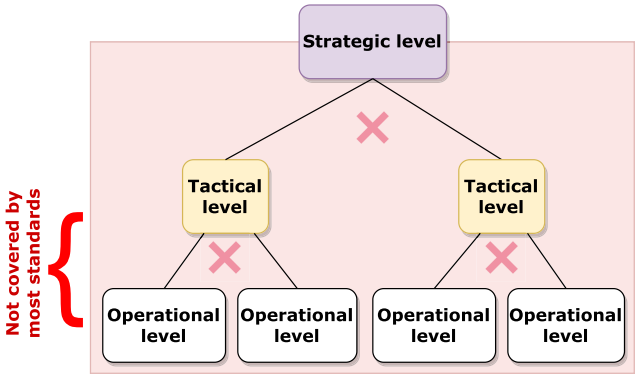


FIGURE 4. The distribution of the organization in silos hinders a fluent communication and collaboration between functional units and the achievement of the holism and unity of action required by a cybersecurity approach.

fundamental because people from different functional areas of the organization must agree on the actions they have to implement, on the metrics that will affect them, on the weight and responsibility that each one will have with respect to the cybersecurity of business assets, and so on. This should not be done independently but jointly, coordinated, taking advantage of existing synergies and forming a team.

For these reasons, it is necessary to provide these levels with tools that ensure that they can design and execute joint cybersecurity actions proactively, quickly, with holistic vision and unity of action; avoiding the appearance of conflicts despite the distribution of teammates among several functional areas.

C. LACK OF HOMOGENEOUS CYBERSECURITY EVALUATION CRITERIA

What has not been measured cannot be improved. This statement, extrapolated to cybersecurity, implies the need to evaluate the effectiveness of cybersecurity controls [64] and safeguards, from a holistic and multidisciplinary perspective, and offer a shared vision of the organization's cybersecurity posture.

When people from different functional areas collaborate to ensure the cybersecurity status of business assets and meet strategic cybersecurity objectives, there is a need to measure progress [65] because this allows continuous decision-making at different levels [66], [67]. But current standards and frameworks define neither measurement mechanisms nor assessment criteria that can be used by tactical and operational levels to fit this need, aspects with which all the parties should agree, and that allow focusing on solutions and not on resolving the differences around the assessment process itself. Otherwise, several discrepancies and conflicts will tend to arise between the areas co-responsible for cybersecurity, which prevents having a clear vision of their real cybersecurity state.

When different organization units, follow non-identical assessment criteria to evaluate the same element

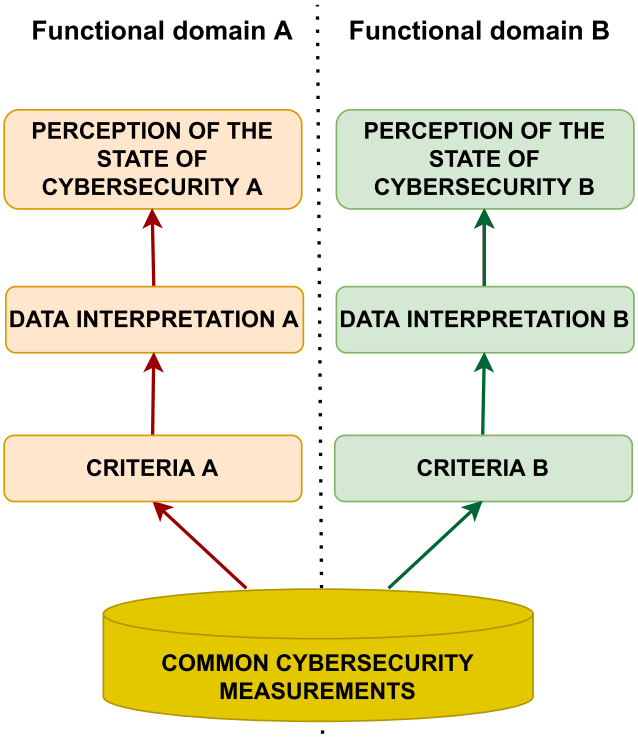


FIGURE 5. Silos in organizations frequently imply the existence of different criteria and disjointed interpretations of the real state of cybersecurity, even when the same data is valued. A common standard should be defined for the evaluation of cybersecurity at these levels.

(cybersecurity in this case), it is likely that none of these evaluations coincide with the rest (fig. 5) unless they share a common vision, which is a common way of interpreting the measurements, leading to a lack of coordination in cybersecurity due to different perceptions. For these reasons, it is necessary to have standardized and homogeneous tools that provide a common shared measurement of the performance and state of cybersecurity at these levels, and also allow quantitative evaluation of the effectiveness of the implemented actions for decision-making in the short and middle terms.

III. TOOLKIT TO SUPPORT CYBERSECURITY MANAGEMENT FROM TACTICAL-OPERATIONAL LEVELS

After a review of models and initiatives commonly used to manage cybersecurity, we designed a proposal that combines the existing elements that may be useful for the purpose of our work with other specific elements designed in our study that complete it to address all the needs identified in Section II. We have always tried that our solution consists of an evolution or a combination of fundamentals already consolidated and accepted, and not of a theoretically excellent proposal but difficult to run in practice by any organization. In addition, special emphasis has been placed on keeping the solution limited to management at lower levels (tactical/operational), assuming that the organization will have specific frameworks for managing at higher levels (strategic/tactical), although

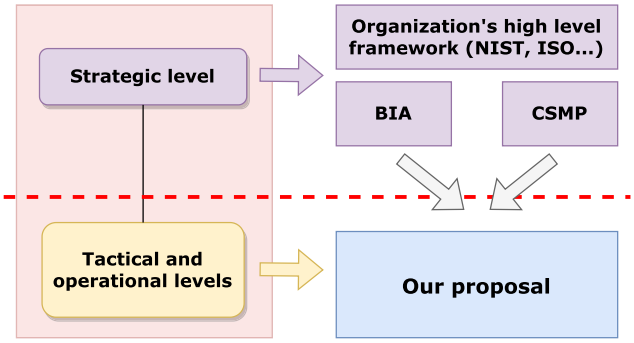


FIGURE 6. BIA and CSMP, both slightly modified, connect the organization's strategic framework to our proposal for tactical and operational levels.

perhaps they may not be appropriate "as is" for cybersecurity management, as explained in Section II.

In the following paragraphs, every decision and auxiliary solution that makes up our proposal will be discussed, justifying the reasons for it.

A. CONNECTING OUR PROPOSAL WITH THE CORPORATE STRATEGY

In our proposal, we chose to minimize the dependence on the high-level framework used at the strategic level to ensure its applicability in different organizations while guaranteeing that it serves as a cybersecurity management tool at tactical and operational levels of the organization and maintain alignment with the corporate strategy from these levels. However, a method is needed to connect and align the activity of lower levels towards the strategy. For this, we propose to use two elements present in almost any medium-sized organization, regardless of the regulatory framework to which they have adhered: the Business Impact Analysis *(BIA)* and the Cybersecurity Master Plan *(CSMP)*, or the set of cybersecurity projects, if applicable, that come from the application of the framework used at strategic levels (fig. 6).

1) BIA REQUIREMENTS FOR ASSET FOCUS AND BUSINESS CONTINUITY

The concept of business continuity refers to the ability of an organization to identify threats that can become disruptive events that affect its activity, and plan the response and recovery in advance to guarantee the normal development of business activities [68], [69]. The greater this capacity, the more resilient is the company.

It is not a new concept, nor is it solely focused on cybersecurity. An entity could be affected by multiple events; some recent events such as the lock-down suffered by the COVID-19 pandemic, but also natural disasters, labor conflicts, lack of qualified workers, events linked to information security, or cybersecurity incidents.

The requirements for cybersecurity are in many ways similar to the requirements for ensuring business continuity: holistic view; impulse from the strategic level to the entire

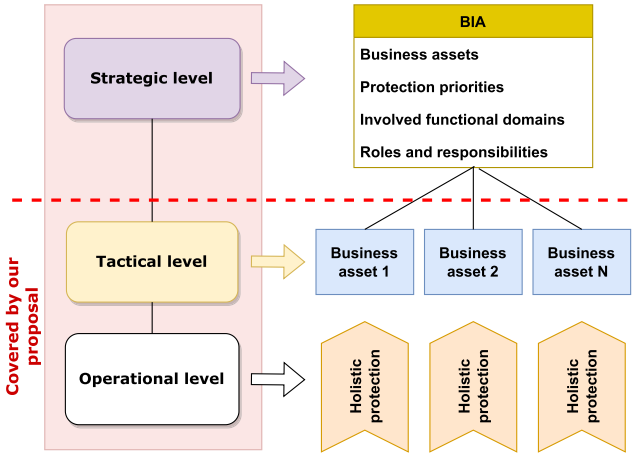


FIGURE 7. Using the BIA to connect the strategic level to the lower ones provides this proposal with the capability of integrating cybersecurity-related business continuity requirements and a focus on the business assets in the daily cybersecurity grinds.

organization; unity of action in crisis management; proactive approach; development of plans to respond and recover in the face of different situations and actions that reduce the impact when crises break out. Therefore, with organizations making massive use of cyberspace and with a great dependence on this medium, cybersecurity, correctly put into practice, contributes significantly to business continuity in crisis situations caused by cybersecurity incidents [70].

In their business continuity management, it is common for organizations to carry out the BIA [71], generating a document in which the organization details aspects such as the critical business processes, the assets on which these processes depend, the criticality of each one, the maximum tolerable interruption times, or the tolerable recovery times. The BIA is, therefore, a strategic declaration of intent coming from the highest level of the organization, where it is evaluated and indicated which assets to protect (and recover, where appropriate) and with what intensity, to ensure that the impact of a crisis on the overall business is as small as possible. It is also common for BIA to define roles, responsibilities, strategies, communication mechanisms, etc. for all areas, and for cybersecurity.

Our proposal provides mechanisms that allow organizations to align cybersecurity with business continuity requirements, as the maximum expression of the organization's survival needs. In particular, at tactical and operational levels, which are often the executors of recovery actions. However, business continuity associated with cybersecurity, expressed as a whole, is difficult to understand at operational and tactical levels. It is too broad and difficult to manage and, therefore, difficult to understand, communicate, and plan at those levels. For this reason, the first decision in our proposal is the application of the "divide and conquer" paradigm to have a smaller and more manageable scope at such levels. In addition, it is more understandable, allowing greater cohesion between the multidisciplinary and holistic operational team in charge of its cybersecurity and continuity.

Since the BIA identifies and prioritizes the business assets that support the organization's activity, we propose focusing cybersecurity efforts on them [72] and assign them as a basic unit at the tactical and operational levels for their cyber protection, understanding that this element is sufficiently manageable at these levels.

Each organization develops a BIA according to its needs, although it is common for a BIA to include information relevant to the business. Nevertheless, to provide it with the utility intended in this work, the BIA must include at least:

- Identification of business assets.
- Functional areas responsible for business assets and those that depend on their results.
- Continuity strategies for different crisis scenarios.
- The parameters in which business assets can be discontinued without generating a disproportionate impact, and therefore, the levels of this discontinuity acceptable to the organization.
- The impact on the business in the event of a discontinuity that extends beyond the parameters considered acceptable by the organization.
- A map of high-level dependencies between the different business assets.
- Based on the above, prioritization that reflects the protection required by business assets. On a scale of three values, LOW, MEDIUM, and HIGH.

In this way in our proposal, the BIA becomes one of the two points of interconnection between the strategic area of the organization and the rest of the lower levels (fig. 7). This provides the following four main strengths for cybersecurity:

- This allows for a more manageable and understandable scope for lower levels of the organization.
- Allows maintaining the focus on the business asset and its derivative assets.
- It allows the integration of business continuity strategies related to cybersecurity in daily activity.
- It allows the incorporation of the risk-based approach (related to business continuity) [73], [74] so that business cyber continuity risk requirements can be introduced in the tactical and operational cybersecurity management cycle.

2) CSMP REQUIREMENTS FOR A STRATEGIC ALIGNMENT

CSMP is a tool commonly used by cybersecurity managers to orchestrate all the needs and context of cybersecurity in a portfolio of cybersecurity programs and projects aligned with the needs of the organization. In this way, the cybersecurity effort and the necessary budget are focused on achieving the organization's strategic cybersecurity objectives and, by extension, the company's business goals.

The design of CSMP includes systematic phases so that it covers all aspects of cybersecurity in an integral way, which allows focusing and optimizing resources to achieve the interests of the company in this area. It includes, among many other aspects, cybersecurity guidelines; strategic

cybersecurity objectives; the definition of high-level cybersecurity controls and safeguards; the definition of cybersecurity architecture, covering all areas where cybersecurity is applicable; the definition of roles, responsibilities, processes, and procedures; the quantification of expenses and investments in cybersecurity, and the high-level planning of cybersecurity actions/projects. This allows an incremental development of the cybersecurity strategy and the achievement of short, medium and long-term goals. From all of the above, which represents a high-level comprehensive plan for cybersecurity management throughout the organization, we would like to emphasize that it is in this CSMP that the framework and regulatory framework related to cybersecurity are defined and the cybersecurity projects required by the organization, as well as the strategic cybersecurity objectives and the specific objectives of each designed project.

Theoretically, CSMP is an optimal tool for providing cybersecurity with a comprehensive vision. However, and this is relevant, during the preparation of this plan, the strategic framework that the organization will use for the direction and management of cybersecurity must be defined, as well as the associated processes and procedures. But if the execution of the CSMP depends on any of the main existing frameworks ''as is'', the problem described in the section II resurfaces, since practically all of the high-level frameworks and standards do not provide methodological tools applicable to tactical and operational levels and focus mainly on the strategic levels; so that even with a CSMP, organizations must develop their processes and procedures to manage cybersecurity at the tactical and operational level. Most of these high-level frameworks indicate that this methodological base should be developed. And this is precisely what our proposal provides. Our proposal can be used to complete the methodological guidelines of high-level frameworks and can be included in the CSMP to be used in cybersecurity management at the tactical and operational levels of the organization.

In our solution, the use of CSMP is proposed as a second point of connection with the strategic level of the organization (fig. 8). To do this, CSMP projects, or cybersecurity projects in the event that there is no properly defined CSMP, must meet certain requirements:

- Every business assets must have their own project in the CSMP. A project may cover more than one asset if its cybersecurity objectives coincide with others.
- These projects must be defined at a high level and specify the objective, but not detail the tactical/operational actions, so that rolling wave planning can be carried out [79] at lower levels as information from the context analysis becomes available. The planning of CSMP projects is therefore simplified.
- The objectives of the indicated projects must be defined based on the cybersecurity metrics and indicators described in our proposal, as developed later in this section.

Building the CSMP as described in our proposal provides four main benefits:

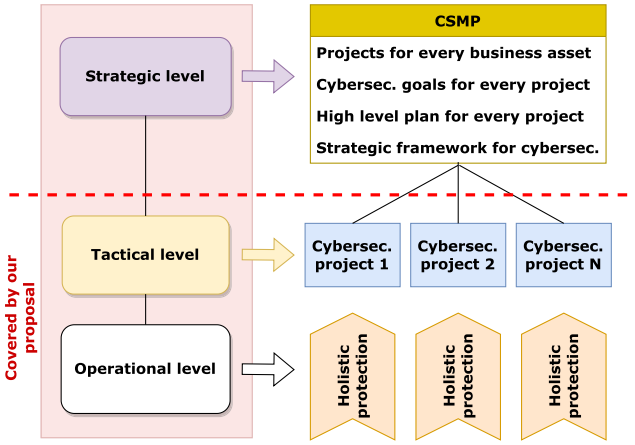


FIGURE 8. Using the CSMP to connect the strategic level to the lower ones provides this proposal with the capability of integrating cybersecurity risks and cybersecurity strategic goals in low levels' activities.

- It allows for more manageable and understandable cybersecurity projects for lower levels of the organization.
- Allows maintaining focus on strategic objectives for business assets and their derivative assets.
- It allows alignment towards the cybersecurity strategy in the daily activity of its management from the lower levels.
- It allows the incorporation of the risk-based approach (related to cybersecurity) [75], [76], [77], [78], so that cybersecurity risks requirements can be introduced in the tactical and operational cybersecurity management cycle.

B. CYBERSECURITY FUNCTIONS FOR BUSINESS ASSETS

With the use of BIA and CSMP as described in our proposal, a multidisciplinary operational team in charge of the cybersecurity of a certain business asset would have a manageable scope. Even so, in our work we propose to make this scope even more manageable to further increase its understanding and facilitate the evaluation of its cybersecurity state. Among the frameworks reviewed in Section II, the most complete and focused on cybersecurity is the NIST cybersecurity framework, which organizes different cybersecurity safeguards in a tree-like manner, very useful, in continuous security functions, categories, and subcategories. The functions provide a high-level strategic view of the cybersecurity risk management process life cycle and their subsequent breakdown into categories, and sub-categories brings this strategic view closer to the tactical and operational levels:

1) **Identify**. This function enables a greater understanding of organization's context to focus and prioritize its efforts in accordance with the risk management strategy and its needs.
2) **Protect**. The purpose is to develop and implement appropriate safeguards and controls to ensure the delivery of critical services. This is the basis for the

subsequent limitation or containment of the impact of a possible cybersecurity incident.

3) **Detect**. The purpose is to develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4) **Respond**. The purpose purpose is to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. It allows, among other aspects, containing the impact of cybersecurity incidents.
5) **Recover**. Its purpose is to develop and implement appropriate activities to maintain resilience plans and recover any capacity or service affected by a cybersecurity incident. Allows the recovery of the usual activities of the organization.

This functional classification is easily understandable and, following it, a tactical/operational team could focus on different aspects of the cybersecurity of the business asset, which could also be evaluated separately. The identification of specific responsibilities of each functional area of cybersecurity is facilitated and favors the creation of specialized operational subgroups in each of the functions, categories or subcategories. In addition, the ''Response'' and ''Recovery'' functions are closely linked to business continuity and cyber resilience, so they fit very well in cybersecurity focused on business assets from the BIA, as indicated in our proposal.

The subcategories (expected outcomes) and categories defined within the NIST framework [48] contribute hierarchically to the achievement of the objectives of each function on which they depend. Each is traceable to the most relevant regulatory frameworks and initiatives, such as CIS CSC, NIST SP 800-53, ISO 27001, which facilitates coexistence with these standards.

Therefore, we have considered it convenient to reuse this classification in functions, categories, and subcategories in our proposal. The NIST framework will not be used in most strategic aspects in order four our proposal to remain independent of the higher level regulatory framework used in the organization: NIST, CMMI, ISO 27001, ENS, etc.

In the rest of our proposal, it is considered that any activity carried out by tactical and operational teams for the cybersecurity of a business asset must be included in one of the defined cybersecurity functions or in its derived hierarchy.

C. UNIFIED LIST OF EXPECTED OUTCOMES FOR THE CYBERSECURITY OF BUSINESS ASSETS

The finest grain level of the NIST classification is a subcategory. In that model they are also called ''expected outcomes'' which is very appropriate because it reflects that these subcategories are the goals, which are achieved with the operational implementation of the corresponding controls and safeguards. In our proposal, we reuse the NIST definition of ''expected outcomes'' since implicitly this denomination is a proactive requirement for the teams in charge of executing cybersecurity actions, an aspect that we consider essential for modern cybersecurity.

However, the expected outcomes from the NIST framework are not the only source of relevant information clearly focused on cybersecurity, and being a fairly broad set, it is true that it is not updated very frequently. There are other sources that are either updated more frequently or simply supplement NIST's set of expected outcomes. For example, in [36], MITRE identifies cyberattacks observed in the real world and the tactics, techniques, and procedures followed by cyber attackers to carry them out: the *modus operandi*. The main mitigation actions for each case are solso defined. In [40], the CIS details the most critical cybersecurity controls that should be implemented in any organization. For this, it uses what it calls the ''Implementation Group'' (IG), numbered from 1 to 3. IGs are a way to identify groups of controls that need to be implemented together to address existing threats. IG1 controls, once implemented, allow for dealing with a wide variety of cyber threats. The IG2 controls include those from IG1, and the IG3 controls include all. Consequently, depending on the context of the organization and the protection needs it requires, it must implement IG1, IG2, or IG3 controls. IG3 is the most complete and allows for a higher level of cybersecurity against the most complex threats (it also includes the most complex and costly controls). The CIS itself, in [45], calculates the level of coverage of the threats identified by MITRE after the implementation of the different IGs, ranging from 77% of threats in the worst case by implementing IG1 to 95% in the best case, implementing IG3; a relevant coverage in any of the cases. Finally, in [47], a series of recommendations are defined, which are applicable to any cybersecurity scenario and can be very useful for minimizing exposure to cyber threats: the nine D's of cybersecurity.

As expected outcomes will determine what cybersecurity actions operational teams need to take, we consider it essential in our proposal to have an expanded list of expected outcomes that brings together not only information from the NIST framework but also from the cited sources. That is why we have approached this task by thoroughly analyzing these sources and integrating them into a Unified List of Expected Outcomes (ULEO) that:

- Retains the same classification of functions, categories, and subcategories as NIST.
- Groups the expected outcomes in the same implementation groups defined by the CIS, with the same meaning.
- Expands the focus and number of original expected outcomes from the NIST model, including inputs from other complementary or more up-to-date sources.
- Maintains alignment with the work of MITRE, so that the application of each IG allows addressing a certain percentage of cyber threats observed in the real world.

When building the ULEO we have been especially careful in the process of integrating controls from other cybersecurity initiatives, to ensure that this range of threat coverage is not altered downwards. In all cases, stricter controls than those proposed by the NIST have been added or replaced by more extensive controls, but in no case the controls were

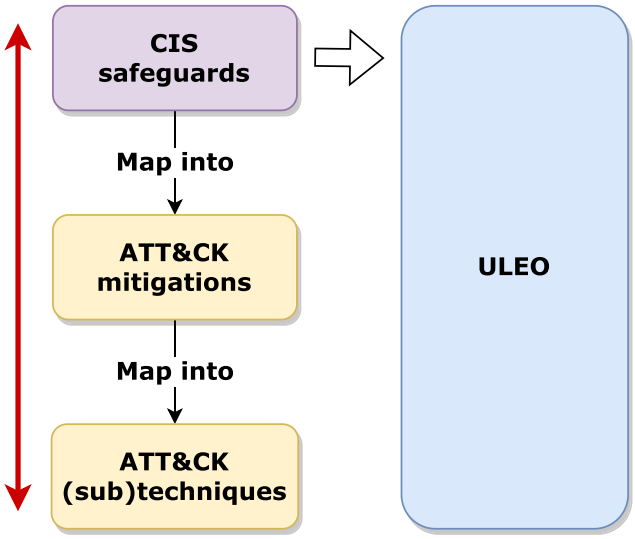


FIGURE 9. Our proposal indirectly incorporates the mitigations and TTPs of MITRE to the ULEO through the inclusion of the corresponding CIS safeguards.

relaxed, which is the reason why these ranges of coverage can be ensured. Therefore, the proposed method maintains or improves the coverage percentages calculated by the CIS in [45].

The following subsections define ULEO and describe the process followed for its analysis and construction.

1) PHASE I. FUSION OF MITRE RECOMMENDATIONS WITH CIS CONTROLS AND NIST SUBCATEGORIES. CREATION OF INITIAL ULEO

The starting point for the construction of ULEO in our proposal is the complete set of functions, categories, and subcategories defined in the NIST framework.

Our proposal does not directly include the mitigations identified by MITRE to address the cyberattacks documented in the ATT&CK©matrix. In [45], the CIS does an excellent job analyzing in depth which of its controls and safeguards allow the implementation of the necessary mitigations to face the Tactics, Techniques and Procedures *(TTPs)* employed in the cyberattacks documented by MITRE. These requirements were grouped into each of the three IGs used in our study. Thus, in our proposal we take advantage of this effort by including the CSCs from CIS which also allows us to indirectly include the needs and requirements identified by MITRE (fig. 9).

In [80], the CIS performed a comparative analysis of the equivalence between the expected outcomes from NIST and CIS CSCs. In our proposal we have taken this initial comparative analysis as a basis, which does not merge elements but rather identifies them, to make the first combination of the expected outcomes of the NIST and CIS CSCs, as follows:

1) Cases where a CIS control or safeguard does not have a related NIST subcategory. In this case, we have that control or safeguard to the list, considering that it complements the NIST model itself, covering cases that it did not consider.
2) Cases where a CIS control or safeguard further defines and completes a similar subcategory within the NIST framework. In this case, we replaced the NIST subcategory with CIS control or safeguard that addresses the same problem, but with greater completeness.
3) Cases in which CIS control or safeguard is defined in less detail and completes a similar subcategory within the NIST framework. In this case, we have maintained the NIST subcategory, ignoring CIS controls or safeguards that address the same problem but with less completeness than NIST.
4) Cases in which CIS controls or safeguards equivalently define a similar subcategory within the NIST framework. In this case, we chose to maintain the NIST subcategory as it addresses the same problem under equal conditions. Choosing an equivalent CIS control or safeguard would not have added or subtracted anything.
5) Cases in which a CIS control or safeguard partially defines a NIST subcategory and vice versa; that is, both NIST and CIS address the same problem, but neither of them does so completely, rather they intersect. In this case, we included both the NIST subcategory and the CIS control or safeguard because both offer a better response to the same problem than either of the two separately.
6) Cases in which a NIST subcategory does not have an equivalent CIS control or safeguard; that is, it is something that only exists within the NIST framework and not within the CIS framework. In this case, we maintained this NIST subcategory because we understand that it provides a security plus.

The previous combination was carried out by analyzing each control, safeguard, and expected outcome, one by one, to identify, after an analysis of the textual description of each item, to which NIST function, category, and subcategory it belonged. In addition, to determine the implementation group it should be placed in. The result of this process is the first version of ULEO.

2) PHASE II. INCORPORATION OF THE NINE D's OF CYBERSECURITY TO THE ULEO

The nine D's of cybersecurity are textual recommendations that lack a classification system. Therefore, in the first place, we have provided each of them with a code that can be shown in Table 1, similar to the functions, categories, and subcategories of the NIST or the controls and safeguards of the CIS in their respective models. We assimilate each of them at the level of a subcategory or expected outcome.

Subsequently, the textual descriptions of each of them were analyzed in the same way that was done with the CSCs of CIS, to identify which function or category of cybersecurity they contribute to. The nine D's of cybersecurity were systematically analyzed with respect to the controls,

TABLE 1. Identifiers assignment for the nine D's of cybersecurity.

ID	Description
9D-1	Deter attacks
9D-2	Detect attacks
9D-3	Drive up difficulty
9D-4	Differentiate protections
9D-5	Dig beneath the threat
9D-6	Diffuse protection throughout the payload
9D-7	Distract with decoys
9D-8	Divert attackers to other targets
9D-9	Depth of defense

safeguards, and subcategories of the initial ULEO previously generated, so that:

1) Cases in which a D does not have a related subcategory in the initial ULEO. We choose to add such D considering that it complements the set.
2) Cases in which a D defines a subcategory of the initial ULEO in a more detailed and complete manner. We decided to replace it with that D which addresses the same problem, but with greater completeness.
3) Cases in which a D defines a subcategory of the initial ULEO in a less detailed or complete manner. We choose to retain this subcategory and not include this D because it addresses the same problem in less depth or detail.
4) Cases in which a D defines a subcategory of the initial ULEO with the same level of detail and depth. We choose to retain this subcategory because they address the same problem under equal conditions. Choosing an equivalent D does not add or subtract anything.
5) Cases in which a D partially defines the same case as a subcategory of the initial ULEO and vice versa, that is, both cases address the same problem, but neither of them does so completely, rather they intersect. In this case, we included both the previously existing subcategory in the initial ULEO and the corresponding D because both offer a better answer to the same problem than either of them separately.
6) Cases in which a subcategory of the initial ULEO does not have an equivalent D, that is, it is something that exists only in the initial ULEO and not in [47]. In this case, we maintained this subcategory because we understood it provides a plus of security.

After this combination, we finished the inclusion of all the intended information in the ULEO: expected outcomes from NIST, controls and safeguards from CIS, the nine D's of cybersecurity, and, indirectly, mitigations from MITRE.

3) PHASE III. FILTERING AND GENERATION OF THE FINAL ULEO

After the two previous phases, the resulting ULEO contained redundant expected outcomes, whose only difference was the application in different IGs, an example of which is shown in Table 2. To remediate this redundancy, we performed a cleaning process consisting of consolidating these redundancies into a single expected outcome, leaving a single appearance that will apply to these IGs. In Table 3 the result of redundancy removal for the case presented in Table 2, can be shown.

TABLE 2. Example of redundant expected outcomes that apply to different IGs.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.AM	ID.AM-1	✓	✓	✓
Identify	ID.AM	ID.AM-1		✓	✓
Identify	ID.AM	ID.AM-1			✓

TABLE 3. Example of redundancy reduction.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.AM	ID.AM-1	✓	✓	✓

The final ULEO was obtained by repeating this process. It incorporates a total of 169 expected outcomes organized in the same functions and categories used by the NIST framework, but keeping traceability to MITRE mitigations while including information from the nine D's of cybersecurity and the CIS CSCs. In Appendix V, Tables 4 to 26 show the ULEO for each function and category. The expected outcomes are referenced by their code, being those that begin with 'CSC' those from the set of CSCs from CIS; those that start with '9D' those corresponding to the nine Ds of cybersecurity as indicated in the Table 1 and the rest, the original of the NIST framework.

4) ULEO BENEFITS

The ULEO we have built provides several advantages to the solution we propose:

- It classifies the expected outcomes into three IGs, following the same approach that the CIS uses for its critical controls. In practice, this allows to obtain three different sets of expected outcomes applicable to three different scenarios where the cybersecurity needs are LOW, MEDIUM, or HIGH.
- As it has been built, it incorporates the best recommendations of the NIST, the CIS, and the 9 D's of cybersecurity, eliminating the existing redundancies between them. It also brings together the best of each approach: security functions (and their division into categories and subcategories), IGs, etc. Moreover, based on the unified list of expected results of the NIST Cybersecurity Framework, not only cybersecurity controls are

considered in our proposal, but also the main controls related to privacy, closely linked, as detailed in [81].
- The expected outcomes of each implementation group allow for effective cyber defense against the TTPs documented by MITRE (and associated cyber threats).
- Its hierarchical arrangement allows the state of cybersecurity to be evaluated with different granularity and to easily identify which aspects must be improved to achieve the expected outcomes.
- Although our proposal should not be understood as a cyber-incident management process, it helps to deal with cyber-incidents by facilitating to the organization to acquire the skills and elements necessary for it, as a consequence of the implementation of the expected results of the functions ''Detect'' and ''Respond'' of the ULEO.
- The mere use of ULEO makes it possible to reduce the risks related to cybersecurity and business continuity by facilitating the organization to acquire the necessary skills and elements for it, as a consequence of the implementation of the expected results of the ''Identify'' and ''Recover'' functions. In addition, the ULEO has been built in such a way that there is a direct mapping from it to the mitigations defined by MITRE to face the most important real cyber threats.

D. CYBER SECURITY DOMAINS

As mentioned throughout this work, many organizations manage their cybersecurity using information security regulatory frameworks. For this reason, it is likely that they have not assimilated the need for participation in many of the functional areas whose involvement is required for cybersecurity. This is a clear mistake that must be corrected if organizations intend to deal with cyber threats using a cybersecurity approach, so it is necessary to change this trend and adopt a much broader and more integrated vision.

To help with this purpose, in our proposal we use the main cybersecurity domains of [82], because it is the most complete work and at the same time focused on cybersecurity of the sources that we have analyzed. To the previous ones, we added an additional domain related to corporate communication, marketing and institutional relations, which we consider essential to face the emerging cyberattacks in the last two years, with an impact on the supply chain and on the image and reputation of the organization; and because it is a necessary area to achieve some of the cybersecurity expected outcomes of the ULEO. In our work we will understand the domains of cybersecurity as the functional areas of an organization with responsibilities in cybersecurity. The complete list of functional areas of cybersecurity included in our proposal can be found in Table 27 (Appendix V), with the following scope:

- **FA1**. In charge of IoT device security.
- **FA2**. Active defense, vulnerability management, threat hunting, SIEM operation, cybersecurity operations center activities, or incident response [83].
- **FA3.** Prepare human resources regarding cybersecurity threats through continuous training and its reinforcement, as well as the design and execution of practical cybersecurity exercises [84].
- **FA4**. In charge of the analysis of internal and external threats, the exchange of threat intelligence with third parties or the preparation and incorporation of Indicators Of Compromise *(IOCs)*.
- **FA5**. With tasks related to the surveillance of applicable regulations and their incorporation into cybersecurity. In addition, the monitoring of different performance indicators, and the establishment of strategies, policies, standards, processes, procedures or corporate instructions.
- **FA6**. Focused on risk treatment, business continuity management, crisis management, establishing the organization's position regarding cyber risks, insurance contracting, risk registration, auditing, defining groups of risk management, or defining those responsible and owners of the processes and assets [85].
- **FA7**. Responsible for cybersecurity risk analysis, vulnerability scanning, supply chain risk identification and analysis, asset inventory, risk monitoring, and penetration testing of infrastructure, people, or systems of information, among others.
- **FA8**.With the mission of leading the secure software development cycle, continuous integration and deployment, user experience security, software quality, API security, identification of information flows in information systems, management of the free software used, or the static or dynamic analysis of the code.
- **FA9**. In charge of the management, development, implementation, and verification of compliance with the standards and regulations defined at the corporate level for cybersecurity: CIS controls, MITRE matrix, NIST framework for the improvement of cybersecurity of critical infrastructures, or the family of standards ISO27000 [19].
- **FA10**. With activities such as management, definition, implementation, operation, prevention, etc., in relation to cryptography, key and certificate management, encryption standards, security engineering, access controls with or without multiple authentication factors, single sign-on, privileged access management, identity management, identity federation, cloud security, container security, endpoint security, data protection and prevention of data leakage, network design to prevent distributed denial of service attacks, development and secure configuration of systems, patch and update management or the establishment of secure reference configurations.
- **FA11**. To promote study, education, and training, attendance at conferences, or participation in related professional groups, training, or certification.
- **FA12**. Specific activities include internal and external corporate communication, social networks

management, marketing, or the establishment and maintenance of institutional relationships with interested third parties with whom the organization maintains some type of contact.

E. AGGREGATED CYBERSECURITY ASSESSMENT

Cybersecurity assessment, especially in environments involving different functional areas, is often problematic because of its ambiguity, different interpretations, or different interests. However, having a unified, realistic and unbiased view of the state of cybersecurity is essential. Based on what was previously discussed in this study, our proposal defines the necessary aspects to provide a shared vision of cybersecurity.

1) IG IDENTIFICATION

In our work, we have elaborated on the ULEO in such a way that it allows a direct association between the protection priority indicated in the BIA for each business asset and different IGs. The correspondence between the priority established in the BIA and the IGs that should be applied to the asset can be shown in Table 28 (Appendix V), in such a way that, to provide cybersecurity to a business asset cataloged with LOW priority, actions must be put in place to achieve all the expected outcomes of the IG1 implementation group. For the assets cataloged with MEDIUM and HIGH priorities, those of the IG2 and IG3 groups, respectively. These groups and their associated actions are homogeneous for all business assets in the organization.

2) RELATIVE WEIGHT OF EACH SECURITY FUNCTION

The hierarchical structure embedded in the ULEO allows us to infer the weight of each cybersecurity function (fig. 10) for each IG with respect to the global cybersecurity of the business asset. These weights can be calculated as a percentage (or normalized between 0.00 and 1.00). In our proposal we calculated the weights of each security function for IG1, IG2 and IG3. These weights have been rounded to the second decimal place and are shown in table 29, Table 30 and Table 31 (Appendix V), respectively, where:

- F, represents the continuous cybersecurity function.
- N_c, represents the number of categories that the function F includes for the corresponding IG.
- W_f, represents the relative weight of the F function with respect to the global cybersecurity value of the asset.

3) RELATIVE WEIGHT OF EACH CATEGORY AND EXPECTED OUTCOME

For the same reasons expressed in the previous point, the ULEO allows determining the weight of each category, for each IG, with respect to each cybersecurity function, as well as the weight of each expected outcome with respect to its category. In our proposal, we calculated the weights of each category and expected outcomes, as shown in Appendix C. The weights corresponding to 'Identify' categories and expected outcomes can be seen in Tables 32 to 34; those related to 'Protect' categories and expected outcomes in Tables 35 to 37; values related to 'Detect' sub-items are shown in Tables 38 to 40; the weights of categories and expected outcomes belonging to 'Respond' are in Tables 41 to 43, and those corresponding to the 'Recover' function are shown in Tables 44 to 46. In all cases:

- C, represents the category.
- N_o, represents the number of expected outcomes of that category.
- W_c, represents the relative weight of C category with respect to its function (rounded to the second decimal place).
- W_o, represents the relative weight of each expected outcome with respect to its category.

A visual description of category weights for functions 'Identify', 'Protect', 'Detect', 'Respond' and 'Recover' is shown in figs. 11, 12, 13, 14 and 15, respectively.

The previous calculations allow a tree-like set of weights to be calculated in an aggregated way for the cybersecurity posture of the business asset in relation to its criticality. At all levels, expected outcome, category, function, or global.

4) DISCRETE LEVELS OF IMPLEMENTATION

It is convenient to define unambiguous values to establish the achievement/implementation status of each expected outcome. This issue is a common source of discrepancies and conflicts in organizations, either because each functional area has different perspectives on implementation status or because they do not have the ability to adequately measure at such a detailed level. Therefore, in our proposal, we have chosen to use Discrete Levels of Implementation *(DLIs)*, as standardized values to communicate the status of implementation of the cybersecurity actions that allows obtaining the expected outcomes (fig. 16). In our study these are the only possible values for expressing the state of progress in the implementation of each action related to an expected outcome.

Because they are not subject to interpretation and have the same meaning regardless of the functional area, action or expected outcome in question, *DLIs* are a good communication mechanism that avoids conflicts between functional areas and provides the same and shared perception of cybersecurity status.

5) ASSET BREAKDOWN

The main element of this proposal is the business asset, understanding that this unit is sufficiently small to be addressed at lower levels without too many problems. However, there may be situations where it is necessary to break down such business assets into secondary assets, for example, because it is easier to take care of cybersecurity in this way or because it facilitates the distribution of tasks between different operational groups of the same functional area or different functional areas. If necessary, the asset can be broken down as many times as necessary, following the guidelines designed

FIGURE 10. Relative weights of each cybersecurity function and the three IGs.

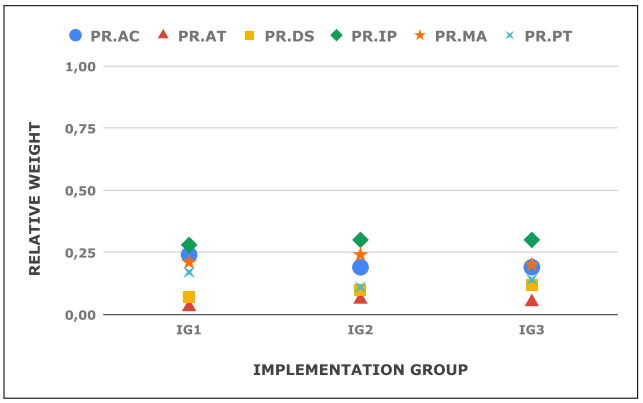


FIGURE 12. Relative weights of every category in 'Protect' function and the three IGs.

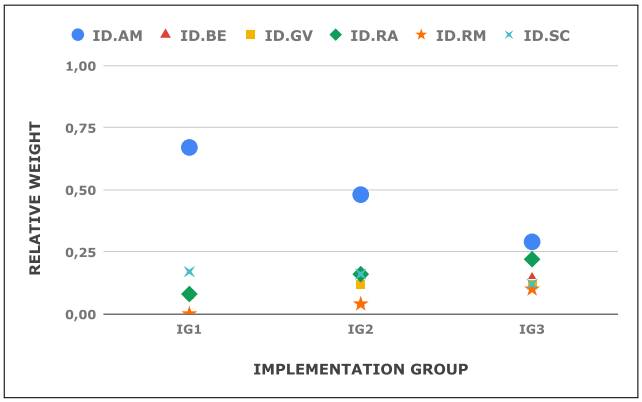


FIGURE 11. Relative weights of every category in 'Identify' function and the three IGs.

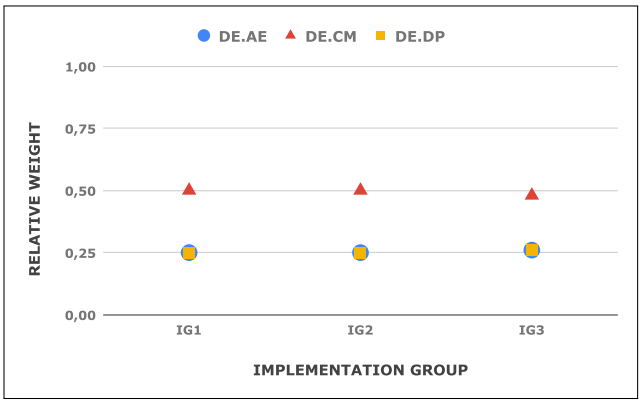


FIGURE 13. Relative weights of every category in 'Detect' function and the three IGs.

in our proposal. Bearing in mind that L represents the level of the asset, with L0 being the business asset and increasing to L1, L2... as the assets are broken down into more manageable assets:

- Each asset that is broken down must be broken down into elements that constitute an independent whole by themselves, as shown in equation 1.

$$Asset(L) \Rightarrow \bigcap_{i=1}^{n} Asset(L+1)_i = 0 \tag{1}$$

- The sub-assets in which an asset is broken down must represent the total of the asset on which they depend. In other words, the total top-level asset has been broken down into the sub-assets that make it up, as shown in equation 2.

$$Asset(L) = \sum_{i=1}^{n} Asset(L+1)_i \tag{2}$$

- Each sub-asset must have a weight (ω), as a reflection of its contribution to the higher-level asset, consisting of a normalized value between 0.00 and 1.00, equivalent to a percentage between 0% and 100% of the parent asset, respectively, as shown in equation 3.

$$Asset(L) = \sum_{i=1}^{n} \omega_i \cdot Asset(L+1)_i \tag{3}$$

subject to the following restriction (equation 4)

$$\sum_{i=1}^{n} \omega_i = 1, \forall \omega \in \mathbb{R}, \omega \subset [0,1] \tag{4}$$

- The implementation group corresponding to the parent asset will apply to all its sub-assets, as specified in equation 5.

$$IG(Asset(L+1)) = IG(Asset(L)) \tag{5}$$

Likewise, there are two types of assets/sub-assets: those that have been broken down into sub-assets, which we call 'inner assets', and those that have not been broken down into sub-assets, which we call 'leaf assets'. It is important to understand this distinction which is necessary for an aggregate evaluation of asset cybersecurity.

Figure 17 shows an example of a properly performed breakdown of a fictitious business asset at three levels. The weights and number of sub-actives in the figure are invented and placed like this for merely didactic purposes. However, it

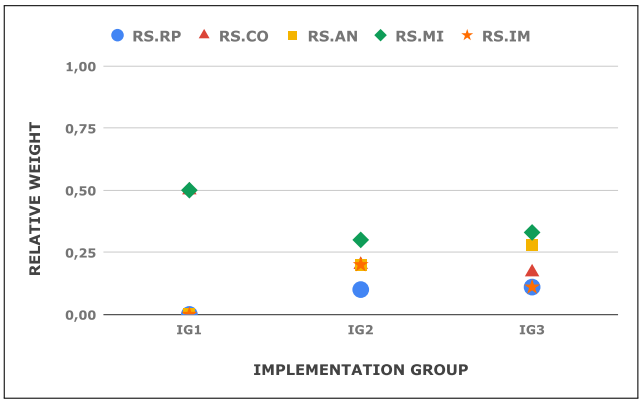


FIGURE 14. Relative weights of every category in 'Respond' function and the three IGs.

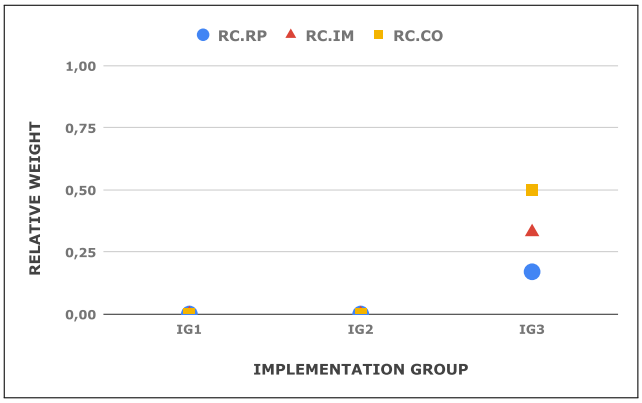


FIGURE 15. Relative weights of every category in 'Recover' function and the three IGs.

is necessary, as can be seen in the figure, that the sum of the weights of the sub-assets into which an asset has been broken down, is 1.00 in all cases. The figure also shows in different colors the inner assets (blue) and the leaf assets (yellow).

6) ASSET's CYBERSECURITY IDEAL STATE AND ASSET's CYBERSECURITY EXPECTED STATE

The Asset's Cybersecurity Ideal State *(ACIS)* will always be 1.00, which is achieved when a DLI of 1.00 has been reached for all the expected outcomes that correspond to it according to the applicable IG. It is important to understand this nuance, since the same level of implementation for the same expected outcomes that for an asset could represent an *ACIS*, for another asset it could represent a state of, for example, 0.54 (so not ideal), simply because a different implementation group applies to it.

The Asset's Cybersecurity Expected State *(ACES)*, will be determined by the organization as a cybersecurity objective, referring to a specific value of one, several, or all cybersecurity functions, categories, or expected outcomes. This expected state could result from any combination of DLIs applied to any applicable set of expected outcomes, which allows reaching that value. Understand this distinction.

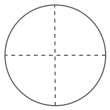
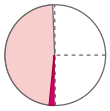
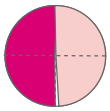
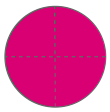
COVERAGE	DLI	EXPLANATION
	0.00	None of the necessary actions have been implemented to obtain the expected outcome.
	0.33	Some of the actions necessary to obtain the expected outcome have been implemented, but less than half.
	0.66	Half of the actions necessary to obtain the expected outcome, or more, have been implemented.
	1.00	All the necessary actions have been implemented to obtain the expected outcome.

FIGURE 16. Discrete levels of implementation (DLIs). black shows the minimum coverage required to be qualified as the corresponding DLI. Pink shows the maximum coverage (together with the black portion) before hopping to the next DLI.

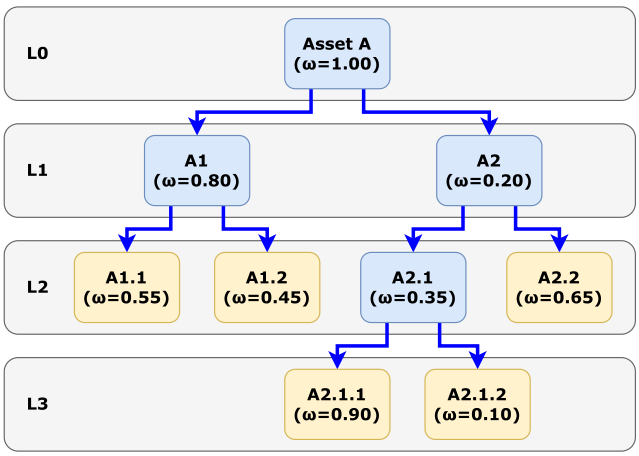


FIGURE 17. Example of a correct asset breakdown.

Although there is only one option to achieve an *ACIS* (the one described in the previous paragraph), to achieve an *ACES*, there may be multiple possible combinations on which a selection process will have to be carried out; this is covered in Section IV.

7) COMPUTING THE ASSETS' CYBERSECURITY STATUS

The defined structure and weights calculated in our proposal allow the evaluation of the cybersecurity status of an asset by adding information in a bottom-up process. The formulas that we have designed in our solution are easy to implement in any programming language or dashboard solution. Its tree-like structure facilitates the implementation of navigation through the organization, assets, sub-assets, functions, categories, and expected outcomes, to detect deficiencies in cases in which

the state of cybersecurity is not the expected or planned at any of these levels.

In the case of a leaf asset, the evaluation is performed as follows:

- **First step.** It consists of assigning to each expected outcome that applies the DLI that best reflects the status of the implementation of the associated actions. Thus, this information can be propagated upwards, starting by calculating the Category's Cybersecurity State (CCS_i) of each cybersecurity categories of the model of our proposal (equation 6).

$$CCS_i = \sum_{j=1}^{n} Wo_{ij} \cdot DLI_{ij} \tag{6}$$

  That is, the weighted sum of the discrete level of implementation of each expected outcome included in the category is calculated, based on its relative weight with respect to this category.
- **Second step**. Once the CCS_i values are known for all categories, the metrics can continue to be propagated upwards to calculate the Function's Cybersecurity State (FCS_i) of each cybersecurity function of the model of our proposal (equation 7).

$$FCS_i = \sum_{j=1}^{n} Wc_{ij} \cdot CCS_{ij} \tag{7}$$

  That is, the weighted sum of the cybersecurity status of each category of the function is calculated, considering its relative weight with respect to this function.
- **Third step**. And finally, having already calculated the FCS_i values for each function, we can calculate, going higher, the Asset's Cybersecurity Status (ACS_i) for each evaluated leaf asset (equation 8).

$$ACS_t = \sum_{j=1}^{n} Wf_{tj} \cdot FCS_{tj} \tag{8}$$

  This formula calculates the weighted sum of the cybersecurity status of each function applied to the asset, considering its relative weight with respect to its global cybersecurity. The t sub-index means that the ACS value is computed at a given moment, and subsequent measurements can throw different values.

In the case of inner assets, the calculation is based on previous knowledge of the ACS_i value of each sub-asset using the technique explained in the previous steps. Once these values are known, this information can be added, and the value of ACS_i for the inner asset can be calculated as follows (equation 9):

$$ACS_t = \sum_{j=1}^{n} Wsa_{tj} \cdot ACSsa_{tj} \tag{9}$$

where $ACSsa_{tj}$ is the ACS_{tj} value calculated independently for each sub-asset and Wsa_i is the relative weight of that sub-asset. In other words, the weighted sum of the cybersecurity status of each sub-asset is calculated while considering its relative weight with respect to the parent asset.

Because of the possibility of having different ACS_t values depending on the moment when the measurement is taken, our proposal allows computing the behavior of the ACS value over the time ($ACSev$), as shown in equation 10.

$$ACSev = \frac{t\sum_{i=1}^{t} t_i ACS_i - \sum_{i=1}^{t} t_i \sum_{i=1}^{t} ACS_i}{t\sum_{i=1}^{t} t_i^2 - (\sum_{i=1}^{t} t_i)^2} \tag{10}$$

$ACSev$ will take values from 0.00 to 1.00, because it is an additive time series. Values close to 1.00 indicate that the $ACIS$ for that asset will be achieved quickly, whereas values close to 0.00 predict ACS for that asset increases slowly and, therefore, it will take longer to achieve its $ACIS$.

8) COMPUTING THE ORGANIZATION's CYBERSECURITY STATUS

Although our proposal does not intend to address the strategic area, thanks to this, it is possible to evaluate the Organization's Cybersecurity Status (OCS) by continuing with bottom-up aggregation, in a similar way to what was explained in the previous section.

If the organization has identified weights for business assets that comply with the provisions for asset breakdown, the OCS can be calculated as follows (equation 11):

$$OCS_t = \sum_{j=1}^{n} Wba_{tj} \cdot ACSba_{tj} \tag{11}$$

where:

- Wba_{tj} is the relative weight of each business asset of the organization.
- $ACSba_{tj}$ is the cybersecurity status of each business asset calculated as described in the previous section. The t subindex, again, means that the $ACSba$ value is computed at a given moment and subsequent measurements can throw different values.

The above formula calculates the weighted sum of the cybersecurity status of each business asset, using its relative weight with respect to the organization. As in the previous paragraphs, owing to the possibility of having different OCS_t values depending on the moment when the measurement is taken, our proposal allows the calculation of the behavior of the OCS value over time ($OCSev$), as shown in equation 12.

$$OCSev = \frac{t\sum_{i=1}^{t} t_i OCS_i - \sum_{i=1}^{t} t_i \sum_{i=1}^{t} OCS_i}{t\sum_{i=1}^{t} t_i^2 - (\sum_{i=1}^{t} t_i)^2} \tag{12}$$

$OCSev$ will take values from 0.00 to 1.00, because it is an additive time series. Values close to 1.00 indicate that the cybersecurity status for the organization will be achieved quickly, whereas values close to 0.00 predict the OCS increases slowly and, therefore, it will take longer to achieve the expected cybersecurity status.

IV. CYBERSECURITY TACTICAL AND OPERATIONAL MANAGEMENT PROCESS

A. OVERVIEW

To articulate all the elements defined in Section III and that in this way our proposal constitutes a systematic mechanism, we have developed a Cybersecurity Tactical and Operational Management Process (CyberTOMP).

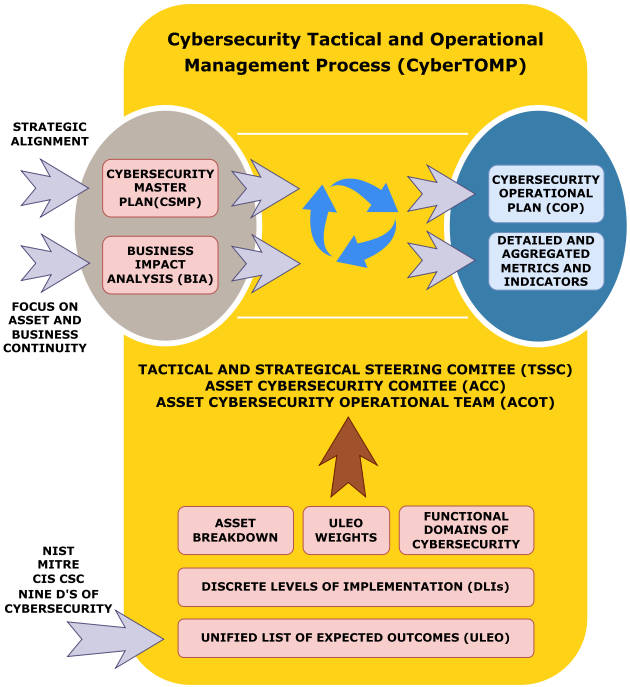


FIGURE 18. CyberTOMP high-level view.

Fig. 18 shows a coarse-grained view of the process, with the main inputs, outputs, and involved elements. The high-level objective of this process is to facilitate cybersecurity management by focusing on a business asset in each case. For this to be possible, the process, which will be discussed in the following sections, will be based on the organization's CSMP and BIA. This, together with the requirements expressed in Section III, provides the necessary alignment with the strategic objectives of the organization, both in terms of cybersecurity and business continuity, as well as a focus on business assets.

As a result of the application of CyberTOMP, a specific Operational Cybersecurity Plan *(COP)* is obtained for the business asset whose cybersecurity is being managed, as well as a set of metrics and indicators detailed and addable upwards. Both results, agreed upon by all functional areas involved in cyber defense/cyber protection of business assets. CyberTOMP facilitates the application of change management techniques [86] by following an inclusive and progressive approach.

The process that we developed achieves the necessary cooperation between all the functional areas of the organization in cybersecurity matters through three multidisciplinary bodies that participate at different times:

- **The Tactical-Strategic Steering Committee *(TSSC)*.** An interdepartmental multidisciplinary committee composed of members of the organization's steering committee, who preferably, participated in both the preparation of the CSMP and the BIA. With initial inclusion, if necessary, of tactical personnel.
- **The Asset's Cybersecurity Committee *(ACC)*.** An interdepartmental multidisciplinary committee made up of all intermediate positions with responsibilities at a tactical level for the business asset to be protected. With sporadic participation, if necessary, of operational personnel.
- **The Asset's Cybersecurity Operational Team *(ACOT)*.** An interdepartmental multidisciplinary team made up of all positions in the organization with responsibilities at the operational level, as well as external personnel incorporated into the organization belonging to service providers, who regularly participate in the daily work of the organization. In both cases, when these tasks are related to the business asset to be protected.

Each of these bodies must include people from all areas of knowledge of the organization that must participate in the cybersecurity of the business asset. In this way, these will be the bodies that facilitate the unity of action and holistic approach. Their participation in the process will be in increasing order, with the TSSC being the body that has to use the least effort in the process and the ACOT being the one that has to make the most.

At a greater level of detail, CyberTOMP includes five phases, that are similar to those commonly accepted for project management [87], with some modifications in the final phase becasue, although considering that the protection of assets emanates from projects defined in the CSMP, it is an ongoing task. These phases are: Initiating, Planning, Execution, Monitoring and Controlling, and Continuous Improvement, each containing a series of clear steps, as presented in fig. 19, which shows CyberTOMP's detailed view.

These phases, as well as the activities included in them, their peculiarities, and their explanations are detailed in the following sections with the intention of serving as a guide for their practical application in any organization. We believe this level of detail is necessary because precisely what our work tries to solve is the lack of procedural elements to manage cybersecurity at the tactical and operational levels.

B. INITIATING

This initial phase of the process is focused on:

- Ensure that cybersecurity management focuses on business assets, using those identified in the BIA.
- Ensure strategic alignment by assigning requirements derived from the BIA as well as tasks, objectives, and high-level requirements from different projects defined in the CSMP.

- Ensure that the required holism is provided to protect the business asset on a daily basis.
- Ensure that guidelines are provided to achieve shared leadership and co-governance in cybersecurity management for each business asset.

These elements have a marked strategic nature, are defined at a high level, and are presumably endowed with greater stability over time. The 'Initiation' phase consists of two main activities as detailed below.

1) DEFINE INITIAL ACC

In this activity (fig. 20), the TSSC analyzes the information contained in both the CSMP and BIA to determine the following:

- The business assets identified in the BIA and their high-level cybersecurity and continuity needs, including the potential needs for actions to respond to cybersecurity incidents and/or to recover from unavailability with regard to cybersecurity.
- The projects defined at a high level in the CSMP for each of the assets established in the BIA, their objectives, and their actions at a high level.
- Based on the above, the functional areas of the organization that should be involved in the cybersecurity of each business asset established in the BIA.
- People, at a tactical level, identified in each of these areas.

This group of individuals identified by the TSSC will form the initial ACC. If the TSSC deems it necessary, it may consult those people directly to determine more accurately whether other people not considered should also be part of the initial ACC. The initial ACC should include, for each person, high-level reasons why that person should be part of the ACC and high-level expectations for the cybersecurity of the business asset from their functional area.

As a guideline for this step, the set of cybersecurity functional domains identified in Section III can be used, which provides a fairly detailed representation of the functional areas involved in cybersecurity. The TSSC will define as many ACCs as business assets need cyber protection.

2) DEFINE INITIAL CYBERSECURITY ASSIGNMENT

In this step (fig. 21), based on the analysis of the BIA and CSMP, the TSSC will prepare a high-level list of cybersecurity and continuity needs and objectives (in relation to cybersecurity) for the business asset and will formalize a cybersecurity assignment for the asset, which will be delivered to the people who form the initial ACC. The needs and objectives will be extracted from the cybersecurity projects included in the CSMP and will be expressed in the form of high-level *ACES*, preferably as requirements on the metrics ACS_i or FCS_i of the asset indicated in the assignment. For example, the objectives of the business asset cybersecurity assignment can be:

- Increasing the ACS_i a 10%.
- Increasing the FCS_i, for the 'Respond' function, a 12%.
- Keeping the ACS_i at the current 75% relative to the current threat context.
- Keeping the ACS_i after a change in prioritization of business assets in the BIA.
- Keeping the ACS_i after a remodeling of the organizational structure.
- Assessing the ACS_i.
- Achieving the *ACIS*.

Or similar objectives. The cybersecurity assignment for the asset includes the indicated goals, the group of people that will form the initial ACC, the written statement of the assignment, and each area or functional unit represented. For practical reasons, it may be more agile to carry out this delivery through a joint meeting where the details of the assignment can be explained. Finally, the assignment must reach all the members of the initial ACC in a more formal way.

The assignment will include a period for the ACC to refine, adjust, and complete it after a more detailed analysis at the tactical level as a step prior to its final formalization.

The TSSC will carry out as many cybersecurity assignments as business assets need cyber protection.

C. PLANNING

This phase of the process is intended to delve into the details of the actions that must be undertaken to achieve the objectives requested in the assignment. For this, a series of iterative activities is carried out until the granularity that allows:

- Breaking down the business assets if it is considered necessary for a better distribution of tasks, greater control, or in general, to facilitate the management of the work to be carried out at tactical and operational levels.
- Identifying and distributing the scope of actions among different areas of knowledge represented in the ACC.
- Providing context to the cybersecurity needs of the assignment and adapting the actions that must be undertaken to the reality of the moment in the cyber field, from a multidisciplinary and holistic approach.
- Agreeing on the distribution of cybersecurity metrics and indicators.
- Updating the initial cybersecurity assignment, completing it with the aspects considered necessary.

In this phase, the ACC deals with planning in two stages that allow:

- Having a tactical-strategic planning, with a minimum participation of the TSSC.
- Having a later tactical-operational planning, more detailed, without the participation of the TSSC, and with the growing involvement of the operational teams.

The 'Planning' phase is consists of eight activities, which are detailed below.

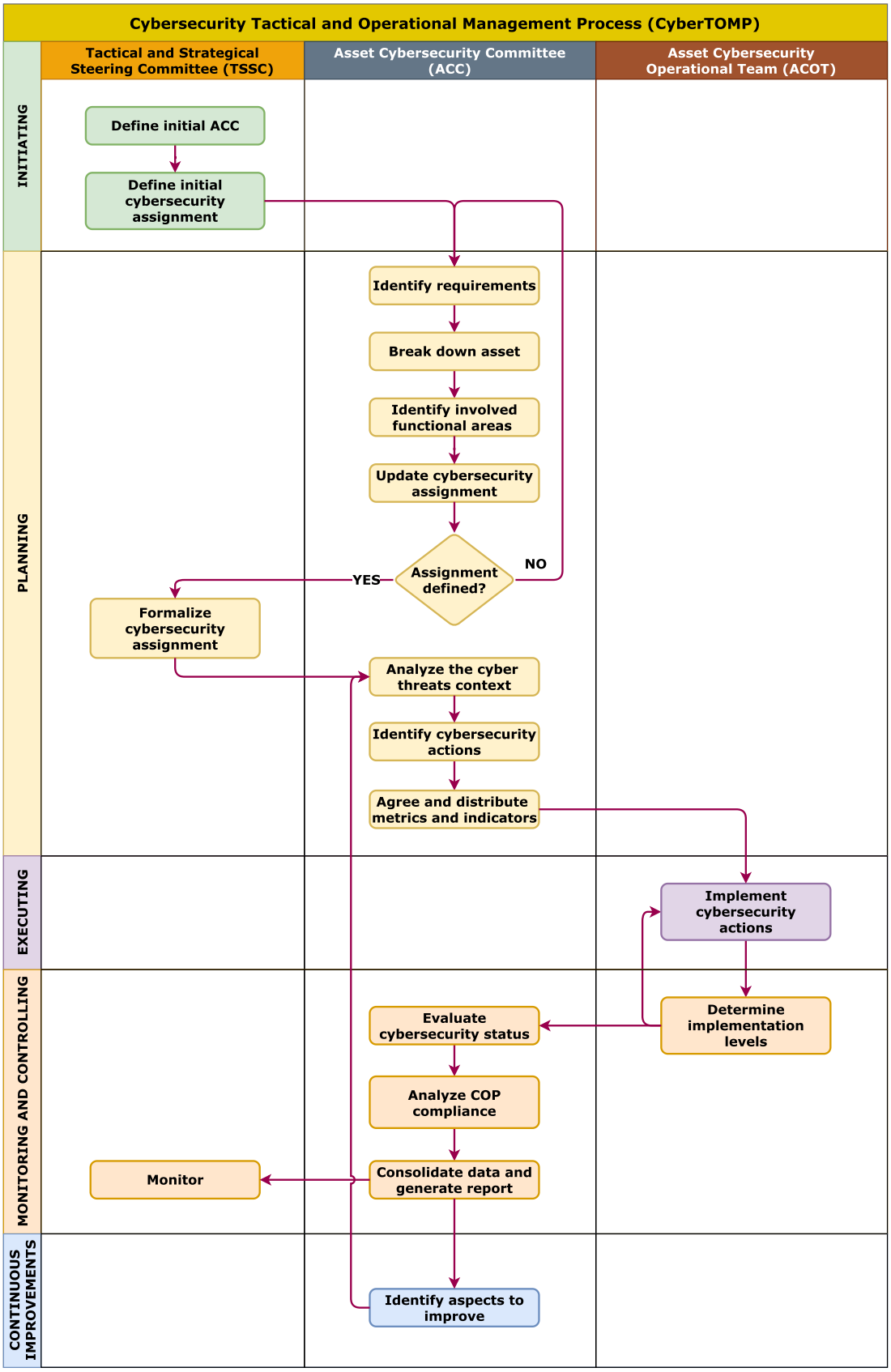


FIGURE 19. Detailed CyberTOMP steps and activities.

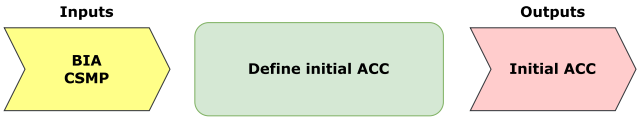


FIGURE 20. Inputs and outputs of 'Define initial ACC' activity.

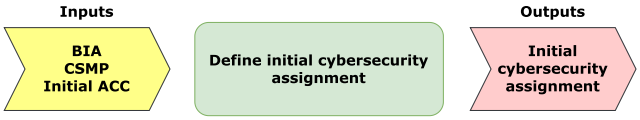


FIGURE 21. Inputs and outputs of 'Define initial cybersecurity assignment' activity'.

1) IDENTIFY REQUIREMENTS

In this activity (fig. 22), the ACC in the cybersecurity assignment for the asset will receive the priority corresponding to it, as the organization has assigned to that asset in the BIA. Accordingly, ACC will be able to directly identify the corresponding IG from the ULEO defined in this study, as described in Section III. Because each IG determines the expected outcomes for each existing function and category, the ACC will know all the expected outcomes whose implementation would allow the business asset to reach the *ACIS*. This value will be used as a reference for the maximum cybersecurity with which the asset must be provided.

The ACC must analyze the objectives (the *ACES*) set by the TSSC in the cybersecurity assignment and determine the categories or expected outcomes of the ULEO that will need to be taken into consideration to achieve that objective without going deeper into the specific actions that involve each of them. The ACC will add this additional detail to the cybersecurity assignment and update the *ACES* to reflect on what was identified.

This step begins with tactical-strategic planning of the actions required for the cybersecurity of the business asset.

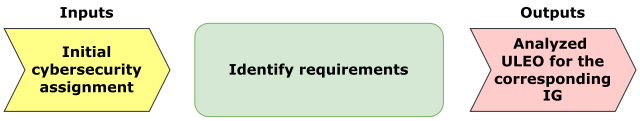


FIGURE 22. Inputs and outputs of 'Identify requirements' activity.

2) BREAK DOWN ASSET

If greater ease of management or understanding is needed, the ACC may break down the asset (fig. 23) into others of smaller caliber. The breakdown mechanism is presented in detail in Section III. Each sub-asset generated in this process is managed by the same ACC within the same assignment.

This subdivision allows different members of the ACC to focus more (although coordinated) on some of the broken-down sub-assets. It can also facilitate the assignment of activities between different areas or operational groups with greater

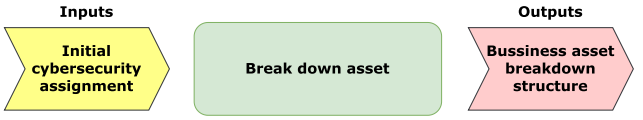


FIGURE 23. Inputs and outputs of 'Break down asset' activity.

specialization in specific tasks, without losing alignment with the proposed objective from the strategic level.

3) IDENTIFY INVOLVED FUNCTIONAL AREAS

It is likely that after the analysis of the requirements and the possible breakdown of assets into smaller ones, the need to incorporate some additional functional areas that must participate in the cybersecurity of the asset will be detected. If this is the case, the ACC will include tactical managers of such functional areas in CyberTOMP (fig. 24). The functional areas described in Section III are clear candidates.

FIGURE 24. Inputs and outputs of 'Identify functional areas involved' activity.

4) UPDATE CYBERSECURITY ASSIGNMENT

The ACC updates the cybersecurity assignment for the business asset (fig. 25) by documenting the identified requirements, the expected outcomes that must be considered to achieve the objectives, the new functional areas identified that must participate in the cybersecurity of the asset, the estimated breakdown of the business asset, and the agreed weights for all. In short, it should provide a more complete vision of cybersecurity assignment and provide the necessary justifications for it.

Once the assignment has been updated, it will be analyzed whether it can be considered complete and final, in which case the ACC will request formal approval from the TSSC. Otherwise, the process iterates, returning to the ''Identify requirements'' step.

An assignment cannot be considered complete if new functional areas are added to the process. If this happens, to prevent this inclusion from being merely cosmetic and ultimately causing tensions due to the assumption of non-agreed responsibilities, it will be necessary to iterate again (from the first step of 'Planning' phase) so that these functional areas can participate in all the steps prior to the final definition of the cybersecurity assignment.

5) FORMALIZE CYBERSECURITY ASSIGNMENT

TSSC analyzes the updated cybersecurity assignment for the asset submitted by ACC. It will evaluate its content, its convenience and feasibility, and the existence of the necessary

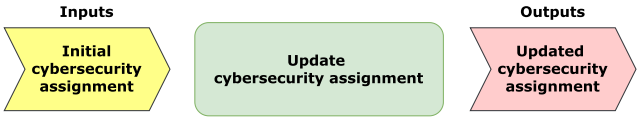


FIGURE 25. Inputs and outputs of 'Update cybersecurity assignment' activity.

consensus to provide holism and unity of action. It will approve the assignment (fig. 26) by signing it, the TSSC as a whole, the Chief Information Security Officer *(CISO)*, or the Chief Executive Officer *(CEO)*. It sends it to all members of the ACC as a final cybersecurity assignment for the protection of the business asset.

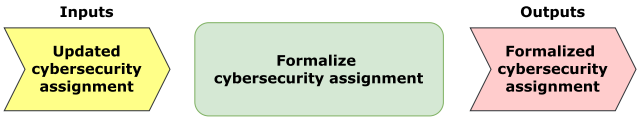


FIGURE 26. Inputs and outputs of 'Formalize cybersecurity assignment' activity.

This step ends the tactical-strategic planning of the actions required for cybersecurity of the business asset.

6) ANALYZE THE CYBER THREATS CONTEXT

In this phase, the ACC, supported by members of the ACOT, if necessary, will analyze the organization's cybersecurity context (fig. 27) in detail. In addition to the cyber threat context, in relation to business assets that they have been commissioned to protect. From both internal and external perspectives.

In this phase, renewed knowledge is acquired regarding the evolution of threats to the business in the cyber context. To express this in more detail, the cybersecurity status of a business asset can be altered simply because the context has changed, new threats have emerged, or there are exceptional situations that involve variations in the exposure level to different cybersecurity risks.

From this point is when the tactical-operational levels use their creativity, skills, and effort to cushion the enormous fluctuations in the cyber context and thus contribute, from the lower levels, to the strategic objectives of cybersecurity and the maintenance of the long-term corporate strategy.

This step is extremely important because allows a later definition of the form ('how') in which different cybersecurity actions must be implemented to ensure the achievement of the expected outcomes.

As a result of this step, it will be documented how low-level assets are impacted by the internal and external cyber context.

In this activity, in the event that it is a second or later iteration, the improvement opportunities identified in the continuous improvement phase of CyberTOMP will also be considered.

This step begins with tactical-operational planning of the actions required for the cybersecurity of the business asset.

FIGURE 27. Inputs and outputs of 'Analyze the cyber threats context' activity.

7) IDENTIFY CYBERSECURITY ACTIONS

In this activity, it is important to understand that expected outcomes are called that way precisely because they are the results that will presumably be obtained by carrying out different actions. Actions defined in greater detail in the textual description of each expected outcome.

For example, the CIS safeguard 'CS-11.1 Establish and Maintain a Data Recovery Process' would be the expected outcome, whereas the actions defined by the CIS for that safeguard would be those that allow it to be achieved: 'Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard'. Only when everything described for that safeguard is done, it can be indicated that it is fully implemented.

As explained in the previous sections, there is only one way to obtain the *ACIS*, but there are many combinations to obtain the *ACES*. Therefore, both *ACC* and *ACOT* must analyze the different existing options that allow reaching the required *ACES*.

In this activity, the ACC will take the approved cybersecurity assignment, where the expected outcomes for which specific actions must be designed have already been identified, as well as the analysis carried out in the cyber threat context. (fig. 28). For each, the *ACC* will analyze the details of its description:

- For ULEO subcategories from the NIST cybersecurity framework, they should review the relevant description [48] in the framework itself or in the associated guides [50], [51].
- For the subcategories included in the ULEO and coming from the CIS, the relevant description [40] in the list of CSCs can be reviewed.
- For the subcategories incorporated into the ULEO and coming from the nine D's of cybersecurity, they should consult the description of each D [47] described in the original work.

The objective of this activity is to identify the potential list of cybersecurity actions that would address the cyber threat

FIGURE 28. Inputs and outputs of 'Identify cybersecurity actions' activity.

context to achieve the goals included in the cybersecurity assignment.

8) AGREE AND DISTRIBUTE METRICS AND INDICATORS

In this activity, the *ACC* and *ACOT* will reach a consensus (fig. 29) to select the expected outcomes and the actions that lead to them, among those identified, in a way that optimizes resources, management is facilitated, the workload and responsibilities of the different participating functional areas are reasonably distributed, existing technologies or knowledge can be reused; conflicts are minimized, etc.

With the above, each functional area of the *ACOT* will have the expected outcomes and the associated tasks that they have to undertake from their scope, the description of such tasks, the roles and responsibilities, metrics and weights, planning of the actions and milestones, their dependencies, and the periods to evaluate the progress. All this, as a whole, will constitute the Cybersecurity Operational Plan *(COP)* for the asset accompanied by the corresponding metrics and indicators. This plan will be fully aligned with the corresponding cybersecurity assignment mandated by the *TSSC* and, by extension, with the BIA and associated CSMP project.

The *ACC* defines a minimum DLI for each expected outcome, which must allow the achievement of what is required by the *TSSC* in the cybersecurity assignment for the asset. In this way, each person from the *ACOT* will know the target level of implementation for the actions that correspond to them. This step ends the tactical-operational planning of the actions required for cybersecurity of the business asset.

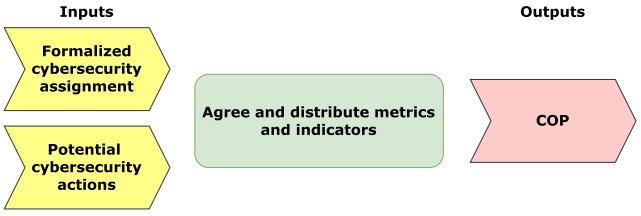


FIGURE 29. Inputs and outputs of 'Agree and distribute metrics and indicators' activity.

D. EXECUTING

The objective of this phase effectively implement the actions planned in the *COP*.

1) IMPLEMENT CYBERSECURITY ACTIONS

In this activity, the *ACOT* will be the team in charge of implementing the specific measures to achieve the expected outcomes that have been assigned (fig. 30), so that the micromanagement of these actions can be carried out in a decentralized manner in each *ACOT* functional area once the *ACC* has already agreed on the set of precise actions.

In practice, this step allows the performance of short-term tasks in a semi-autonomous and self-organized manner, ultimately contributing to the organization's cybersecurity and business continuity objectives (in relation to cybersecurity).

The different members of the *ACOT* can be helped, especially in the more technical functional areas, by the different existing guides, such as, for example, [33], [50] o [46].

FIGURE 30. Inputs and outputs of 'Implement cybersecurity actions' activity.

E. MONITORING AND CONTROL

This phase is focused on evaluating the cybersecurity status of business assets in relation to the cybersecurity assignment ordered by the *TSSC* and the corresponding *COP* generated in previous phases, to build valuable information so that the different levels of the organization can clearly understand the cybersecurity situation of the asset, with the necessary detail, and make decisions in this regard.

The evaluation of the state of cybersecurity will be carried out at three levels: operational, tactical, and strategic, which will be carried out with different frequencies, the most frequent being the operational evaluation, followed by the tactical one and the least frequent, the strategic evaluation, for a correct assessment of the impact of the actions as well as the new needs in the short, medium, and long term, respectively.

1) DETERMINE IMPLEMENTATION LEVELS

In this activity, with the periodicity indicated by the *ACC*, each member of the *ACOT* establishes the current *NDI* for each expected outcome that has been assigned (fig. 31), as indicated in Section III. In this way, the *ACC* will have the *NDI* for all expected outcomes included in the *COP* of the asset.

Together with this information, the *ACOT* will succinctly detail difficulties, synergies, proposals arising during the course of the work, or unexpected situations or situations not initially analyzed, if they exist. This will be performed individually for each expected outcome.

Progress information, together with the relevant information that allows its contextualization, will be included in an Operational Cybersecurity Report *(OCR)*, which can be as complex or simple as the organization requires.

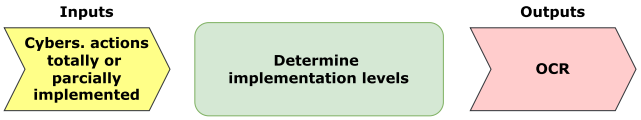


FIGURE 31. Inputs and outputs of 'Determine implementation levels' activity.

2) EVALUATE CYBERSECURITY STATUS

In this activity, with the agreed frequency, the *ACC* will receive the *OCRs* sent by the *ACOT* and proceed to evaluate the cybersecurity of the asset (fig. 32) using the *DLIs* contained in that report. They will do it following what is specified in Section III, taking into account the relative weights and calculating, for the business asset, the values CCS_i, FCS_i and ACS_i, so that at the end, the information aggregation and construction process will have, for each asset and sub-asset into which the business asset has been broken down:

- The status of achievement of each expected outcome.
- The cybersecurity status with respect to each category.
- The cybersecurity status with respect to each function.
- The cybersecurity status of the business asset.

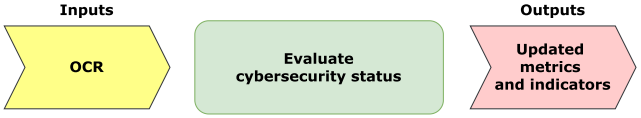


FIGURE 32. Inputs and outputs of 'Evaluate cybersecurity status' activity.

3) ANALYZE COP COMPLIANCE

In this activity, with the frequency that has been agreed upon for the tactical evaluation of cybersecurity, the *ACC* will analyze the current state and evolution of the different metrics and indicators associated with the cybersecurity assignment (fig. 33), calculated and aggregated in the previous step using the different *OCRs* that the *ACOT* has been sending to it and that have not yet been jointly analyzed or compared with the *COP* forecasts. It is recommended that this activity coincide with the last release of *OCR* by *ACOT* in order to have the most up-to-date view possible.

In addition, it will use the relevant information provided by the *ACOT* in the *OCRs* to contextualize possible deviations from what was planned and understand the circumstances that may have caused such deviations or the synergies and opportunities that may exist. All of this will be included in the Tactical Cybersecurity Report *(TCR)*.

Finally, the *ACC* updates, if it exists, the organization's cybersecurity dashboard with the current CCS_i, FCS_i, and ACS_i values.

4) CONSOLIDATE DATA AND GENERATE REPORT

In this activity, with the periodicity required by the *TSSC*, the *ACC* will analyze the degree of achievement of what is required in the cybersecurity assignment for the business asset, using such an assignment as a source and also the information of the different *TCRs*. It is recommended that this task is carried out coinciding with the generation of the last *TRC* to obtain the most up-to-date and recent view. With all this, it will generate a Strategic Cybersecurity Report *(SCR)* that will broadly identify the advances or delays and their main causes, as well as evolutionary data and tactical decisions taken or planned, if appropriate, in a very executive way (fig.34).

The *ACC* will report the status to the *TSSC*, forwarding that report.

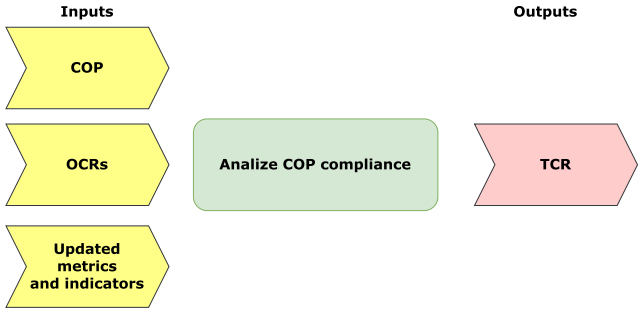


FIGURE 33. Inputs and outputs of 'Analyze COP compliance' activity.

5) MONITORING

The *TSSC* receives, with the required frequency, the last *SCR* regarding cybersecurity assignment for the protection of the business asset. With this information and that of the rest of the cybersecurity assignments they have assigned, they can, if desired, calculate the *OCS* value, taking into account the weights that could have been defined at a strategic level for each business asset.

FIGURE 34. Inputs and outputs of 'Consolidate data and generate report' activity.

The TSSC will use this monitoring information (fig. 35) to modify or update the cybersecurity assignment for strategic decision-makers in general or to generate additional strategic information that it deems necessary. This aspect is not addressed in detail in CyberTOMP, whose main scope is the tactical and operational levels.

F. CONTINUOUS IMPROVEMENT

The purpose of this phase is to identify the margins for improvement in different aspects, which can later be used as a basis for designing and executing additional actions in cybersecurity.

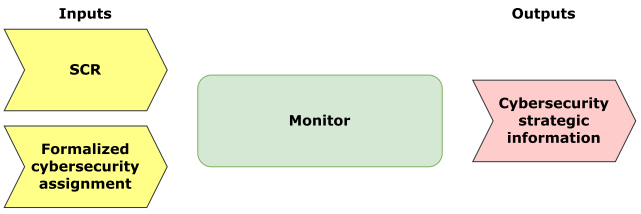


FIGURE 35. Inputs and outputs of 'Monitor' activity.

1) IDENTIFY ASPECTS TO IMPROVE

In this activity (fig. 36), the *ACC* will analyze the information from the *TCR*, paying attention not so much to possible deviations, but to the relevant information provided by the different members of the *ACOT*, which may include identified synergies, barriers found, opportunities, difficulties, and so on. The improvements likely to be identified in this activity are, without being an exhaustive list:

- New mechanisms for better coordination between functional areas.
- New mechanisms for better coordination and communication in the *ACC*.
- The need to search for alternatives for the implementation of operational actions that have been more complex or costly to implement in practice than initially planned.
- The use of tools that allow greater agility in work.
- The possibility of including common elements that suppose an optimization of costs and effort.
- The need to reinforce the operational work with new staff.
- Others of a similar nature.

This identification must be the result of a joint debate within the *ACC* and must not focus on the search for solutions, an aspect that is dealt with in the new analysis of the context, but on the identification and documentation of improvement opportunities.

Once this activity is done, the process must iterate again from the activity "Analyze the cyber threats context". Thus, CyberTOMP allows design of a new modified *COP* to include new cybersecurity actions to improve the detected weaknesses and adapt to the dynamic cyber threat context.

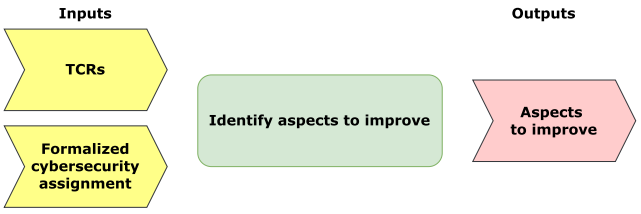


FIGURE 36. Inputs and outputs of 'Identify aspects to improve' activity.

G. PERIODICITY AND END OF THE PROCESS

CyberTOMP only ends when the *TSSC* carries out a new cybersecurity assignment for the same business asset or when it is decided from by strategic sphere of the organization. Otherwise, CyberTOMP will continue even if the *ACES* or *ACIS* has been reached. This is because, as has been commented on throughout this document, that state can change simply because the context changes. For example:

- If the context of cyberspace varies significantly and controls currently in place for the cybersecurity of the asset no longer have the same validity.

TABLE 4. ULEO for 'Identify' function and 'Assets Management' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.AM	CSC-1.1	✓	✓	✓
Identify	ID.AM	CSC-12.4		✓	✓
Identify	ID.AM	CSC-14.1	✓	✓	✓
Identify	ID.AM	CSC-2.2	✓	✓	✓
Identify	ID.AM	CSC-3.1	✓	✓	✓
Identify	ID.AM	CSC-3.2	✓	✓	✓
Identify	ID.AM	CSC-3.6	✓	✓	✓
Identify	ID.AM	CSC-3.7		✓	✓
Identify	ID.AM	ID.AM-1	✓	✓	✓
Identify	ID.AM	ID.AM-2	✓	✓	✓
Identify	ID.AM	ID.AM-2		✓	✓
Identify	ID.AM	ID.AM-3		✓	✓

TABLE 5. ULEO for 'Identify' function and 'Business Environment' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.BE	9D-1		✓	✓
Identify	ID.BE	ID.BE-1			✓
Identify	ID.BE	ID.BE-2			✓
Identify	ID.BE	ID.BE-3			✓
Identify	ID.BE	ID.BE-4			✓
Identify	ID.BE	ID.BE-5			✓

TABLE 6. ULEO for 'Identify' function and 'Governance' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.GV	CSC-17.4		✓	✓
Identify	ID.GV	ID.GV-1	✓	✓	✓
Identify	ID.GV	ID.GV-2		✓	✓
Identify	ID.GV	ID.GV-3			✓
Identify	ID.GV	ID.GV-4			✓

TABLE 7. ULEO for 'Identify' function and 'Risk Assessment' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.RA	9D-1		✓	✓
Identify	ID.RA	CSC-18.2		✓	✓
Identify	ID.RA	CSC-18.5			✓
Identify	ID.RA	CSC-3.7		✓	✓
Identify	ID.RA	ID.RA-1	✓	✓	✓
Identify	ID.RA	ID.RA-2			✓
Identify	ID.RA	ID.RA-3			✓
Identify	ID.RA	ID.RA-4			✓
Identify	ID.RA	ID.RA-6			✓

TABLE 8. ULEO for 'Identify' function and 'Risk Management Strategy' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.RM	9D-8		✓	✓
Identify	ID.RM	ID.RM-1			✓
Identify	ID.RM	ID.RM-2			✓
Identify	ID.RM	ID.RM-3			✓

TABLE 9. ULEO for 'Identify' function and 'Supply Chain Risk Management' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.SC	ID.SC-1		✓	✓
Identify	ID.SC	ID.SC-2	✓	✓	✓
Identify	ID.SC	ID.SC-3		✓	✓
Identify	ID.SC	ID.SC-4			✓
Identify	ID.SC	ID.SC-5	✓	✓	✓

- If there are organizational changes that eliminate, add, or reorganize the functional areas or personnel associated with it.
- If the implemented solutions depend on formalized contracts with service providers that end.
- If the business asset is expanded or reduced with new functionalities or components.
- If employees leave the organization or move horizontally and are replaced by others with different skills or training, or they are not replaced.
- If there is a budget reduction that prevents the maintenance of cybersecurity measures implemented around the asset.

TABLE 10. ULEO for 'Protect' function and 'Identity Management and Access Control' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.AC	CSC-12.5		✓	✓
Protect	PR.AC	CSC-12.6		✓	✓
Protect	PR.AC	CSC-13.4		✓	✓
Protect	PR.AC	CSC-4.7	✓	✓	✓
Protect	PR.AC	CSC-5.2	✓	✓	✓
Protect	PR.AC	CSC-5.6		✓	✓
Protect	PR.AC	CSC-6.8			✓
Protect	PR.AC	PR.AC-1	✓	✓	✓
Protect	PR.AC	PR.AC-2			✓
Protect	PR.AC	PR.AC-3		✓	✓
Protect	PR.AC	PR.AC-3	✓	✓	✓
Protect	PR.AC	PR.AC-4	✓	✓	✓
Protect	PR.AC	PR.AC-5	✓	✓	✓
Protect	PR.AC	PR.AC-6			✓
Protect	PR.AC	PR.AC-7	✓	✓	✓

TABLE 11. ULEO for 'Protect' function and 'Awareness and Training' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.AT	CSC-14.9		✓	✓
Protect	PR.AT	CSC-15.4		✓	✓
Protect	PR.AT	PR.AT-1	✓	✓	✓
Protect	PR.AT	PR.AT-2		✓	✓

TABLE 12. ULEO for 'Protect' function and 'Data Security' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.DS	9D-6			✓
Protect	PR.DS	CSC-3.4	✓	✓	✓
Protect	PR.DS	PR.DS-1		✓	✓
Protect	PR.DS	PR.DS-2		✓	✓
Protect	PR.DS	PR.DS-3	✓	✓	✓
Protect	PR.DS	PR.DS-4			✓
Protect	PR.DS	PR.DS-5			✓
Protect	PR.DS	PR.DS-6		✓	✓
Protect	PR.DS	PR.DS-7		✓	✓
Protect	PR.DS	PR.DS-8			✓

H. RECOMMENDATIONS FOR A CORRECT APPLICATION

Practical implementation of CyberTOMP can be facilitated or improved by applying a series of recommendations:

TABLE 13. ULEO for 'Protect' function and 'Information Protection Processes and Procedures' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.IP	9D-3		✓	✓
Protect	PR.IP	9D-5		✓	✓
Protect	PR.IP	9D-8		✓	✓
Protect	PR.IP	9D-9	✓	✓	✓
Protect	PR.IP	CSC-11.1	✓	✓	✓
Protect	PR.IP	CSC-16.1		✓	✓
Protect	PR.IP	CSC-16.14			✓
Protect	PR.IP	CSC-18.4			✓
Protect	PR.IP	CSC-2.5		✓	✓
Protect	PR.IP	CSC-2.6		✓	✓
Protect	PR.IP	CSC-2.7			✓
Protect	PR.IP	CSC-4.3	✓	✓	✓
Protect	PR.IP	PR.IP-1	✓	✓	✓
Protect	PR.IP	PR.IP-10		✓	✓
Protect	PR.IP	PR.IP-11	✓	✓	✓
Protect	PR.IP	PR.IP-12		✓	✓
Protect	PR.IP	PR.IP-2		✓	✓
Protect	PR.IP	PR.IP-3			✓
Protect	PR.IP	PR.IP-4	✓	✓	✓
Protect	PR.IP	PR.IP-5			✓
Protect	PR.IP	PR.IP-6	✓	✓	✓
Protect	PR.IP	PR.IP-7		✓	✓
Protect	PR.IP	PR.IP-8			✓
Protect	PR.IP	PR.IP-9	✓	✓	✓

TABLE 14. ULEO for 'Protect' function and 'Maintenance' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.MA	9D-5		✓	✓
Protect	PR.MA	9D-9		✓	✓
Protect	PR.MA	CSC-12.1	✓	✓	✓
Protect	PR.MA	CSC-12.3		✓	✓
Protect	PR.MA	CSC-13.5		✓	✓
Protect	PR.MA	CSC-16.13			✓
Protect	PR.MA	CSC-18.3		✓	✓
Protect	PR.MA	CSC-4.2	✓	✓	✓
Protect	PR.MA	CSC-4.6	✓	✓	✓
Protect	PR.MA	CSC-4.8		✓	✓
Protect	PR.MA	CSC-4.9		✓	✓
Protect	PR.MA	CSC-7.3	✓	✓	✓
Protect	PR.MA	CSC-8.1	✓	✓	✓
Protect	PR.MA	CSC-8.10		✓	✓
Protect	PR.MA	CSC-8.3	✓	✓	✓
Protect	PR.MA	CSC-8.9		✓	✓
Protect	PR.MA	PR.MA-1			✓

TABLE 15. ULEO for 'Protect' function and 'Protective Technology' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.PT	9D-4		✓	✓
Protect	PR.PT	9D-7			✓
Protect	PR.PT	CSC-4.12			✓
Protect	PR.PT	CSC-4.4	✓	✓	✓
Protect	PR.PT	CSC-4.5	✓	✓	✓
Protect	PR.PT	CSC-9.5		✓	✓
Protect	PR.PT	PR.PT-1	✓	✓	✓
Protect	PR.PT	PR.PT-2	✓	✓	✓
Protect	PR.PT	PR.PT-3			✓
Protect	PR.PT	PR.PT-4			✓
Protect	PR.PT	PR.PT-5	✓	✓	✓

- **Application of change management techniques**. In the development of our proposal, we understand the following circumstances concur:
  - A collaborative habit is required to reach consensus.
  - By employing three collegiate groups for decision-making, those roles that would normally have the possibility of making decisions individually may understand it as an attack on their competencies and present opposition to the changes.

  To facilitate both, we recommend the professional application of specific techniques for change management that ease the applicability of this proposal. For example, finding change agents to actively participate in the implementation. This change management approach should include training in soft skills that will equip participants with the ability to achieve win-win agreements.
- **The necessary role of CISO**. In light of what is stated in our solution, this could give the impression that the role of the CISO is diluted, becoming a point of potential conflict. It is recommended that the CISO have a relevant leadership role in the *TSSC*. Leadership, not necessarily hierarchical superiority. However, as the role with the most developed skills in cybersecurity, it should be the person responsible for ensuring the correct execution of CyberTOMP and who mediates in the case of conflicts or doubts.
- **Automation**. The use of tools to automate the calculation of metrics and indicators in the cybersecurity evaluation process can significantly facilitate the use of CyberTOMP and the generation of reports. All metrics and indicators have been defined in such a way that they can be easily automated and information can be provided

TABLE 16. ULEO for 'Detect' function and 'Anomalies and Events' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Detect	DE.AE	CSC-8.12			✓
Detect	DE.AE	DE.AE-1		✓	✓
Detect	DE.AE	DE.AE-2		✓	✓
Detect	DE.AE	DE.AE-3	✓	✓	✓
Detect	DE.AE	DE.AE-4			✓
Detect	DE.AE	DE.AE-5			✓

TABLE 17. ULEO for 'Detect' function and 'Security Continuous Monitoring' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Detect	DE.CM	CSC-13.1		✓	✓
Detect	DE.CM	CSC-13.5		✓	✓
Detect	DE.CM	CSC-3.14			✓
Detect	DE.CM	DE.CM-1		✓	✓
Detect	DE.CM	DE.CM-2			✓
Detect	DE.CM	DE.CM-3			✓
Detect	DE.CM	DE.CM-4	✓	✓	✓
Detect	DE.CM	DE.CM-5			✓
Detect	DE.CM	DE.CM-6			✓
Detect	DE.CM	DE.CM-7	✓	✓	✓
Detect	DE.CM	DE.CM-8		✓	✓

TABLE 18. ULEO for 'Detect' function and 'Detection Processes' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Detect	DE.DP	CSC-17.1	✓	✓	✓
Detect	DE.DP	CSC-17.4		✓	✓
Detect	DE.DP	CSC-17.5		✓	✓
Detect	DE.DP	DE.DP-2			✓
Detect	DE.DP	DE.DP-3			✓
Detect	DE.DP	DE.DP-5			✓

at all levels in almost real time, reducing the workload of the *ACC*.

- **Gradual implementation**. A progressive application is recommended, starting with a business asset that is relatively simple to manage and with few functional areas involved, and subsequently including others of greater complexity until this proposal is applied to all the business assets of the organization. The application to simpler cases in the first instance allows the refinement of the process, training of the team and obtaining good results that serve as a hook for the expansion of the solution.

TABLE 19. ULEO for 'Respond' function and 'Analysis' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.AN	CSC-17.9			✓
Respond	RS.AN	RS.AN-1		✓	✓
Respond	RS.AN	RS.AN-2			✓
Respond	RS.AN	RS.AN-3			✓
Respond	RS.AN	RS.AN-5		✓	✓

TABLE 20. ULEO for 'Respond' function and 'Communications' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.CO	CSC-17.4	✓	✓	✓
Respond	RS.CO	CSC-17.5		✓	✓
Respond	RS.CO	RS.CO-5			✓

TABLE 21. ULEO for 'Respond' function and 'Improvements' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.IM	RS.IM-1		✓	✓
Respond	RS.IM	RS.IM-2		✓	✓

TABLE 22. ULEO for 'Respond' function and 'Mitigation' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.MI	CSC-1.2	✓	✓	✓
Respond	RS.MI	CSC-4.10		✓	✓
Respond	RS.MI	CSC-7.7		✓	✓
Respond	RS.MI	RS.MI-1			✓
Respond	RS.MI	RS.MI-2			✓
Respond	RS.MI	RS.MI-3			✓

TABLE 23. ULEO for 'Respond' function and 'Response Planning' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.RP	CSC-17.6		✓	✓
Respond	RS.RP	RS.RP-1			✓

V. CONCLUSION

Tactical and operational levels are responsible for the practical implementation of cybersecurity. The standards used for

TABLE 24. ULEO for 'Recover' function and 'Communications' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Recover	RC.CO	RC.CO-1			✓
Recover	RC.CO	RC.CO-2			✓
Recover	RC.CO	RC.CO-3			✓

TABLE 25. ULEO for 'Recover' function and 'Improvements' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Recover	RC.IM	RC.IM-1			✓
Recover	RC.IM	RC.IM-2			✓

TABLE 26. ULEO for 'Recover' function and 'Recovery Planning' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Recover	RC.RP	RC.RP-1			✓

TABLE 27. Functional areas involved in cybersecurity, reused and improved in our proposal.

FA ID	Main cybersecurity responsibilities
FA1	Physical security
FA2	Security operations
FA3	User education
FA4	Threat intelligence
FA5	Governance
FA6	Enterprise risk management
FA7	Risk assessment
FA8	Application security
FA9	Frameworks and standards
FA10	Security architecture
FA11	Career development
FA12	Corporate communications

TABLE 28. Correspondence between cyberprotection priorities and IGs.

Cyberprotection priority (from BIA)	Corresponding IG
LOW	IG1
MEDIUM	IG2
HIGH	IG3

TABLE 29. Weights of cybersecurity functions for IG1.

F	N_c	W_f
Identify	4	0.27
Protect	6	0.40
Detect	3	0.20
Respond	2	0.13
Recover	0	0.00

TABLE 30. Weights of cybersecurity functions for IG2.

F	N_c	W_f
Identify	6	0.30
Protect	6	0.30
Detect	3	0.15
Respond	5	0.25
Recover	0	0.00

TABLE 31. Weights of cybersecurity functions for IG3.

F	N_c	W_f
Identify	6	0.26
Protect	6	0.26
Detect	3	0.13
Respond	5	0.22
Recover	3	0.13

TABLE 32. Weights for category 'Identify' and IG1.

C	N_o	W_c	W_o
ID.AM	8	0.67	0.125
ID.BE	0	0.00	0.00
ID.GV	1	0.08	1.00
ID.RA	1	0.08	1.00
ID.RM	0	0.00	0.00
ID.SC	2	0.17	0.50

TABLE 33. Weights for category 'Identify' and IG2.

C	N_o	W_c	W_o
ID.AM	12	0.48	$1/12$
ID.BE	1	0.04	1.00
ID.GV	3	0.12	$1/3$
ID.RA	4	0.16	0.25
ID.RM	1	0.04	1.00
ID.SC	4	0.16	0.25

cybersecurity encourage organizations to develop procedural elements for effective cybersecurity management at these levels, but do not provide such a procedural basis so that it can be used as is. This causes indeterminacy in how each organization manages cybersecurity at lower levels, often resulting in a lack of holism, strategic alignment, differing perceptions of the state of cybersecurity or difficulty quickly adapting to a changing cyber threat landscape.

TABLE 34. Weights for category 'Identify' and IG3.

C	N_o	W_c	W_o
ID.AM	12	0.29	$1/12$
ID.BE	6	0.15	$1/6$
ID.GV	5	0.12	0.20
ID.RA	9	0.22	$1/9$
ID.RM	4	0.10	0.25
ID.SC	5	0.12	0.20

TABLE 35. Weights for category 'Protect' and IG1.

C	N_o	W_c	W_o
PR.AC	7	0.24	$1/7$
PR.AT	1	0.03	1.00
PR.DS	2	0.07	0.50
PR.IP	8	0.28	0.125
PR.MA	6	0.21	$1/6$
PR.PT	5	0.17	0.20

TABLE 36. Weights for category 'Protect' and IG2.

C	N_o	W_c	W_o
PR.AC	12	0.19	$1/12$
PR.AT	4	0.06	0.25
PR.DS	6	0.10	$1/6$
PR.IP	18	0.30	$1/18$
PR.MA	15	0.24	$1/15$
PR.PT	7	0.11	$1/7$

TABLE 37. Weights for category 'Protect' and IG3.

C	N_o	W_c	W_o
PR.AC	15	0.19	$1/15$
PR.AT	4	0.05	0.25
PR.DS	10	0.12	0.10
PR.IP	24	0.30	$1/24$
PR.MA	17	0.20	$1/17$
PR.PT	11	0.14	$1/11$

TABLE 38. Weights for category 'Detect' and IG1.

C	N_o	W_c	W_o
DE.AE	1	0.25	1.00
DE.CM	2	0.50	0.50
DE.DP	1	0.25	1.00

TABLE 39. Weights for category 'Detect' and IG2.

C	N_o	W_c	W_o
DE.AE	3	0.25	$1/3$
DE.CM	6	0.50	$1/6$
DE.DP	3	0.25	$1/3$

TABLE 40. Weights for category 'Detect' and IG3.

C	N_o	W_c	W_o
DE.AE	6	0.26	$1/6$
DE.CM	11	0.48	$1/11$
DE.DP	6	0.26	$1/6$

TABLE 41. Weights for category 'Respond' and IG1.

C	N_o	W_c	W_o
RS.RP	0	0.00	0.00
RS.CO	1	0.50	1.00
RS.AN	0	0.00	0.00
RS.MI	1	0.50	1.00
RS.IM	0	0.00	0.00

TABLE 42. Weights for category 'Respond' and IG2.

C	N_o	W_c	W_o
RS.RP	1	0.10	1.00
RS.CO	2	0.20	0.50
RS.AN	2	0.20	0.50
RS.MI	3	0.30	$1/3$
RS.IM	2	0.20	0.50

TABLE 43. Weights for category 'Respond' and IG3.

C	N_o	W_c	W_o
RS.RP	2	0.11	0.50
RS.CO	3	0.17	$1/3$
RS.AN	5	0.28	0.20
RS.MI	6	0.33	$1/6$
RS.IM	2	0.11	0.50

TABLE 44. Weights for category 'Recover' and IG1.

C	N_o	W_c	W_o
RC.RP	0	0.00	0.00
RC.IM	0	0.00	0.00
RC.CO	0	0.00	0.00

Our proposal comprises a common set of expected cybersecurity results rooted in the most recognized cybersecurity standards and initiatives, as well as a set of metrics that allow a homogeneous evaluation of cybersecurity at different levels. This is orchestrated by CyberTOMP, a process for managing cybersecurity at tactical and operational levels.

Together, these elements complement the standard for cybersecurity used at a strategic level, regardless of what

TABLE 45. Weights for category 'Recover' and IG2.

C	N_o	W_c	W_o
RC.RP	0	0.00	0.00
RC.IM	0	0.00	0.00
RC.CO	0	0.00	0.00

TABLE 46. Weights for category 'Recover' and IG3.

C	N_o	W_c	W_o
RC.RP	1	0.17	1.00
RC.IM	2	0.33	0.50
RC.CO	3	0.50	$1/3$

this standard is, being able to be used as is, out of the box, for the holistic management of cybersecurity at all levels while maintaining alignment with the corporate cybersecurity strategy.

This proposal is being implemented in an entity in the Public Sector, a process that will provide the necessary feedback for its evolution and formal validation, results we hope to share with the scientific community in a future study.

APPENDIX A
ULEO TABLES

See Tables 4–26.

APPENDIX B
FUNCTIONAL AREAS INVOLVED IN CYBERSECURITY AND CORRESPONDENCE CYBERPROTECTION PRIORITIES - IGs

See Tables 27 and 28.

APPENDIX C
WEIGHTS OF EVERY CYBERSECURITY FUNCTION, CATEGORY AND EXPECTED OUTCOME

See Tables 29–46.

REFERENCES

[1] F. Y. Sattarova and T. H. Kim, "IT security review: Privacy, protection, access control, assurance and system security," *Int. J. Multimedia Ubiquitous Eng.*, vol. 2, no. 2, pp. 17–32, 2007.

[2] J. L. Fennelly, *Effective Physical Security*. Oxford, U.K.: Butterworth-Heinemann, 2016.

[3] M. E. Whitman and J. Herbert Mattord, *Management of Information Security*. Boston, MA, USA: Cengage Learning, 2013.

[4] R. von Solms, "Information security management: Why standards are important," *Inf. Manage. Comput. Secur.*, vol. 7, no. 1, pp. 50–58, Mar. 1999.

[5] M. E. Whitman and J. H. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2021.

[6] T. Chmielecki, P. Pacyna, P. Potrawka, N. Rapacz, R. Stankiewicz, and P. Wydrych, "Enterprise-oriented cybersecurity management," in *Proc. Ann. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.

[7] N. Kshetri, *Cybersecurity Management: An Organizational and Strategic Approach*. Toronto, ON, Canada: University of Toronto Press, 2021.

[8] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[9] R. Reid and J. Van Niekerk, "From information security to cyber security cultures," in *Proc. Inf. Secur. South Afr.*, Aug. 2014, pp. 1–7.

[10] J. V. D. Ham, "Toward a better understanding of 'Cybersecurity,'" *Digit. Threats, Res. Pract.*, vol. 2, no. 3, pp. 1–3, Sep. 2021.

[11] M. Roopak, G. Y. Tian, and J. Chambers, "An intrusion detection system against DDoS attacks in IoT networks," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2020, pp. 562–567.

[12] R. A. Rothrock, J. Kaplan, and F. Van der Oord, "The board's role in managing cybersecurity risks," *MIT Sloan Manag. Rev.*, vol. 59, no. 2, pp. 12–15, 2018.

[13] K. T. Dean, "Cyber-security holism: A system of solutions for a distributed problem," Marine Corps Command and Staff College, Quantico, VA, USA, Tech. Rep. ADA601717, 2013.

[14] H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 4, pp. 332–340, Dec. 2019.

[15] R. Phillips and B. Tanner, "Breaking down silos between business continuity and cyber security," *J. Bus. Continuity Emergency Planning*, vol. 12, no. 3, pp. 224–232, 2019.

[16] R. Rajan, N. P. Rana, N. Parameswar, S. Dhir, Sushil, and Y. K. Dwivedi, "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management," *Technol. Forecasting Social Change*, vol. 170, Sep. 2021, Art. no. 120872.

[17] I. N. Fovino, "Cybersecurity, our digital anchor," Eur. Union, Luxembourg, Tech. Rep. JRC121051, 2020, doi: 10.2760/352218.

[18] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," *Int. J. Informat. Visualizat.*, vol. 4, no. 4, p. 225, Dec. 2020.

[19] A. Bahuguna, R. K. Bisht, and J. Pande, "Roadmap amid chaos: Cyber security management for organisations," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–6.

[20] R. Miñana. (2021). *?'Qué es Capability Maturity Model Integration? (CMMI)*. Accessed: Jul. 7, 2022. [Online]. Available: https://www2.deloitte.com/es/es/pages/technology/articles/que-es-cmmi-capability-maturity-modelintegration.html

[21] K. Balla, M. Tang, P. Mowat, M. Rasking, S. Chaobo, E. van Veenendaal, and Z. Hongbao, "Changes in CMMI 2.0 and how they can affect TMMi," TMMi Foundation, Bulverde, TX, USA, Tech. Rep., 2020.

[22] ISACA. *CMMI Adoption & Transition Guidance 2021*. Accessed: Jul. 7, 2022. [Online]. Available: https://cmmiinstitute.com/getattachment/5868888b-5f37-4715-bc8b-c43250ec0abc/attachment.aspx

[23] C. Agutter, "ITIL 4 essentials, second edition," IT Governance Publishing Ltd., Cambridge, U.K., Tech. Rep. 5524, 2020.

[24] *ITIL Foundation. ITIL 4 Edition. Glossary*, Axelos, London, U.K., 2019.

[25] R. Jašek, L. Králík, and M. Popelka, "ITIL and information security," in *Proc. AIP Conf.*, Helsinki, 2015, Art. no. 550020.

[26] E. R. Larrocha, G. Díaz, J. M. Minguet, M. Castro, and A. Vara, "Filling the gap of information security management inside ITIL: Proposals for posgraduate students," in *Proc. IEEE EDUCON Conf.*, Apr. 2010, pp. 907–912.

[27] J. Gillingham. (Aug. 2021). *An Introduction To Information Security Management in ITIL*. Accessed: Jul. 7, 2022. [Online] Available: https://www.invensislearning.com/blog/information-security-management/

[28] *UNE-ISO/IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información (SGSI) Requisitos*. AENOR, Madrid, Spain, 2014

[29] *UNE-ISO/IEC 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Prácticas Para Los Controles de Seguridad de la Información*, AENOR, Madrid, Spain, 2015.

[30] H. R. Suárez, J. D. P. Álvarez, and M. G. Hidalgo, "Ciber-resiliencia. Aproximación a un marco de medición," Nat. Inst. Commun. Technol. (INTECO), Tech. Rep., 2014.

[31] *IMC_01—Metodología de Evaluación de Indicadores Para Mejora de la Ciberresiliencia (IMC)*, Spanish Nat. Cybersecur. Inst. (INCIBE), 2020.

[32] G. D. España, "Real decreto 311/2022, de 3 de mayo, por el que SE regula el esquema nacional de seguridad," *Boletín Oficial del Estado*, vol. 106, pp. 61715–61804, May 2020.

[33] CCN. *Guías Esquema Nacional de Seguridad 2022*. Accessed: Jul. 7, 2022. [Online] Available: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

[34] *Guía de Seguridad CCN-STIC-806. Esquema Nacional de Seguridad, Plan de Adecuación*, Centro Criptológico Nacional, Madrid, Spain, 2011.

[35] Centro Criptológico Nacional. (2021). *Adecuación al ENS y Seguimiento del Progreso*. Accessed: Jul. 7, 2022. [Online]. Available: https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia/2-uncategorised/48-adecuacion-al-ens-y-seguimiento-del-progreso.html
[36] MITRE. *MITRE ATT&CK©, 2021*. Accessed: Jul. 7, 2022. [Online] Available: https://attack.mitre.org/
[37] E. S. Blake, A. Andy, P. M. Doug, C. N. Kathryn, G. P. Adam, and B. T. Cody, "MITRE ATT&CK©: Design and philosophy," MITRE, McLean, VA, USA, Tech. Rep., 2020
[38] R. Kwon, T. Ashley, J. Castleberry, and S. N. G. Gourisetti, "Cyber threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping," in *Proc. Resilience Week (RWS)*, Oct. 2020.
[39] W. Xiong, E. Legrand, and O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE Enterprise ATT&CK matrix," *Softw. Syst. Model.*, vol. 21, pp. 157–177, Jun. 2021.
[40] *CIS Security Controls, Version 8*, CIS, East Greenbush, NY, USA, 2021
[41] B. Shamma, *Implementing CIS Critical Security Controls for Organizations on a Low-Budget*. Ann Arbor, MI, USA: ProQuest LLC, 2018.
[42] S. Gros, "A critical view on CIS controls," in *Proc. 16th Int. Conf. Telecommun. (ConTEL)*, Jun. 2021, pp. 122–128.
[43] OWASP. (2021). *OWASP TOP 10 Project*. Accessed: Jul. 7, 2022. [Online] Available: https://owasp.org/www-project-top-ten/
[44] M. Bach-Nutman, "Understanding the top 10 OWASP vulnerabilities," 2020, *arXiv:2012.09960*.
[45] *Center for Internet Security, CIS Community Defense Model, Version 2.0*, CIS, East Greenbush, NY, USA, 2021.
[46] MITRE. (2022). *MITRE ATT&CK© Enterprise Mitigations*. Accessed: Jul. 7, 2022. [Online] Available: https://attack.mitre.org/mitigations/enterprise/
[47] K. S. Wilson and M. A. Kiy, "Some fundamental cybersecurity concepts," *IEEE Access*, vol. 2, pp. 116–124, 2014.
[48] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST, Gaithersburg, MD, USA, 2018
[49] Organización de los Estados Americanos y AWS, "Ciberseguridad, marco NIST. Un abordaje integral de la ciberseguridad," Org. Amer. States (OEA), USA, White Paper, 5th ed. OEA, 2019.
[50] NIST Computer Security Resource Center. *SP 800 Series, 2021*. Accessed: Jul. 7, 2022. [Online] Available: https://csrc.nist.gov/publications/sp800
[51] *NIST Special Publication 800–53. Revision 5. Security and Privacy Controls for Information Systems and Organizations*, NIST, Gaithersburg, MD, USA, 2020
[52] *Adquisition and sustainment, Cybersecurity Maturity Model Certification (CMMC) Model Overview. Version 2.0*, Office of the Under Secretary of Defense, Department of Defense, Richmond, VA, USA, 2021
[53] Office of the Under Secretary of Defense. (Dec. 2021). *Adquisition and Sustainment, CMMC 2.0 Spreadsheet and Mapping*. Accessed: Jul. 7, 2022. [Online] Available: https://www.acq.osd.mil/cmmc/docs/CMMCModel_V2_Mapping.xlsx
[54] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrepreneurship Sustainability Issues*, vol. 4, no. 4, pp. 559–573, 2017, doi: 10.9770/jesi.2017.4.4(12).
[55] M. Tvaronaviciene, T. Pleta, and S. D. Casa, "Cyber security management model for critical infrastructure protection," in *Proc. Int. Sci. Conf. Contemp. Issues Bus., Manag. Econ. Eng.*, 2021, pp. 133–139.
[56] K. Barbara, E. W. N. Bernroider, and R. Walser, "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework," in *Proc. Nordic Conf. Secure IT Syst.*, Cham, Switzerland: Springer, 2018, pp. 369–384.
[57] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal," *J. Reliable Intell. Environments*, vol. 7, no. 2, pp. 69–84, Jun. 2021.
[58] L. Maximilian, E. Markl, and M. Aburaia, "Cybersecurity management for (industrial) Internet of Things-challenges and opportunities," *J. Inf. Technol. Softw. Eng.*, vol. 8, no. 5, pp. 1–9, 2018.
[59] S. Ali, "Cybersecurity management for distributed control system: Systematic approach," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 11, pp. 10091–10103, Nov. 2021.
[60] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020.
[61] F. Alrimawi, L. Pasquale, and B. Nuseibeh, "On the automated management of security incidents in smart spaces," *IEEE Access*, vol. 7, pp. 111513–111527, 2019.
[62] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information security and cybersecurity management: A case study with SMEs in Portugal," *J. Cybersecurity Privacy*, vol. 1, no. 2, pp. 219–238, Apr. 2021.
[63] M. S. Tisdale, "Architecting a cybersecurity management framework," *Issues Inf. Syst.*, vol. 17, no. 4, pp. 1–284, 2016.
[64] L. Axon, A. Erola, A. Janse van Rensburg, J. R. C. Nurse, M. Goldsmith, and S. Creese, "Practitioners' views on cybersecurity control adoption and effectiveness," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Aug. 2021, pp. 1–10.
[65] United States Government Accountability Office, "Critical infrastructure protection. Sector-specific agencies need better measure cybersecurity progress," U.S. Government Accountability Office (GAO), USA, Tech. Rep. GAO-16-79, 2015.
[66] T. Kissoon, "Optimum spending on cybersecurity measures," *Transforming Government, People, Process Policy*, vol. 14, no. 3, pp. 417–431, doi: 10.1108/TG-11-2019-0112.
[67] J. Breier and L. Hudec, "On selecting critical security controls," in *Proc. Int. Conf. Availability, Rel. Secur.*, Sep. 2013, pp. 582–588.
[68] P. Speight, "Business continuity," *J. Appl. Secur. Res.*, vol. 6, no. 4, pp. 529–554, 2011.
[69] B. Zawada, "The practical application of ISO 22301," *J. Bus. Continuity Emergency Planning*, vol. 8, no. 1, pp. 83–90, 2014.
[70] M. H. Bejarano, R. J. Rodriguez, and J. Merseguer, "A vision for improving business continuity through cyber-resilience mechanisms and frameworks," in *Proc. 16th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2021, pp. 1–5.
[71] R. L. Tammineedi, "Business continuity management: A standards-based approach," *Inf. Secur. J., A Global Perspective*, vol. 19, no. 1, pp. 36–50, Mar. 2010.
[72] M. Clark, J. Espinosa, and W. Delone, "Defending organizational assets: A preliminary framework for cybersecurity success and knowledge alignment," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2020, pp. 4283–4292.
[73] H. Kure, S. Islam, and M. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Appl. Sci.*, vol. 8, no. 6, p. 898, May 2018.
[74] A. Couce-Vieira, D. R. Insua, and A. Kosgodagan, "Assessing and forecasting cybersecurity impacts," *Decis. Anal.*, vol. 17, no. 4, pp. 356–374, Dec. 2020.
[75] Z. A. Collier and I. Linkov, and J. H. Lambert, "Four domains of cybersecurity: A risk-based systems approach to cyber decisions," *Environ. Syst. Decis.*, vol. 33, pp. 2194–5411, Nov. 2013.
[76] A. M. Rea-Guaman, J. Mejía, T. San Feliu, and J. A. Calvo-Manzano, "AVARCIBER: A framework for assessing cybersecurity risks," *Cluster Comput.*, vol. 23, no. 3, pp. 1827–1843, Sep. 2020.
[77] C. T. Harry and N. Gallagher, "An effects-centric approach to assessing cybersecurity risk," Center Int. Secur. Stud., Univ. Maryland, College Park, MD, USA, Tech. Rep. resrep20424, 2019.
[78] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Anal.*, vol. 40, no. 1, pp. 183–199, Jan. 2020.
[79] J. R. S. Cristóbal, "Complexity in project management," *Proc. Comput. Sci.*, vol. 121, pp. 762–766, Jan. 2017.
[80] CIS. (2021). *CIS Critical Security Controls V8 Mapping to NIST CSF*. Accessed: Jul. 7, 2022. [Online] Available: https://www.cisecurity.org/white-papers/cis-controlsv8-mapping-to-nist-csf/
[81] NIST. (2021). *Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5*. Accessed: Sep. 23, 2022. [Online] Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx
[82] H. Jiang. (2021). *Cybersecurity Domain Map Ver 3.0*. Accessed: Jul. 7, 2022. [Online]. Available: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/
[83] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," *J. Assoc. Inf. Sci. Technol.*, vol. 71, no. 8, pp. 939–953, Aug. 2020.
[84] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100361.
[85] H. I. Kure, S. Islam, M. Ghazanfar, A. Raza, and M. Pasha, "Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system," *Neural Comput. Appl.*, vol. 34, no. 1, pp. 493–514, Jan. 2022.

[86] A. Zimmermann, *Gestión del Cambio Organizacional: Caminos y Herramientas*, 2nd ed. Quito: Ediciones Abya-Yala, 2000.
[87] *A guide to the Project Management Body of Knowledge. PMBoK Guide*. 7th ed., Project Management Institute, Newtown Square, PA, USA, 2021.

MANUEL DOMÍNGUEZ-DORADO received the B.Sc. and M.Sc. degrees in computer science from the University of Extemadura and the master's degree in cybersecurity management (CISO) from the International Institute for Global Security Studies. He worked as a Researcher with the University of Extemadura. Nowadays, he works as the Cybersecurity Manager of the Public Business Entity Red.es. His research interests include cybersecurity in organizations and in communications networks and cybersecurity management.

JAVIER CARMONA-MURILLO received the Ph.D. degree in computer science and communications from the University of Extremadura, Spain, in 2015. From 2005 to 2009, he was a Research and Teaching Assistant. Since 2009, he has been an Associate Professor with the Department of Computing and Telematics System Engineering, Universidad de Extremadura. During the past years, he has spent research periods with the Centre for Telecommunications Research, King's College London, U.K., and Aarhus University, Denmark. His current research interests include 5G networks, mobility management protocols, performance evaluation, and the quality of service support in future mobile networks.

DAVID CORTÉS-POLO received the degree in computer science from the University of Extremadura, Spain, and the Ph.D. degree in telematics from the University of Extremadura, in 2015. From 2011 to 2014, he worked as a Researcher and a Teaching Assistant with the University of Extremadura. From 2020 to 2022, he was an Associate Professor with the Department of Computing and Telematics System Engineering, Universidad de Extremadura. Since September 2022, he has been an Assistant Professor at King Juan Carlos University, Madrid. His research interests include IP-based mobility management protocols, performance evaluation, and network CDR analytics.

FRANCISCO J. RODRÍGUEZ-PÉREZ received the degree in computer science engineering and the Ph.D. degree from the University of Extremadura, Spain, in 2000 and 2015, respectively. His research interests include the design and implementation of algorithms and signaling techniques to improve reliability, performance, delay, computing load, and energy consumption, and other metrics of prioritized quality of service aware flows over multiprotocol label switching packet transport networks, the Internet of Things systems, wireless *ad-hoc* networks, and smart cities environments.