



TESIS DOCTORAL

**Gestión y evaluación holística de la
ciberseguridad en el Sector Público**

Manuel Domínguez Dorado

PROGRAMA DE DOCTORADO EN TECNOLOGÍAS INFORMÁTICAS

Con la conformidad de los directores

Dr. Francisco Javier Rodríguez Pérez y Dr. David Miguel Cortés Polo

Esta tesis cuenta con la autorización del director y codirector de la misma y de la Comisión Académica del programa. Dichas autorizaciones constan en el Servicio de la Escuela Internacional de Doctorado de la Universidad de Extremadura

Cáceres, 2024

“Daría todo lo que sé, por la mitad de lo que ignoro.”

René Descartes

PREFACIO

Esta tesis, presentada como un compendio de artículos, ha sido remitida de acuerdo con los requisitos de la Universidad de Extremadura para la consecución del título de Doctor en el Programa Doctoral de Tecnologías Informáticas. Los doctores Francisco Javier Rodríguez Pérez y David Miguel Cortés Polo han supervisado la investigación presentada en este documento. Los resultados de investigación han sido desarrollados principalmente en la Universidad de Extremadura.

AGRADECIMIENTOS

Después de un largo recorrido que se extiende desde mis estudios universitarios de primer, segundo y tercer ciclo hasta el intento inicial frustrado de completar una tesis doctoral, hoy me encuentro ante la culminación de este viaje académico. Este logro marca el cierre de una etapa y la sanación de una herida que ha persistido durante décadas. Cada paso, cada obstáculo, ha contribuido a mi crecimiento personal y profesional y no cambiaría ni un detalle de este camino.

En este proceso, he sido acompañado por seres queridos que me han brindado su apoyo incondicional. A mi esposa Elena y mi hija Claudia, les agradezco por haber comprendido la importancia de este proyecto en mi vida, incluso en los momentos en que la dedicación a la investigación significaba sacrificar tiempo en familia. Agradezco también al resto de mi familia, desde mi madre hasta mis sobrinos, cuyo aliento ha sido fundamental en este recorrido.

Quiero expresar mi profundo agradecimiento a mis directores de tesis, Paco y David, quienes no solo me guiaron académicamente, sino que también me brindaron su amistad y compañerismo a lo largo de los años. Su acompañamiento y orientación han sido cruciales para llegar a este punto. Además, valoro enormemente el estilo de dirección generoso que han adoptado, centrado en mi crecimiento como investigador.

No puedo dejar de mencionar al grupo de investigación GÍTACA, cuya colaboración y recursos han sido fundamentales para el desarrollo de mi tesis doctoral. A todos sus miembros, especialmente a Javi, les estoy profundamente agradecido por su apoyo.

Aunque por motivos de confidencialidad permanezcan en el anonimato, agradezco a las dos organizaciones que se han prestado a poner en práctica los distintos resultados de la tesis, para aportar sus impresiones y retroalimentar los trabajos de investigación.

Debo reconocer igualmente la contribución de numerosos investigadores a lo largo del mundo cuyos trabajos han servido como base para mi investigación. Aunque sus nombres están referenciados en mi tesis y en los artículos que he publicado, quiero expresar mi gratitud expresamente por su invaluable aporte al campo académico.

Finalmente, deseo dar las gracias a aquellas pocas personas que, desde el final de mis estudios de doctorado, intentaron obstaculizar mi camino. A pesar de los desafíos que enfrenté, estas experiencias me enseñaron importantes lecciones que contribuyeron a mi crecimiento personal y reafirmaron mi determinación de seguir adelante en mi carrera investigadora.

A todos ellos, les dedico esta tesis doctoral.

Manuel Domínguez Dorado

Cáceres, España, 2024

RESUMEN

En el contexto actual de ciberseguridad, existe un panorama creciente de ciberamenazas y una probabilidad, igualmente creciente, de que estas se transformen en ciberriesgos aprovechando las debilidades de las organizaciones y exponiéndolas, por tanto, a potenciales impactos. En dicho contexto, esta tesis aborda el objetivo de desarrollar un modelo que facilite a las entidades del Sector Público la gestión de la ciberseguridad, centrada en el activo de negocio, desde niveles tácticos y operativos, conservando el holismo y la unidad de acción requerida.

El aumento de la digitalización en las organizaciones a lo largo del tiempo ha provocado que éstas hayan considerado como esenciales distintos activos en diferentes momentos. Inicialmente el hardware era por sí mismo uno de los activos con mayor relevancia, posteriormente la información ocupó su lugar y, en la actualidad, la propia continuidad operativa de la organización, la confiabilidad que ésta puede ofrecer a terceros o la reputación, se encuentran entre los aspectos más críticos para cualquier entidad digitalizada. Es por ello que la tesis adopta el activo de negocio como unidad de referencia para la gestión de la ciberseguridad. La digitalización ha llevado, además, a las organizaciones a una dependencia creciente del ciberespacio, donde el control directo sobre los activos de los que dependen es muy reducido.

El perímetro de las organizaciones, en este mismo proceso, se ha ido difuminando y ha pasado de estar completamente contenido en las instalaciones físicas de la organización a, en la actualidad, sobrepasar los límites de esta y fusionarse, a través del ciberespacio, con terceros, con sus propios empleados, clientes, proveedores o socios. Esta difuminación progresiva de los límites de la propia organización ha requerido de la participación de más personas en la ciberseguridad, desde departamentos individuales hasta toda la organización e incluso entidades de la cadena de suministro. Las amenazas y riesgos para las organizaciones han variado de igual forma, dando lugar a diferentes enfoques de seguridad como la seguridad física, de la información y la ciberseguridad, que han evolucionado consecutivamente a modo de muñecas *Matrioska* para cubrir las nuevas necesidades. Sin embargo, la evolución de la tecnología no ha seguido una progresión lineal, sino que ha sido, y está siendo, un proceso explosivo con un reflejo directo en la rapidez con la que las organizaciones se ven avocadas a digitalizarse y asumir la dependencia del ciberespacio para no quedar atrás. Pero ese ritmo incesantemente acelerado ha dificultado el desarrollo simultáneo de los marcos de trabajo específicos junto con las capacidades y cultura de ciberseguridad necesarias. Esto ha llevado a situaciones donde los enfoques de seguridad de la información se aplican a escenarios que requieren ciberseguridad, impidiendo abordar las ciberamenazas de forma adecuada.

Además de esa falta de adaptación a la ciberseguridad, los modelos y estándares existentes aplicados comúnmente a la ciberseguridad tienen otras carencias. Una de ellas, relevante, es que suelen definir muy bien su aplicación a nivel estratégico pero rara vez profundizan y desarrollan los elementos procedimentales requeridos para el resto de los niveles de la organización. Es decir, no detallan de forma clara cómo la aplicación de ese estándar o marco debe capilarizar al resto de niveles organizativos y dejan a la interpretación de cada organización el desarrollo de toda esa parte, dando lugar a implementaciones del mismo completamente diferente entre organizaciones, o entre distintos departamentos de una misma organización o, en muchas ocasiones,

dejando un vacío que afecta a los niveles tácticos y operativos, máximos encargados de desarrollar la estrategia en ciberseguridad. Esta indefinición impide también establecer políticas de seguridad que se extiendan a entidades de la cadena de suministros de una forma homogénea y en general impide una acción conjunta de ciberseguridad. Otra carencia notable es la referida a las métricas. Estos modelos en raras ocasiones incorporan métricas y, cuando lo hacen, estas métricas están definidas de una forma que son sólo útiles a medio o largo plazo para los niveles estratégicos de la organización. Pero en general no incorporan un conjunto de métricas concretas que permitan la evaluación de la ciberseguridad tanto a los niveles estratégicos, como también a los niveles tácticos u operativos (largo plazo, medio plazo y corto plazo, respectivamente). Por ello, estos niveles no cuentan con herramientas que le permitan valorar el efecto de las actuaciones de ciberseguridad y adaptarlas al contexto cambiante de ciberamenazas para contribuir a los objetivos estratégicos de ciberseguridad, teniendo que desarrollar su trabajo con una visibilidad muy limitada. Por último, los modelos existentes son en su mayor parte evoluciones de los modelos de seguridad de la información que arrastran un sesgo notable respecto al conjunto de disciplinas que deberían contribuir a lograr un estado de ciberseguridad elevado en la organización. No contemplan, por decirlo así, el enfoque completamente holístico que requiere la ciberseguridad, con implicación de toda la organización, por lo que su aplicación práctica, per se, no puede derivar en una gestión holística de la ciberseguridad. A modo de resumen, estos modelos y estándares no constituyen marcos exhaustivos que alineen la acción en ciberseguridad tanto horizontal como verticalmente, no proporcionan un conjunto uniforme de procedimientos ni métricas de ciberseguridad adecuadas para todos los niveles, ni permiten una acción conjunta, como requiere la ciberseguridad.

Esta tesis desarrolla el cuerpo procedimental requerido por los niveles tácticos y operativos de las entidades públicas para facilitar la gestión holística de la ciberseguridad corporativa y su adaptación al contexto cambiante de ciberamenazas. Un modelo que puede ser aplicado con independencia del marco estratégico superior utilizado en la misma. Esto es, independiente del estándar de seguridad utilizado en la organización, se adapta y alinea con el que se esté utilizando, permitiendo un trabajo holístico cuasi autónomo y coordinado en los niveles inferiores o en la cadena de suministro. Dicho modelo tiene sus raíces en las iniciativas, marcos y buenas prácticas de ciberseguridad más reconocidos. Sobre ellos se ha realizado un análisis detallado como parte de los trabajos de investigación, buscando puntos comunes de alineación con los estándares de seguridad más implantados a nivel estratégico en las organizaciones.

Para contribuir a facilitar la implantación de dicho modelo, la tesis aborda el campo de los algoritmos evolutivos de optimización multicriterio, desarrollando algoritmos genéticos y herramientas basadas en ellos. Estos desarrollos, aplicados como parte del marco, permiten a dichos niveles mejorar la eficiencia en la toma de decisiones respecto a las actuaciones necesarias para la consecución de los objetivos de ciberseguridad, cualquiera que sea el nivel de la organización, o de su cadena de suministro, sobre el que se hayan definido dichos objetivos.

Para el seguimiento del nivel de cumplimiento de dichos objetivos el modelo desarrollado proporciona un conjunto de métricas que pueden ser agregadas de forma ascendente, esto es, parten del nivel operativo y se propagan hasta el nivel estratégico pasando por el nivel táctico de la organización. Esta concepción de las métricas permite que las mismas aporten valor a todos los niveles, supliéndoles con la

información que cada uno de ellos necesita, pero manteniendo la coherencia y la homogeneidad a lo largo y ancho de la organización. Estas métricas, que han sido validadas por la comunidad científica en las publicaciones correspondientes, son independientes del campo de conocimiento desde el que se deban implementar las actuaciones de ciberseguridad que correspondan y también son también de aplicación en un contexto donde parte de ellas deban transferirse a servicios externalizados a entidades de la cadena de suministro.

Para asegurar que el modelo cubre particularmente los requisitos del Sector Público, los trabajos de investigación de la tesis han abordado el análisis de la problemática relacionada con la gestión de la ciberseguridad en relación con las especificidades de los organismos públicos. Estas especificidades incluyen la práctica habitual de la externalización o la composición mixta de sus equipos de trabajo, con personal propio y de terceros que les proporcionan servicios. También se han analizado sus dificultades específicas para atraer y retener talento en ciberseguridad, la rigidez de su estructura y, en general, la necesidad que tienen de contratar servicios de seguridad gestionada con empresas del sector privado. Los resultados complementan el modelo con la aportación de mecanismos y técnicas para la contratación de servicios de ciberseguridad con terceros. Adicionalmente los trabajos realizados incluyen la identificación de habilidades y capacidades en ciberseguridad requeridas por las entidades del Sector Público, la identificación de requisitos exigibles a entidades proveedoras en el caso de externalización y la capacitación de los equipos multidisciplinares para su implicación en la ciberseguridad corporativa.

Los resultados de estos trabajos de investigación y la aplicación práctica experimental del marco de gestión desarrollado en la tesis, permiten considerarlo como una herramienta útil capaz de coexistir sin conflictos, en la gestión de la ciberseguridad, con la aplicación de los estándares de seguridad aplicados en niveles estratégicos. Asimismo, proporciona un nivel elevado de visibilidad sobre el estado de ciberseguridad de cada activo de la organización y sobre aquellas acciones que hay que emprender para mejorarlo. Eleva la concienciación de los equipos multidisciplinares sobre la contribución específica de su campo de conocimiento a la ciberseguridad global de la organización y facilita a ésta la identificación explícita de requisitos multidisciplinares relativos a la ciberseguridad que deben ser exigidos a terceros de la cadena de suministro o entrenados internamente. Todo lo anterior, orquestado mediante procesos homogéneos que cubren toda la organización y la cadena de suministro, desarrollados *ex profeso* en la tesis.

Estos mismos resultados han abierto la puerta a futuras líneas de investigación. Específicamente, la aplicación de gemelos digitales para evaluar a la organización respecto a escenarios de ciberriesgos concretos y la aplicación del marco para entrenar a los equipos multidisciplinares en conciencia situacional en ciberseguridad o la posibilidad de realizar predicciones sobre la aplicación del marco.

Palabras clave – gestión táctico-operativa de la ciberseguridad, ciberseguridad holística, ciberseguridad para el activo de negocio, ciberseguridad en el Sector Público.

CONTENIDO

Prefacio	i
Agradecimientos	iii
Resumen	v
Lista de abreviaturas y glosario	xi
Introducción	1
Trasfondo y motivaciones	3
Evolución de los activos prioritarios en las organizaciones.....	4
Evolución vertiginosa en el proceso de digitalización	4
Evolución de los estándares de gestión de la seguridad	6
Evolución de las fronteras de las organizaciones	8
Evolución de la participación en ciberseguridad: holismo	9
Las entidades del Sector Público	10
Objetivos y metodología de investigación	12
Resultados de la tesis y colaboraciones	14
Modelo de gestión y evaluación holística de la ciberseguridad	17
Soluciones algorítmicas para la optimización	51
Soluciones tecnológicas para facilitar la implantación práctica	69
Extensiones metodológicas para la ciberseguridad de la cadena de suministro	75
Detección y mitigación de ciberamenazas usando VNFs en SDNs.....	107
Conclusiones y trabajo futuro	125
Conclusiones	127
Trabajo futuro	129
Referencias.....	133

LISTA DE ABREVIATURAS Y GLOSARIO

Algoritmo evolutivo de optimización multicriterio	Un algoritmo evolutivo de optimización multicriterio es una técnica basada en los principios de la evolución natural que busca soluciones óptimas para problemas con múltiples objetivos en conflicto, utilizando procesos de selección, cruce y mutación para evolucionar una población de soluciones hacia un conjunto de soluciones de compromiso.
Algoritmo genético	Un algoritmo genético es un método de optimización y búsqueda basado en los principios de la selección natural y la genética, que utiliza técnicas como la mutación, el cruce y la selección para evolucionar soluciones a problemas complejos a lo largo de varias generaciones.
Ciberactivista	Grupo de ciberatacantes cuya finalidad principal es la protesta o reivindicación de ideas, generalmente de índole político o social.
Ciberamenaza	Probabilidad de existencia de un evento negativo, emanado del ciberespacio, con potenciales efectos negativos sobre la organización
Ciberatacante	Actor malicioso que perpetra un ciberataque. Existen diversas clasificaciones, si bien es común la que distingue los ciberatacantes según su nivel de conocimiento y los recursos de los que dispone: principiante, ciberatacante experto solitario, grupo ciberactivista, grupo de ciberdelincuencia organizada, ciberatacantes soportados por un estado.
Ciberataque	Ciberamenaza intencional enfocada en robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones, reputación o u otros activos o interrumpir la continuidad de servicios y actividades, utilizando el ciberespacio.
Ciberespacio	Conjunto de sistemas de información interconectados a través de redes propiedad de múltiples actores, en la cual empresas, organizaciones y usuarios desarrollan sus actividades y operaciones.
Ciberincidente	Materialización fehaciente de una ciberamenaza debido a la existencia de una debilidad.
Ciberresiliencia	Capacidad de una organización de resistir y recuperarse de un ciberincidente.
Ciberriesgo	Probabilidad de que se produzcan impactos sobre la organización por la materialización de una ciberamenaza aprovechando una debilidad.

Ciberseguridad	Disciplina/enfoque especialmente indicado para afrontar las amenazas emanadas de la dependencia de las organizaciones del ciberespacio.
Ciberseguridad holística	La ciberseguridad holística es un enfoque integral de la ciberseguridad que considera todos los elementos interrelacionados, incluyendo personas, procesos, tecnología y entorno, de todos los campos de conocimiento de la organización, para asegurar la defensa completa y efectiva contra ciberamenazas.
CyberSOC	Centro de operaciones de ciberseguridad. Es una unidad centralizada en una organización que se dedica a monitorizar, detectar, responder y gestionar incidentes de seguridad informática. Su principal objetivo es proteger los sistemas de información y datos sensibles de la organización contra ciberataques y otras amenazas cibernéticas
Conciencia situacional	La conciencia situacional es la percepción y comprensión de los elementos y eventos que ocurren en un entorno específico, así como la capacidad de anticipar cómo estos factores pueden influir en futuras condiciones y decisiones.
Debilidad/Vulnerabilidad	En relación con la ciberseguridad, carencia de una organización que puede facilitar que se materialice una ciberamenaza.
Gemelo digital	Un gemelo digital es una réplica virtual precisa de un objeto, sistema o proceso físico real, sincronizada con éste, que se utiliza para simular, analizar y optimizar su rendimiento mediante la recopilación y el procesamiento de datos del mundo real.
Gobernanza	En una organización, y en relación con la ciberseguridad, la gobernanza es el conjunto de políticas, procedimientos y estructuras organizativas que gestionan y dirigen la protección de los activos de la organización contra ciberamenazas. Incluye la implementación de estrategias, el cumplimiento de normativas y la asignación de responsabilidades, entre otros aspectos.
Holismo	El holismo es una teoría o enfoque que sostiene que los sistemas y sus propiedades deben ser analizados en su totalidad, y no solamente a través de las partes que los componen, ya que el comportamiento y las propiedades del todo no pueden ser completamente entendidos solo a partir de la suma de sus partes.
Internet oscura (Dark Web)	Capa de Internet, no accesible mediante los buscadores tradicionales, oculta tras protocolos de encaminamiento y conexiones que garantizan el anonimato y comúnmente utilizada por los cibercriminales para planificar y coordinar ciberataques, así como vender

	<p>productos y servicios de apoyo a los mismos. También para vender los datos e información resultante de la ejecución de dichos ciberataques.</p>
ISO 27000	<p>Familia de normas estandarizadas por ISO (<i>International Organization for Standardization</i>) enfocadas a la seguridad de la información. De ellas, la más conocida, por ser una norma certificable, es la ISO 27001, que cubre los aspectos necesarios para el establecimiento de un sistema de gestión de seguridad de la información.</p>
Mainframe	<p>Un mainframe es una computadora de gran tamaño y alta capacidad de procesamiento, diseñada para manejar grandes volúmenes de datos y aplicaciones críticas en una organización.</p>
Nivel estratégico	<p>En una organización, y en relación con la ciberseguridad, el conjunto de personas encargadas de la gobernanza de la ciberseguridad. Su actividad habitualmente se sitúa en el largo plazo y sus objetivos son objetivos estratégicos de ciberseguridad. Su composición generalmente comprende distintos campos de conocimiento. Jerárquicamente se sitúa en la posición más alta de la organización.</p>
Nivel táctico	<p>En una organización, y en relación con la ciberseguridad, el conjunto de personas encargadas de la planificación de proyectos y actuaciones de ciberseguridad. Su actividad habitualmente se sitúa en el medio plazo y sus objetivos son objetivos tácticos de ciberseguridad. Su composición generalmente comprende distintos campos de conocimiento. Jerárquicamente se sitúa en una posición intermedia en la organización.</p>
Nivel operativo	<p>En una organización, y en relación con la ciberseguridad, el conjunto de personas encargadas de la implementación práctica de las actuaciones de ciberseguridad. Su actividad habitualmente se sitúa en el corto plazo y sus objetivos son objetivos operativos de ciberseguridad. Su composición generalmente comprende distintos campos de conocimiento. Jerárquicamente se sitúa en la posición más baja de organización.</p>
Niveles inferiores	<p>En el contexto de este documento, los niveles inferiores son el táctico y el operativo.</p>
Seguridad de la información	<p>Disciplina/enfoque especialmente indicado para afrontar las amenazas emanadas de la dependencia de las organizaciones de la información gestionada por sus sistemas de información.</p>
Seguridad física	<p>Disciplina/enfoque especialmente indicado para afrontar las amenazas emanadas de la dependencia de las</p>

	organizaciones de instalaciones de procesos de datos y comunicaciones e instalaciones físicas en general.
Seguridad informática o IT	Disciplina/enfoque especialmente indicado para afrontar las amenazas emanadas de la dependencia de las organizaciones del hardware, el software y las comunicaciones.
Silo organizacional	Término utilizado en el ámbito empresarial para describir una situación en la que diferentes departamentos, equipos o unidades dentro de una organización operan de manera aislada y no comparten información, recursos, ni colaboran entre sí de manera efectiva. Estos "silos" pueden llevar a una falta de comunicación y coordinación, lo que puede reducir la eficiencia y efectividad de la organización en su conjunto.
Tecnologías disruptivas	Las tecnologías disruptivas son innovaciones tecnológicas que alteran significativamente la forma en que funcionan las industrias, los mercados o las sociedades.

1

INTRODUCCIÓN

Este capítulo se adentra en el trasfondo y las motivaciones de la tesis, destacando la necesidad de un modelo de gestión de ciberseguridad que orqueste todas las actividades para proporcionar un enfoque holístico desde los niveles inferiores de la organización, con capacidad de autoorganización. Se argumenta que este enfoque permite amortiguar mejor los cambios en el contexto de ciberamenazas, cuya dinámica y rápida evolución no pueden abordarse fácilmente desde niveles superiores debido a su percepción más abstracta y a las métricas que solo ofrecen información relevante a medio o largo plazo. Se destaca que el modelo resultante es aplicable a cualquier entidad, tanto pública como privada, pero se ha tenido especial cuidado en incorporar los requisitos específicos del sector público para garantizar su utilidad en este ámbito. Además, se detallan los objetivos específicos de la investigación y los resultados obtenidos en cada caso, respaldados por publicaciones que han sido validadas por la comunidad científica.

1.1

Trasfondo y motivaciones

Es un hecho ampliamente reconocido que el panorama actual de las ciberamenazas está en constante crecimiento y, al mismo tiempo, su complejidad y sofisticación han aumentado de manera exponencial [1]. Este incremento en número y especialización se produce a un ritmo acelerado, lo que representa un desafío significativo para entidades públicas y privadas, con un aumento continuo de los ciberataques y un impacto difícil de gestionar para estas organizaciones [2].

En el pasado, los ciberataques solían asociarse con individuos solitarios o expertos en tecnología, pero en la actualidad, esta visión romántica ha desaparecido casi por completo. La ciberdelincuencia organizada [3] es ahora común, con ataques con motivaciones económicas como el ransomware [4] y el ciberchantaje [5], así como servicios específicos en la Internet oscura [6], como el ransomware como servicio [7], lo que demuestra la profesionalización de las organizaciones ciberdelinquentes [8].

La creciente digitalización de entidades públicas y privadas [9] ha llevado a un aumento de los grupos de ciberdelinquentes respaldados por estados, que ven en el ciberespacio una oportunidad para dañar empresas estratégicas [10], servicios esenciales [11] e infraestructuras críticas [12], así como la reputación de las instituciones públicas [13], en un contexto de guerra híbrida [14] contra los estados oponentes.

Es esencial que ese proceso de digitalización, por tanto, vaya acompañado de una estrategia de ciberseguridad que permita garantizar la continuidad de estos servicios [15] y la integridad, privacidad y seguridad de los datos a medio, corto y largo plazo [16].

Ante esta situación, los estados están implementando medidas para diseñar estrategias nacionales de ciberseguridad [17], establecer planes y objetivos asociados a estas estrategias [18], y promover programas y proyectos adaptados para garantizar la seguridad cibernética de sus sociedades e intereses [19]. En este contexto, las organizaciones del sector público, responsables de la confianza de los ciudadanos en los servicios públicos digitales, necesitan contar con herramientas que les permitan asegurar que estos servicios sean ciberresilientes [20] (capaces de resistir y recuperarse ante un ciberincidente) y cumplan con las estrategias y planes de ciberseguridad de su Estado o de las entidades supranacionales que correspondan [21], proporcionando así las garantías necesarias a los ciudadanos [22].

Este enfoque, presentado de manera general, resulta fácil de comprender. Sin embargo, al profundizar en un nivel de detalle más específico, es crucial comprender todos los factores que dificultan que las entidades, especialmente las del Sector Público, aborden la ciberseguridad de manera efectiva y con garantías [23]. Los siguientes apartados, derivados de un análisis exhaustivo del estado del arte, servirán como una reflexión sobre estos factores.

1.1.1

Evolución de los activos prioritarios en las organizaciones

A lo largo del proceso de digitalización de las organizaciones, estas han priorizado la protección de sus activos más valiosos en cada etapa (**Ilustración 1**). Estos activos no han sido constantes, sino que han evolucionado con el avance de la digitalización.

Inicialmente, en la era de los *mainframes*, el hardware era una inversión clave, utilizada por un grupo limitado dentro de la organización, principalmente en departamentos financieros o de ingeniería [24]. Con la popularización de la informática personal, cada usuario tuvo su propio ordenador y algún tipo de interconexión, lo que aumentó la exposición de las empresas a amenazas y riesgos informáticos [25], [26]. A medida que se implementaban procesos de negocio digitales y se reducía el uso del papel, la información gestionada por los sistemas se convertía en el activo más valioso [27].

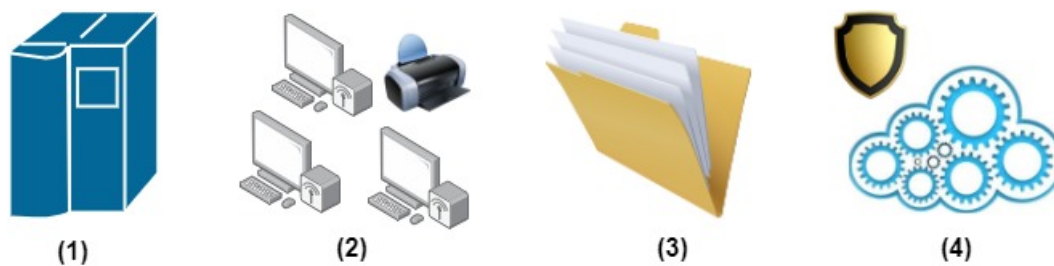


Ilustración 1. Evolución de los activos relevantes para las organizaciones en cada fase de sus procesos de digitalización: desde los costosos mainframes de los años 70 (1), hasta la capacidad de operación en el ciberespacio y la confianza para con terceros en la actualidad (4), pasando por el parque informático (2) o la información generada por los sistemas de información corporativos (3).

En la actualidad, con la expansión del ciberespacio, las entidades interactúan directamente, con sistemas interconectados, a través del ciberespacio, lo que dificulta distinguir entre lo propio y lo ajeno. Esta dependencia del ciberespacio hace que la capacidad operativa y la confianza ofrecida a terceros sea el activo más preciado para las organizaciones [28], y la ciberresiliencia, uno de los principales objetivos [29].

En cada fase del proceso de digitalización, las organizaciones han considerado aquellas amenazas específicas de sus activos más relevantes, adoptando las medidas necesarias y los enfoques apropiados para ello.

1.1.2

Evolución vertiginosa en el proceso de digitalización

La progresión detallada en la sección 1.1.1 no ha seguido un ritmo uniforme en cada fase. Por el contrario, la digitalización de las organizaciones ha avanzado de una forma exponencial, lo que no sólo ha aumentado la complejidad del escenario en cada evolución, sino que además ha reducido drásticamente el tiempo disponible para adaptarse a la nueva realidad [30]. Como resultado, los cambios se suceden rápidamente sin que las organizaciones tengan la oportunidad de adaptarse

adecuadamente (**Ilustración 2**). Y esto las expone a un riesgo significativo que deben ser capaces de abordar.

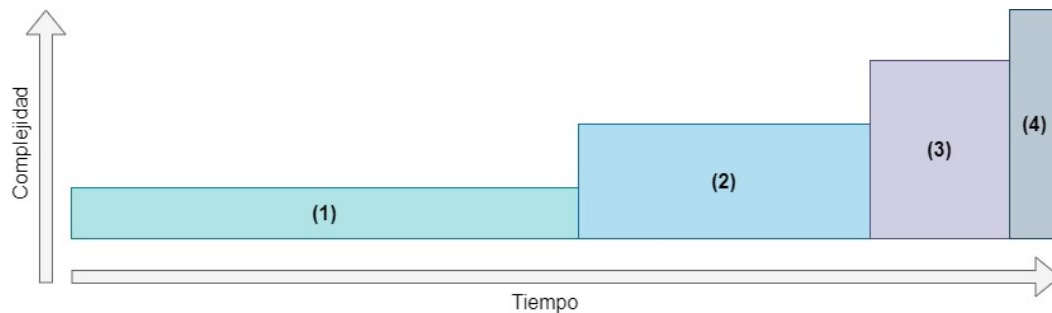


Ilustración 2. Al mismo tiempo que los distintos contextos han ido creciendo en complejidad con el tiempo, los cambios de enfoque se han sucedido con una aceleración creciente. Si la era de la seguridad física eléctrica fue relativamente pausada (1), el periodo de la seguridad IT fue mucho menor (2); y esta aceleración no lineal se ha mantenido durante el periodo donde la seguridad de la información era el contexto imperante (3) y finalmente en el actual contexto de ciberseguridad (4) debido al vertiginoso ritmo de la evolución tecnológica y de la digitalización de las organizaciones.

Esta situación ha tenido repercusiones relacionadas con la ciberseguridad en varios niveles:

- En la capacitación del personal: La rápida adopción de elementos disruptivos en los procesos de digitalización, como el ciberespacio [31], dificulta que el personal interno de las organizaciones tenga el tiempo necesario para adaptarse y adquirir las habilidades de ciberseguridad necesarias de manera segura [32].
- En la escasez de profesionales: La falta de tiempo para la adaptación también se ha reflejado en el ámbito académico y empresarial, lo que ha generado una escasez de profesionales en ciberseguridad [33] debido a la alta demanda y poca oferta, creando una brecha entre las habilidades necesarias y las disponibles para contratar [34].
- En la toma de decisiones: Si bien en las primeras etapas de la digitalización, un enfoque estratégico a largo plazo era suficiente para la toma de decisiones relacionadas con la seguridad, el rápido avance del proceso ha llevado a plazos más cortos y decisiones más frecuentes en todos los niveles de la organización [35]. Actualmente, los cambios se producen con una rapidez tal que la toma de decisiones en ciberseguridad no puede recaer exclusivamente en el ámbito estratégico, sino que también debe involucrar niveles inferiores, manteniendo la alineación con los intereses de la organización [36].
- En la evolución de los modelos y marcos de referencia: Si las personas no pueden adaptarse rápidamente a los cambios, los modelos y marcos diseñados para la gestión de la ciberseguridad tampoco pueden hacerlo, como se detalla en la sección 1.1.3. No contar con estándares adecuados que guíen en la gestión y evaluación de la nueva realidad impide a estas organizaciones una adopción con garantías de los nuevos avances tecnológicos.

Así pues, en la actualidad nos encontramos con una adopción masiva y acelerada de tecnologías disruptivas por parte de organizaciones de todo tipo. Esto hace que dichas organizaciones dependan de activos que hasta ahora eran secundarios, exponiéndoles a un nuevo panorama de amenazas. Y para afrontar dichas amenazas, debido al ritmo vertiginoso de estos cambios, no cuentan con marcos y procedimientos adecuados ni con personal preparado. Simplemente, las cosas ocurren demasiado rápido.

1.1.3

Evolución de los estándares de gestión de la seguridad

Las amenazas de seguridad que pueden afectar a cada activo derivan de su naturaleza, y dado que la naturaleza de los activos ha evolucionado con el tiempo, también lo han hecho las amenazas y los riesgos asociados [37], [38]. Por lo tanto, se ha vuelto necesario desarrollar modelos y marcos de trabajo que puedan abordar el conjunto de amenazas y riesgos de seguridad en cada momento. Así, hemos visto enfoques como la seguridad física (que aborda las amenazas principalmente sobre el hardware y las instalaciones físicas), la seguridad informática o de TI (que aborda las amenazas sobre los activos tecnológicos software, hardware y comunicaciones), la seguridad de la información (que aborda las amenazas sobre la información gestionada por los sistemas de información de la organización) y, en la actualidad, la ciberseguridad (que aborda las amenazas emanadas de la dependencia del ciberespacio) [39].

Normalmente, cada nuevo modelo considera las amenazas y riesgos contemplados por el modelo predominante, agregando características nuevas que permitan abordar las nuevas amenazas y riesgos en el siguiente avance del proceso de digitalización [40], [41]. Por ejemplo, el enfoque de seguridad de la información incluye medidas específicas para tratar las amenazas y riesgos de seguridad física, de seguridad informática y de seguridad de la información, pero no las específicas del enfoque de ciberseguridad. Del mismo modo, el enfoque de ciberseguridad incorpora las características de los anteriores y añade los específicos derivados de la adopción del ciberespacio.

El problema, como se ha explicado en el apartado 1.1.2, radica en que la rapidez del proceso de digitalización [42] y, en particular, el salto desde un enfoque de seguridad de la información a uno de ciberseguridad no ha permitido un desarrollo adecuado de este último [43]. En muchas ocasiones, se aplican enfoques y estándares de seguridad de la información en situaciones donde debería aplicarse un enfoque y un modelo de gestión de ciberseguridad, o se confunden ambos enfoques [44]. Sin embargo, esto no permite cubrir de manera adecuada las amenazas y riesgos asociados al ciberespacio, ni permite proteger adecuadamente los activos críticos emergentes (**Ilustración 3**) que están tomando gran relevancia para para las organizaciones en la actualidad [45]. Esto se debe a dos razones principales:

- Un desarrollo deficiente de estándares y marcos para la ciberseguridad: A pesar de existir iniciativas valiosas de ciberseguridad, no se ha logrado desarrollar un modelo completo. Los estándares dedicados a la seguridad de la información han sido modificados para adaptarse, pero siguen centrándose en la información como activo y no en la capacidad operativa y la confianza ofrecida a terceros. Además, generalmente los modelos existentes no abordan la necesidad de tomar decisiones a diferentes niveles de la organización, no solo estratégico; si bien alguno menciona la necesidad, ninguno desarrolla esta parte crucial. Esto lleva a que cada organización adapte sus procesos internos de manera independiente para abordar la ciberseguridad, lo que no es consistente, no se puede aplicar a otras organizaciones y no permite contratar personal o servicios de ciberseguridad sin una formación específica sobre los procedimientos exclusivos de cada organización.

- Una formación deficiente de personas y profesionales: La capacitación en modelos específicos de ciberseguridad no se ha producido adecuadamente debido a los problemas mencionados anteriormente lo cual dificulta el cambio de paradigma.

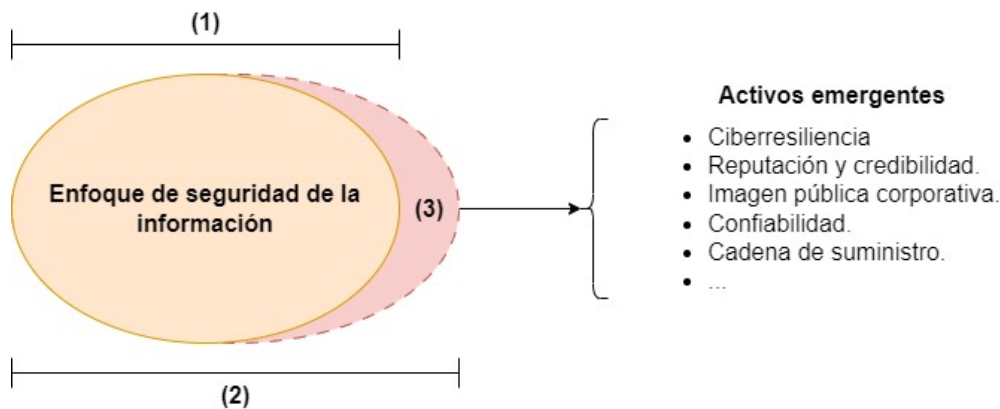


Ilustración 3. La aplicación de un enfoque de seguridad de la información (1) a un contexto de ciberamenazas (2) necesariamente deja sin cubrir aquellas amenazas específicas del ciberespacio (3) que atentan contra activos distintos de la información. El análisis de riesgos de un enfoque de seguridad de la información se fundamenta en que el activo prioritario es la información y las debilidades y amenazas, son las que pueden poner en riesgo dicha información en cualquiera de sus dimensiones. Pero, quizás, el activo más importante en la actualidad está dejando de ser la información o no es la información exclusivamente.

La paradoja reside en que, aunque un modelo de seguridad de la información, como el propuesto en la familia de normas ISO 27000, no pueda satisfacer por completo los requisitos de la ciberseguridad, ofrece otros beneficios: este modelo es maduro, puede certificarse como norma y resulta fácil contratar personal para su implementación y auditoría [46]; contar con estándares es importante [47]. Por lo tanto, en la actualidad, las circunstancias no son propicias para que las organizaciones abandonen este estándar sin más. Al menos no hasta que las entidades de normalización generen un marco de ciberseguridad integral no fundamentado en modelos de seguridad de la información, dado que estos basan el análisis de riesgos en las dimensiones de la información (confidencialidad, integridad y disponibilidad, al menos), entendiéndola como el activo de mayor relevancia. Pero en un contexto de ciberseguridad la información no es, en muchos casos, el activo más importante en las organizaciones [48]. Es cada vez más común que las organizaciones prioricen la propia continuidad de sus operaciones [49], [50], la confiabilidad que transmiten a terceros con los que tienen que relacionarse [51], [52], la imagen y reputación [53] o la protección de su cadena de suministro ya que, siendo esta ajena a su propio control, es esencial para su supervivencia. Hechos como la capacidad de una campaña de noticias falsas lanzada por un grupo de ciberdelincuentes para desestabilizar un gobierno o hacer caer una empresa en bolsa, sin afectar la información ni los datos gobernados por la organización, ponen de manifiesto que el foco, en un contexto cibernético, no puede situarse exclusivamente en la información [54]. Los ciberataques a empresas que forman parte de la cadena de suministro son otro claro ejemplo de que, sin que la información propia se vea afectada, las operaciones de la organización pueden verse perjudicadas.

Sin embargo, que no sea factible o conveniente prescindir de momento de un modelo más clásico de seguridad de la información, no implica que éste no deba complementarse con modelos adicionales que cubran las áreas en las que existe margen de mejora [55].

1.1.4

Evolución de las fronteras de las organizaciones

La evolución digital de las organizaciones ha llevado a una expansión de sus fronteras físicas. Inicialmente, los *mainframes* se encontraban en centros de procesamiento dentro de los edificios de las organizaciones y no tenían conectividad externa. Con el tiempo, las redes locales internas permitieron que la digitalización se extendiera por toda la organización dentro de sus límites físicos. Conforme las organizaciones adoptaban el uso del ciberespacio, parte de su actividad abandonaba las instalaciones físicas y se expandía al ámbito cibernético [56], [57]. Hoy en día, algunas organizaciones operan exclusivamente en el ciberespacio, mientras que otras que aún operan dentro de límites físicos tienen una presencia digital significativa que a menudo es incluso mayor. La interconexión de sedes [58], la interconexión con sistemas de diferentes entidades [59], el trabajo remoto o híbrido [60], el uso de proveedores de servicios en la nube [61] y otros elementos similares han sido adoptados casi naturalmente por las empresas, a veces impulsadas por la inercia o por la demanda de clientes o proveedores (**Ilustración 4**).

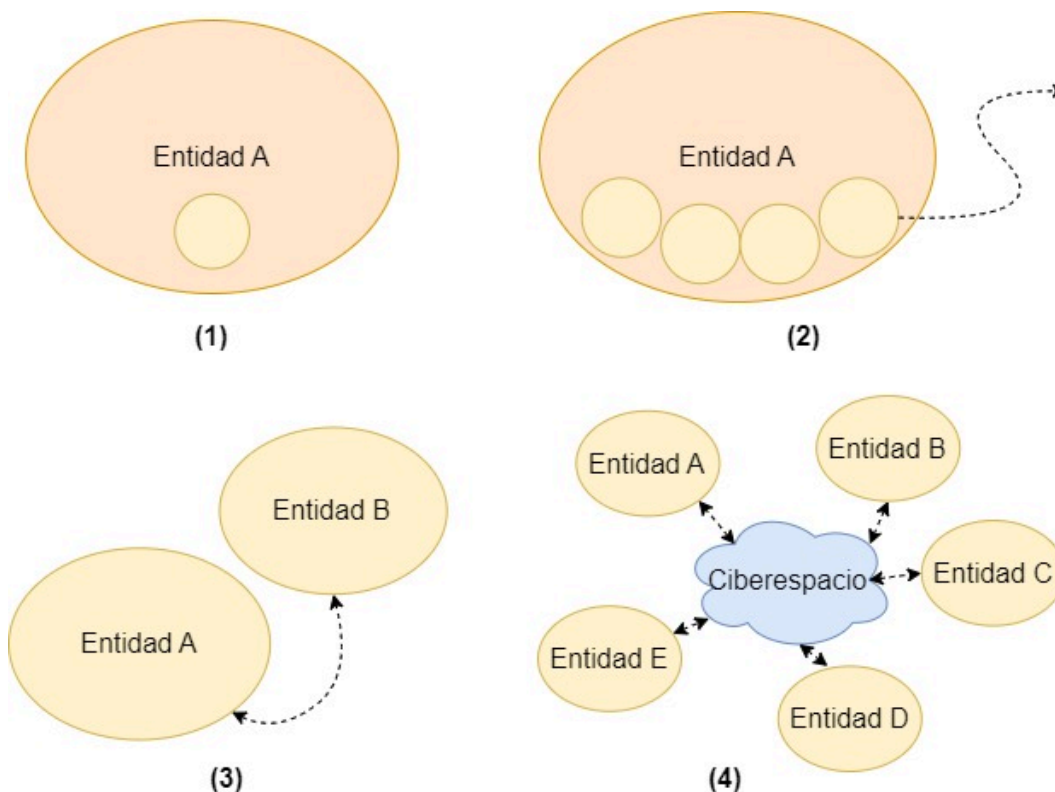


Ilustración 4. A medida que las empresas han avanzado en su digitalización, sus propias fronteras se han difuminado. En primera instancia, con la digitalización de sólo un departamento interno (1); posteriormente con la digitalización parcial de la organización, las redes locales y el incipiente acceso a Internet (2). Esto dio paso a la interconexión entre entidades donde la digitalización era generalizada, habitualmente con conexiones privadas (3), extendiendo sus fronteras más allá de los límites físicos. En la actualidad, es habitual una interconexión de organizaciones a través del ciberespacio para ofrecer servicios conjuntos lo cual hace difícil distinguir su propio perímetro y controlar este ecosistema virtual (4).

Como resultado de esta rápida expansión, se ha producido una pérdida de control sobre los activos fundamentales del negocio. En sus inicios, las organizaciones tenían

un control estricto sobre todo lo que les importaba en términos de activos. Sin embargo, con el tiempo, el deseo de obtener ventajas como un mayor alcance o visibilidad, o una mayor cercanía a sus partes interesadas, ha llevado a ceder este control, gradual, pero rápidamente. En muchos casos, esto ha resultado en una gran dependencia de terceros, lo que hace que la continuidad del negocio dependa en gran medida de ellos, a menudo sin un análisis previo adecuado de los riesgos asociados [62].

En este contexto, la gestión de la ciberseguridad en la cadena de suministro cobra una importancia especial, y surge la necesidad de establecer un vocabulario y un modelo comunes, así como de cooperar con terceros, ya que la propia organización puede verse afectada por el estado de ciberseguridad de estos y viceversa. Es decir, la necesidad de ser ciberresilientes se ha convertido en una prioridad para prácticamente todas las organizaciones [63] y la cooperación y el establecimiento de métricas homogéneas y entendibles ha pasado de ser algo aconsejable a ser algo imprescindible.

1.1.5

Evolución de la participación en ciberseguridad: holismo

A medida que las organizaciones evolucionaban en su proceso de digitalización, también lo hacía el número de personas y áreas de conocimiento necesarias para abordar los desafíos en cada etapa. Inicialmente, solo equipos de ingenieros eléctricos o físicos se ocupaban de proteger el activo principal, el computador. Sin embargo, con la expansión de la digitalización en la organización, más departamentos y áreas dependían de los activos importantes en ese momento, lo que requería la contribución de un mayor número de personas desde diversos campos de conocimiento para su protección [64].

Durante mucho tiempo, los equipos de tecnología eran responsables de asegurar la información cuando esta era el activo principal, pero no estaban solos en esta tarea. Los departamentos de desarrollo de procesos, jurídicos y de comunicación también desempeñaban un papel cada vez más relevante. Esta tendencia continuó hasta que, bajo un enfoque de ciberseguridad, toda la organización se debe transformar en una unidad de acción completa [65]. Y no sólo la propia organización, sino que es necesario el establecimiento de canales de colaboración estrecha con terceros que forman parte de la cadena de suministro [66].

La creciente dependencia de un mayor número de personas, departamentos y organizaciones de los activos de la organización, entendidos estos como la capacidad de seguir operando en el ciberespacio y ofrecer confianza a terceros, demanda un enfoque holístico (**Ilustración 5**). Esto implica la participación proactiva y conjunta de todos, y desde todos los campos de especialización, en la ciberseguridad de la organización [67].

A pesar de que el término "holismo" se utiliza ampliamente, a veces no se comprende bien y en la práctica se aplica con frecuencia incorrectamente [68]. Los modelos y estándares existentes no desarrollan adecuadamente los elementos que facilitarían la consecución de una ciberseguridad holística efectiva, lo que a menudo resulta en la participación limitada de distintas áreas funcionales de las organizaciones en la

ciberseguridad, su participación de forma descoordinada o en silos organizacionales sin colaboración entre ellos y, en general una gestión ineficaz de las ciberamenazas y los ciberriesgos [69].

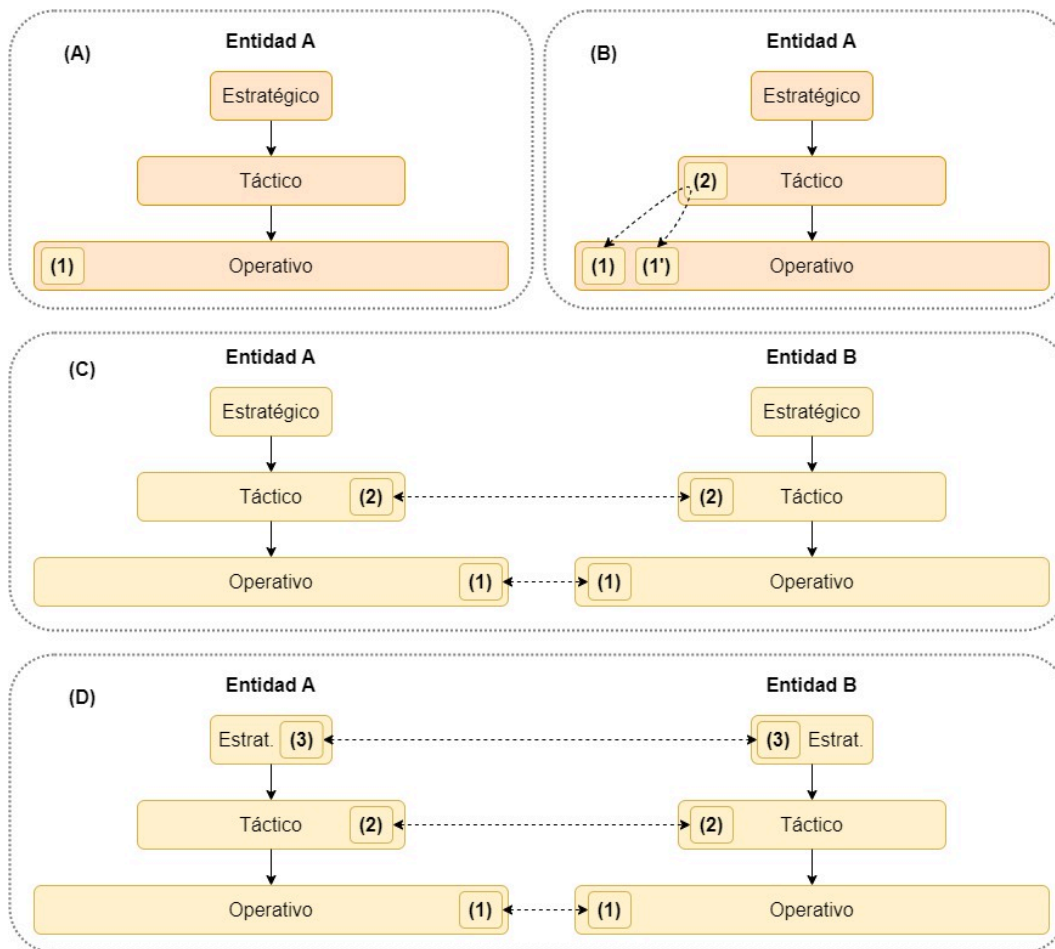


Ilustración 5. En los inicios (A), cuando la digitalización afectaba sólo a una unidad operativa (1) de una organización, las actuaciones en seguridad dependían exclusivamente de dicha unidad. Con la extensión de la digitalización (B), diversas unidades operativas debían participar en la seguridad informática y a veces se coordinaban para ello a través de niveles superiores (1-2-1'). Con un enfoque de seguridad de la información (C), donde la entidad estaba ampliamente digitalizada, gran parte de la misma trabajaba coordinada internamente para aportar seguridad a la información (como en los casos A y B) y, eventualmente, según el grado de colaboración con otras organizaciones, una coordinación parcial con ellas a nivel táctico (2-2) u operativo (1-1). En un enfoque de ciberseguridad la dependencia de terceros y la necesidad de cooperación aumenta considerablemente a todos los niveles, requiriéndose una coordinación interna completa y una cooperación con terceros a todos los niveles para afrontar las ciberamenazas (1-1, 2-2, 3-3).

1.1.6

Las entidades del Sector Público

Los principios mencionados anteriormente son aplicables a organizaciones de todo tipo. Sin embargo, es importante destacar que los desafíos y circunstancias discutidos, que obstaculizan la adopción de un enfoque integral de gestión de la ciberseguridad, se vuelven más pronunciados en las entidades del Sector Público debido a sus características [70] distintivas y particulares (**Ilustración 6**). En resumen:

- Las entidades públicas suelen contar con personal multidisciplinario altamente capacitado en gestión, pero tienden a subcontratar trabajos técnicos a empresas privadas. Esto les permite escalar con las necesidades y atender nuevos proyectos en un contexto fuertemente regulado en cuanto a la contratación de nuevo personal [71]. Como consecuencia, los equipos multidisciplinarios involucrados en la ciberseguridad corporativa suelen estar formados por empleados internos de diversas áreas funcionales, además de personal externo de empresas privadas [72], [73]. Debido a la rotación frecuente del personal externo por la propia naturaleza de los contratos, la formación de equipos sincronizados dentro de cada área funcional se vuelve más compleja dado que son equipos efímeros. Esto se complica aún más a nivel organizacional, donde se requiere la coordinación de un gran equipo multidisciplinario que involucra, además de distintas áreas internas, a múltiples proveedores de diferentes campos de conocimiento para lograr una ciberseguridad holística efectiva [74].
- Es común que cada área funcional de una organización pública mantenga varios contratos para incorporar capacidades de su área de especialización a sus equipos [75]. Sin embargo, rara vez se especifica en estos contratos que el personal contratado debe ser capaz de aplicar estas capacidades a la ciberseguridad [76]. Esto se debe principalmente a un problema de desconocimiento, ya que las áreas no tecnológicas tradicionalmente no han tenido un papel activo en la ciberseguridad corporativa desde su campo particular y suelen carecer de los conocimientos necesarios [77]. Como resultado, estas áreas funcionales a menudo encuentran difícil asumir las tareas de ciberseguridad que les corresponden, incluso si han externalizado sus actividades técnicas a empresas privadas.
- La estructura organizativa de las entidades del sector público tiende a ser rígida y poco adaptable [78]. Por lo general, están organizadas en silos con funciones muy específicas y cadenas de mando definidas, lo que dificulta una respuesta ágil a las amenazas y riesgos cibernéticos [79], [80]. Adaptarse a estos desafíos de manera holística y con una unidad de acción es complicado en este contexto.
- La rápida evolución de las necesidades en ciberseguridad ha creado una escasez de profesionales en este campo [34], [33]. Estos perfiles se caracterizan por su hiperespecialización y la necesidad continua de formación dinámica y costosa [81]. Esto ha llevado a las organizaciones a desarrollar políticas para atraer, desarrollar y retener talento en ciberseguridad [82]. Sin embargo, las empresas privadas tienen más facilidad para ofrecer formación especializada, desarrollar talento y aplicar políticas de retribución, ya sea en salario o mediante otras formas, en comparación con las entidades del sector público [83]. Estas últimas están limitadas por regulaciones que a menudo dificultan la contratación rápida de profesionales altamente cualificados en ciberseguridad, así como la capacitación y retención de estos empleados mediante un plan individualizado de retribución e incentivos capaz de competir con los ofrecidos por las empresas del sector privado.
- Es habitual que las entidades del sector público contraten servicios de seguridad gestionada o centros de operaciones de ciberseguridad para garantizar la disponibilidad de personal cualificado en ciberseguridad en todo momento [84], [85]. Sin embargo, estos servicios suelen tener un enfoque principalmente tecnológico y a menudo no pueden abordar eficazmente la

ciberseguridad holística a nivel organizacional [86]. Es aún más difícil si es un proveedor de servicios quien debe impulsar una visión holística de la ciberseguridad de toda la organización, incluida la definición de acciones para otras áreas de conocimiento y sus proveedores asociados.

- La amplia dependencia de la subcontratación [87], frecuentemente en modalidad remota, hace que las entidades del sector público sean especialmente vulnerables a los ciberataques dirigidos a su cadena de suministro, que suele ser más extensa que la de las empresas privadas [88], [70].

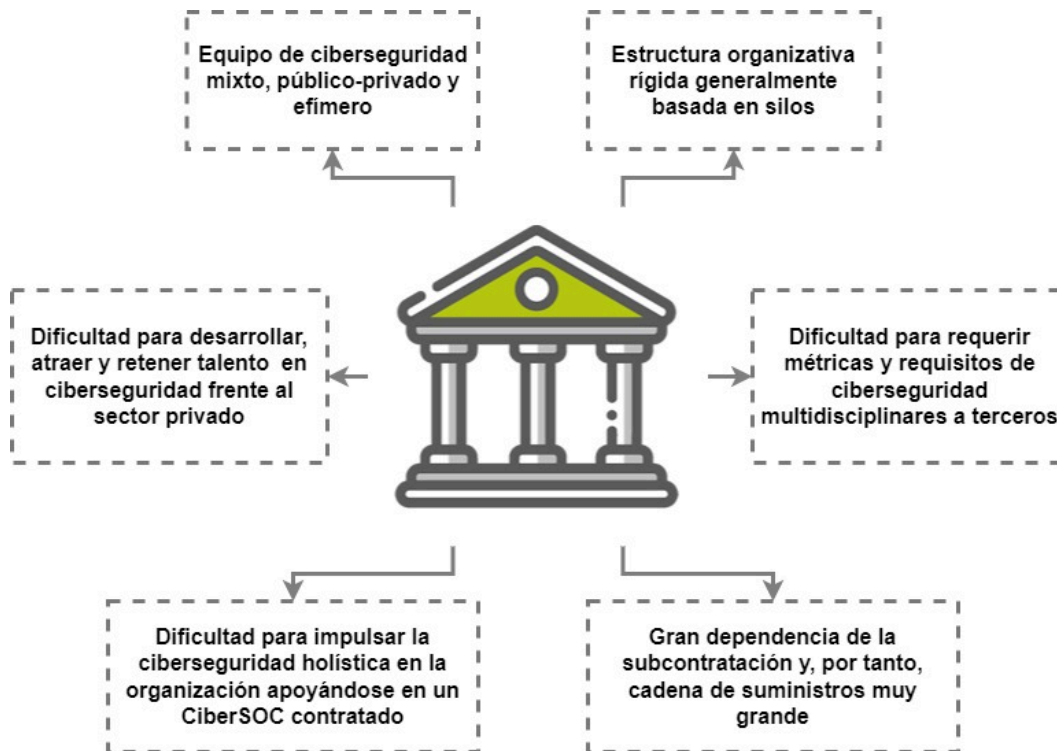


Ilustración 6. Las entidades del Sector Público cuentan con características propias que dificultan la implantación de un enfoque holístico de gestión de la ciberseguridad y que deben ser tenidas en cuenta para que dicho enfoque pueda ser una realidad.

Por ende, al buscar un marco que permita a las entidades del sector público gestionar táctica y operativamente la ciberseguridad, es crucial considerar estas particularidades. De lo contrario, el modelo resultante podría no adaptarse completamente a sus necesidades.

1.2

Objetivos y metodología de investigación

La profesionalización de la ciberdelincuencia está generando un aumento significativo en el número, complejidad e impacto de los ciberataques dirigidos a organizaciones de diversos sectores a una velocidad alarmante. Las entidades públicas se encuentran

cada vez más en la mira de grupos de ciberdelincuentes organizados o respaldados por estados, cuyos objetivos van desde obtener beneficios económicos hasta desestabilizar e interrumpir infraestructuras críticas y estratégicas. Frente a este escenario, los estándares y marcos de trabajo predominantes, originalmente centrados en la seguridad de la información, están empezando a adaptarse gradualmente al ámbito de la ciberseguridad. Aunque se están desarrollando otras iniciativas para abordar diversos aspectos de la ciberseguridad, ninguna de ellas proporciona un modelo completo que pueda estructurar la ciberseguridad tanto horizontal como verticalmente dentro de las organizaciones. Además, estos enfoques no detallan suficientemente los elementos necesarios para una aplicación uniforme entre los diferentes departamentos de una misma organización o entre las organizaciones que forman parte de la cadena de suministro.

Esta tesis se centra en la búsqueda, a través de un enfoque estructurado, de una solución metodológica especialmente diseñada para el Sector Público que facilite la gestión y evaluación holística de la ciberseguridad, involucrando a los niveles tácticos y operativos multidisciplinarios de las organizaciones públicas, así como a su cadena de suministro. Todo ello, complementando y coexistiendo con los estándares y normas implantados por dichas organizaciones a nivel estratégico.

De este objetivo principal, se han identificado los siguientes objetivos más específicos:

- O1. **Diseño de un marco de trabajo para la gestión y evaluación de la ciberseguridad en el Sector Público.** Esto implica analizar los diversos factores que dificultan la gestión efectiva de la ciberseguridad en las entidades públicas, con el fin de proponer soluciones metodológico-procedimentales integradoras que aborden estas dificultades desde una perspectiva completa. Se busca entender el problema en su totalidad y ofrecer soluciones específicas para resolverlo.
- O2. **Desarrollo de soluciones algorítmicas para la optimización.** Se pretende que las entidades públicas puedan aplicar el modelo diseñado de manera efectiva para garantizar que están optimizando la eficiencia en la consecución de sus objetivos estratégicos de ciberseguridad. Por lo tanto, como objetivo adicional en esta tesis, se plantea analizar la viabilidad de utilizar algoritmos evolutivos de optimización multicriterio para maximizar estos objetivos estratégicos de la organización pública, en línea con el modelo diseñado. Además del análisis, se pretende implementar realmente el algoritmo.
- O3. **Análisis y desarrollo de soluciones tecnológicas para facilitar la implantación práctica del modelo.** Se busca que el modelo sea aplicable en la práctica, no solo en teoría, ya que un modelo que no pueda ser fácilmente implementado está destinado al olvido o a una implementación defectuosa. Por lo tanto, en esta tesis, se plantea como objetivo analizar y desarrollar soluciones tecnológicas que faciliten a las entidades públicas la aplicación práctica del modelo. Además, se pretende validar estas soluciones mediante aplicaciones experimentales.
- O4. **Diseño de extensiones metodológicas para abordar la ciberseguridad de la cadena de suministro.** El diseño de un modelo de gestión y evaluación de la ciberseguridad holística en el Sector Público debe considerar sus particularidades, como las extensas cadenas de suministro y la alta dependencia de la subcontratación. Estas características aumentan su exposición a ciberamenazas específicas de la cadena de suministro. Por ello, en esta tesis se propone un análisis detallado de estas particularidades, así como el diseño de las extensiones metodológicas que se requieran tras este análisis.

Estas extensiones permitirán aplicar el modelo a todos los componentes de la cadena de suministro que contribuyen a la ciberseguridad global de la organización. Ambos aspectos son objetivos fundamentales de esta investigación.

Para alcanzar con éxito los objetivos establecidos, se empleó una metodología que incluyó una revisión exhaustiva del estado actual del conocimiento en diversas áreas, como la gestión de la ciberseguridad, los modelos y estándares de seguridad, las iniciativas específicas de ciberseguridad, el uso de algoritmos evolutivos en la optimización multicriterio aplicado a la gestión de la ciberseguridad, la gestión de activos organizacionales, el mentoring y coaching en ciberseguridad, la externalización de capacidades en el sector público, la gestión de recursos humanos y servicios públicos, la arquitectura de centros de operaciones de ciberseguridad, la gestión de la cadena de suministro en ciberseguridad, la gestión de conflictos de interés, la gestión de ciber crisis o la capacitación en ciberseguridad. Este análisis reveló la amplia gama de factores que dificultan que las entidades públicas adopten de manera efectiva un enfoque holístico de ciberseguridad en línea con el contexto de ciberamenazas y ciberriesgos en el que operan.

A partir de esta revisión exhaustiva, se diseñaron diversos elementos para crear un marco facilitador destinado a la gestión táctico-operativa de la ciberseguridad holística, enfocado específicamente en el activo de negocio y dirigido a las entidades del Sector Público. Estos resultados fueron validados empíricamente, utilizando en algunos casos métodos matemáticos y en otros ensayos experimentales, según su naturaleza. Gracias a la colaboración de dos entidades, una del sector público y otra del sector privado, que accedieron a probar los resultados preliminares de la investigación, gran parte de estos pudieron ser aplicados en la práctica. Los hallazgos derivados de estas implementaciones fueron reincorporados al trabajo de investigación durante diversas iteraciones, lo que permitió refinar y optimizar los resultados obtenidos.

1.3

Resultados de la tesis y colaboraciones

En esta sección se presentan los resultados de las investigaciones llevadas a cabo en esta tesis, así como la colaboración llevada a cabo con otros investigadores durante el periodo doctoral. Los resultados de investigación y las contribuciones de esta tesis se encuentran embebidas en las siguientes publicaciones que, en conjunto, permiten presentar la tesis como un compendio de publicaciones:

- [J1] **M. Domínguez-Dorado**, J. Carmona-Murillo, D. Cortés-Polo, F. J. Rodríguez-Pérez, “CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels”. *IEEE Access* 2022, 10, 122454–122485.

- [J2] **M. Domínguez-Dorado**, D. Cortés-Polo, J. Carmona-Murillo, F. J. Rodríguez-Pérez and J. Galeano-Brajones, "Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management". MDPI Applied Science, vol. 13, no. 6327, 2023.
- [J3] **M. Domínguez-Dorado**, F. J. Rodríguez-Pérez, J. Galeano-Brajones, J. Calle-Cancho, and D. Cortés-Polo, "Fleco: A tool to boost the adoption of holistic cybersecurity management," Software Impacts, p. 100614, 2024.
- [J4] **M. Domínguez-Dorado**, F. J. Rodríguez-Pérez, J. Carmona-Murillo, D. Cortés-Polo and J. Calle-Cancho, "Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study". MDPI Information, vol. 14, no. 586, pp. 1-31, 2023.

Finalmente, durante el periodo doctoral ha sido posible la colaboración en distintos proyectos y con otros investigadores que han proporcionado resultados de investigación adicionales.

- [J5] **M. Domínguez-Dorado**, J. Calle-Cancho, J. Galeano-Brajones, F. J. Rodríguez-Pérez, and D. Cortés-Polo, "Detection and mitigation of security threats using virtualized network functions in software-defined networks". Applied Sciences, vol. 14, no. 1, p. 374, 2023.

2

MODELO DE GESTIÓN Y EVALUACIÓN HOLÍSTICA DE LA CIBERSEGURIDAD

Este capítulo contiene un artículo clave en la tesis que vertebra y guía el resto de los trabajos y resultados de investigación de la misma. En dicho artículo, se hace un análisis pormenorizado de aquellos elementos que dificultan la adopción de un modelo holístico de la ciberseguridad y se hace una revisión exhaustiva de los distintos estándares, normas, regulaciones y de la literatura existente, para detectar cómo y hasta qué punto los modelos y mecanismos actuales permiten afrontar esas dificultades. Con ello, en el artículo se diseña una base de conocimiento común de ciberseguridad holística que sirve para homogeneizar los conceptos de la ciberseguridad holística entre distintas áreas o departamentos de la organización y entre esta y las entidades pertenecientes a su cadena de suministro. El artículo también define y desarrolla pormenorizadamente los procesos, procedimientos y estructuras, basándose en esa base de conocimientos, necesarios para aplicar ciberseguridad holística centrada en el activo de negocio, desde los niveles tácticos y operativos de la organización involucrando a la cadena de suministro. Todo ello preservando la alineación con las necesidades estratégicas de ciberseguridad. Finalmente, este trabajo desarrolla un conjunto de métricas agregables de forma ascendente que proporcionan valor a todos los niveles de la organización y permite tanto la evaluación de los niveles de ciberseguridad como el seguimiento del grado de consecución y el establecimiento de los objetivos estratégicos de ciberseguridad. Estas métricas, son de aplicación, donde corresponda, a las entidades de la cadena de suministro, como participante de la ciberseguridad global de la organización.

Este resultado de investigación corresponde al objetivo de la tesis O1, definido en el apartado 1, Objetivos y metodología de investigación.

Referencia: M. Domínguez-Dorado, J. Carmona-Murillo, D. Cortés-Polo, F. J. Rodríguez-Pérez, “*CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels*”. IEEE Access 2022, 10, 122454–122485. <https://doi.org/10.1109/ACCESS.2022.3223440>

Factor de impacto de la publicación (JIF) en JCR 2022: 3.9

Categoría: COMPUTER SCIENCE, INFORMATION SYSTEMS. Ranking JIF: 73/158 (Q2).

Categoría: ENGINEERING, ELECTRICAL & ELECTRONIC. Ranking JIF: 100/275 (Q2).

Categoría: TELECOMMUNICATIONS. Ranking JIF: 41/88 (Q2).

Licencia: <https://creativecommons.org/licenses/by/4.0/>

© 2024 Los autores.

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-DORADO¹, JAVIER CARMONA-MURILLO²,
DAVID CORTÉS-POLO³, AND FRANCISCO J. RODRÍGUEZ-PÉREZ²

¹Department of Information Systems and Digital Toolkit, Public Business Entity Red.es., 28020 Madrid, Spain

²Department of Computing and Telematics Engineering, Universidad de Extremadura, 10003 Cáceres, Spain

³Department 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

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek¹.

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

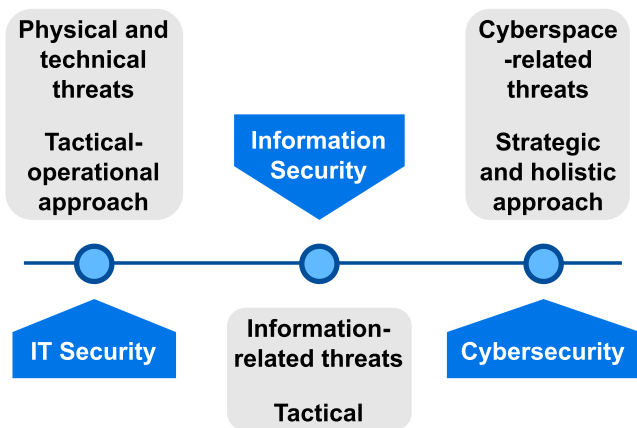


FIGURE 1. From IT security to Cybersecurity. Moving from a single-departmental approach to an organization-wide approach.

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



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.

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 Maturity 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.

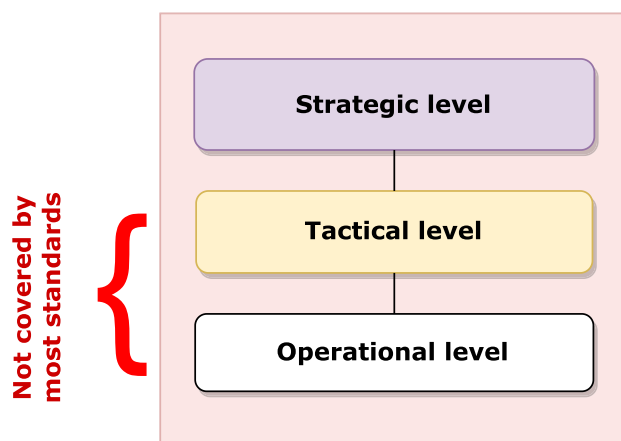


FIGURE 3. It is necessary to provide the tactical and operational levels with homogeneous methodological tools for cybersecurity management.

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

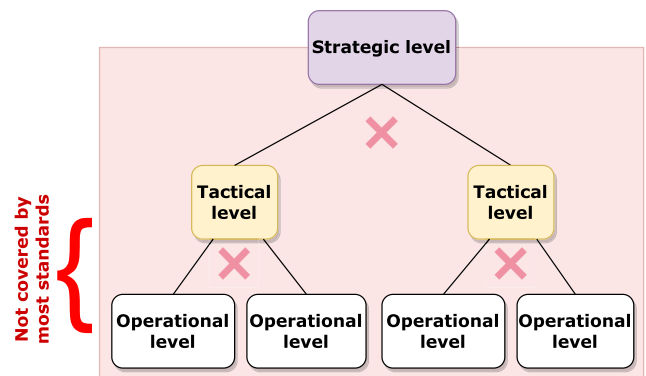


FIGURE 4. The distribution of the organization in silos hinders a fluent communication and collaboration between functional units and the achievement of the holism and unity of action required by a cybersecurity approach.

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

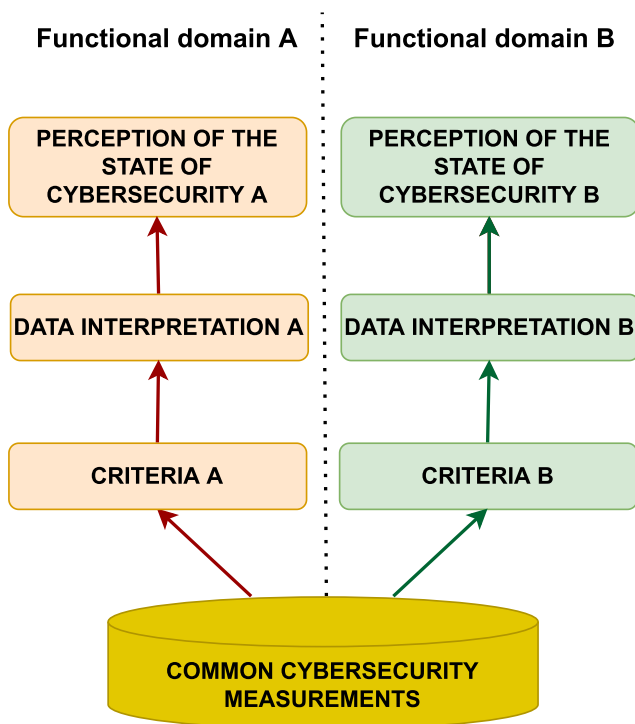


FIGURE 5. Silos in organizations frequently imply the existence of different criteria and disjointed interpretations of the real state of cybersecurity, even when the same data is valued. A common standard should be defined for the evaluation of cybersecurity at these levels.

(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

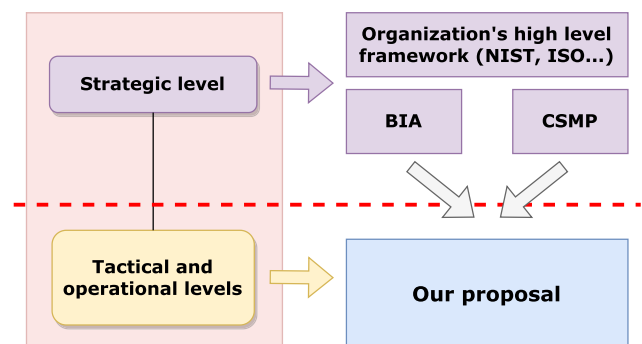


FIGURE 6. BIA and CSMP, both slightly modified, connect the organization's strategic framework to our proposal for tactical and operational levels.

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

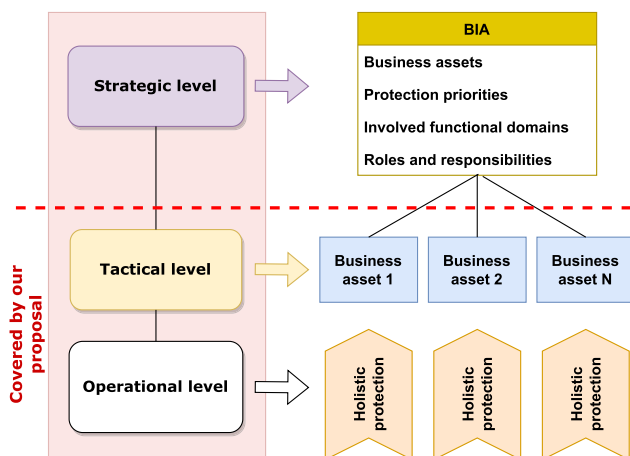


FIGURE 7. Using the BIA to connect the strategic level to the lower ones provides this proposal with the capability of integrating cybersecurity-related business continuity requirements and a focus on the business assets in the daily cybersecurity grinds.

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:

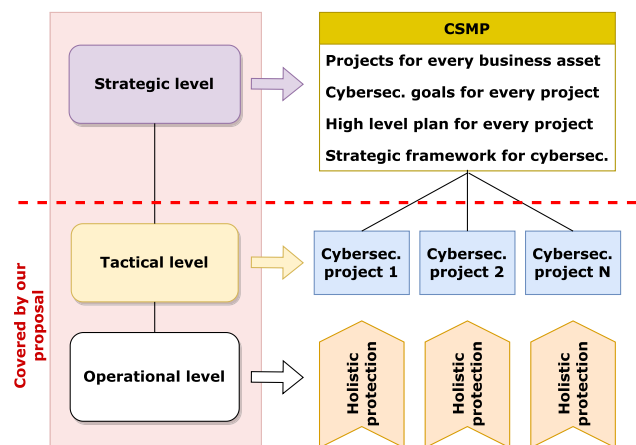


FIGURE 8. Using the CSMP to connect the strategic level to the lower ones provides this proposal with the capability of integrating cybersecurity risks and cybersecurity strategic goals in low levels' activities.

- 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 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 for 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 also 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

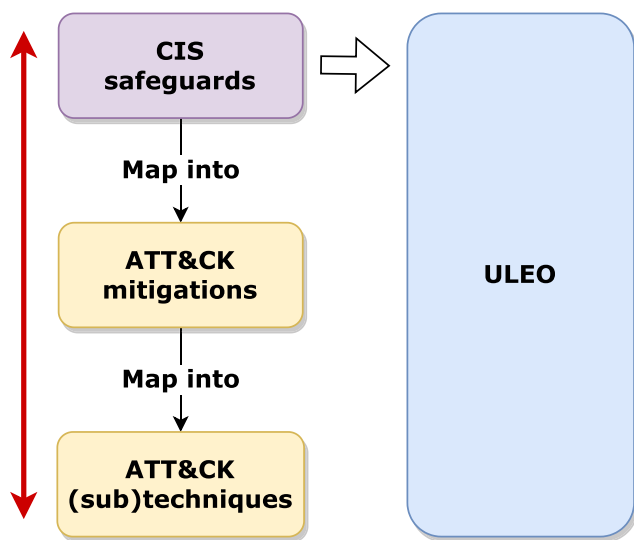


FIGURE 9. Our proposal indirectly incorporates the mitigations and TTPs of MITRE to the ULEO through the inclusion of the corresponding CIS safeguards.

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

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	✓	✓	✓

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.

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.

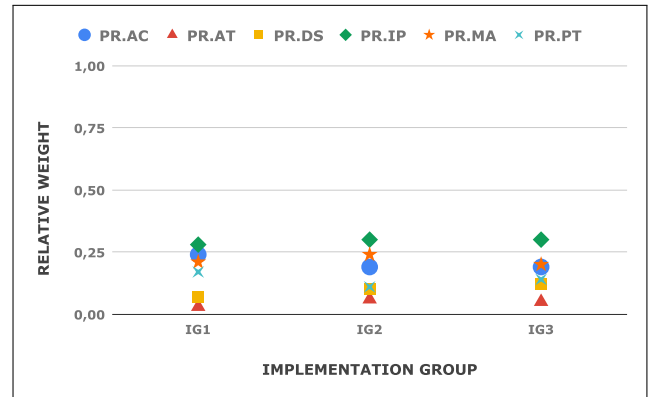


FIGURE 12. Relative weights of every category in 'Protect' function and the three IGs.

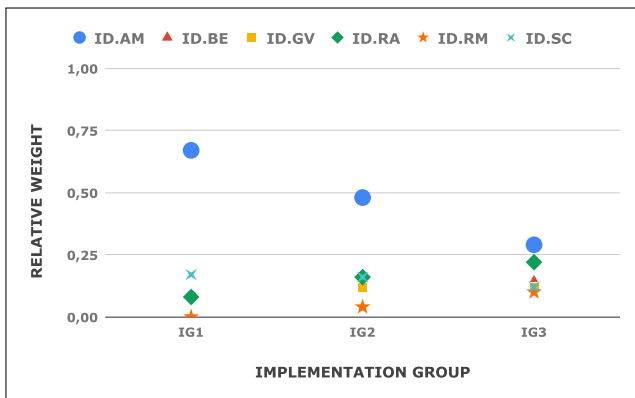


FIGURE 11. Relative weights of every category in 'Identify' function and the three IGs.

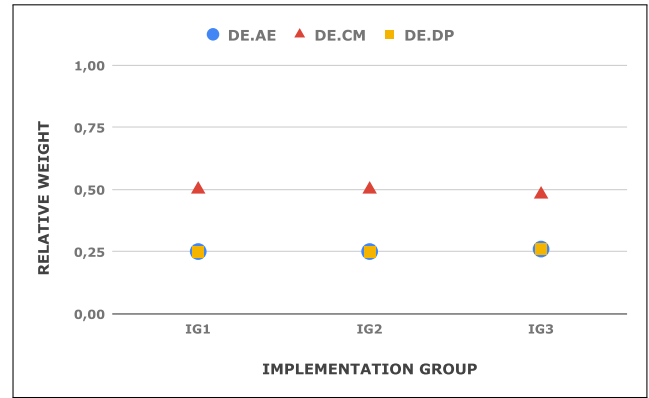


FIGURE 13. Relative weights of every category in 'Detect' function and the three IGs.

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.

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

- 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.

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

- 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.

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

subject to the following restriction (equation 4)

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

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

$$IG(Asset(L + 1)) = IG(Asset(L)) \quad (5)$$

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

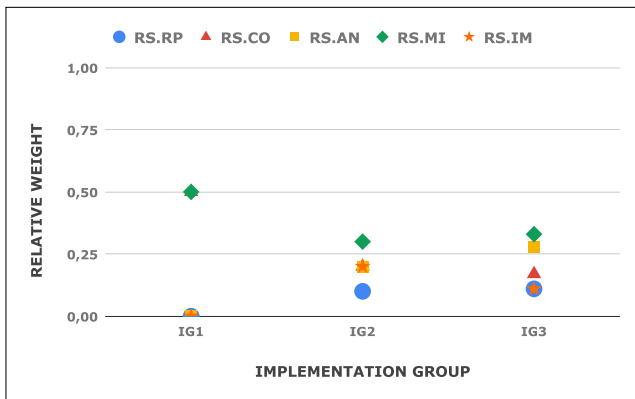


FIGURE 14. Relative weights of every category in 'Respond' function and the three IGs.

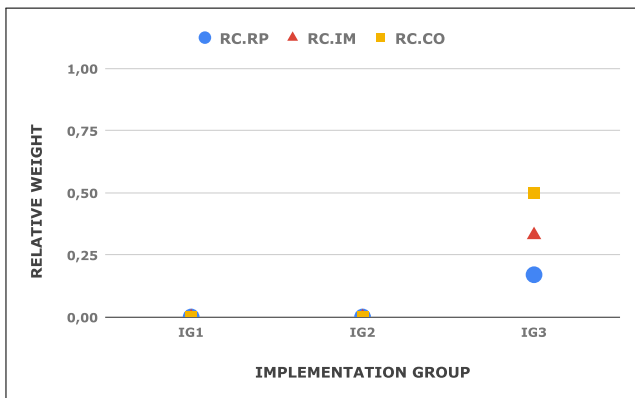


FIGURE 15. Relative weights of every category in 'Recover' function and the three IGs.

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.

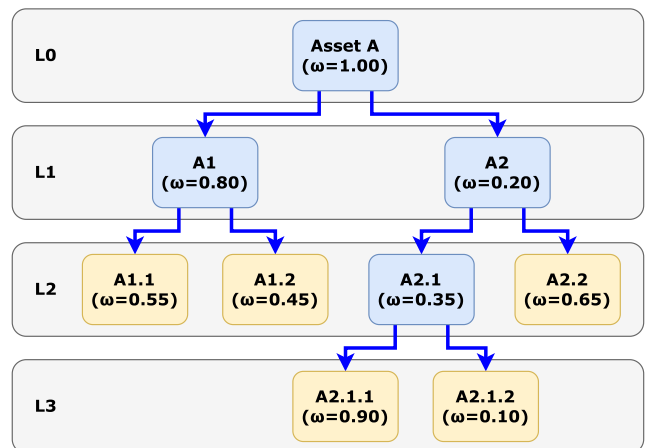


FIGURE 17. Example of a correct asset breakdown.

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).

$$CCS_i = \sum_{j=1}^n W_{Oij} \cdot DLI_{ij} \quad (6)$$

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).

$$FCS_i = \sum_{j=1}^n W_{Cij} \cdot CCS_{ij} \quad (7)$$

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).

$$ACS_t = \sum_{j=1}^n W_{fij} \cdot FCS_{ij} \quad (8)$$

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):

$$ACS_t = \sum_{j=1}^n W_{sa_{ij}} \cdot ACS_{sa_{ij}} \quad (9)$$

where $ACS_{sa_{ij}}$ is the ACS_{ij} value calculated independently for each sub-asset and $W_{sa_{ij}}$ 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 (ACS_{ev}), as shown in equation 10.

$$ACS_{ev} = \frac{t \sum_{i=1}^t t_i ACS_i - \sum_{i=1}^t t_i \sum_{i=1}^t ACS_i}{t \sum_{i=1}^t t_i^2 - (\sum_{i=1}^t t_i)^2} \quad (10)$$

ACS_{ev} will take values from 0.00 to 1.00, because it is an additive time series. Values close to 1.00 indicate that the ACS 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 ACS .

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):

$$OCS_t = \sum_{j=1}^n W_{ba_{ij}} \cdot ACS_{ba_{ij}} \quad (11)$$

where:

- $W_{ba_{ij}}$ is the relative weight of each business asset of the organization.
- $ACS_{ba_{ij}}$ is the cybersecurity status of each business asset calculated as described in the previous section. The t subindex, again, means that the ACS_{ba} 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 (OCS_{ev}), as shown in equation 12.

$$OCS_{ev} = \frac{t \sum_{i=1}^t t_i OCS_i - \sum_{i=1}^t t_i \sum_{i=1}^t OCS_i}{t \sum_{i=1}^t t_i^2 - (\sum_{i=1}^t t_i)^2} \quad (12)$$

OCS_{ev} 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).

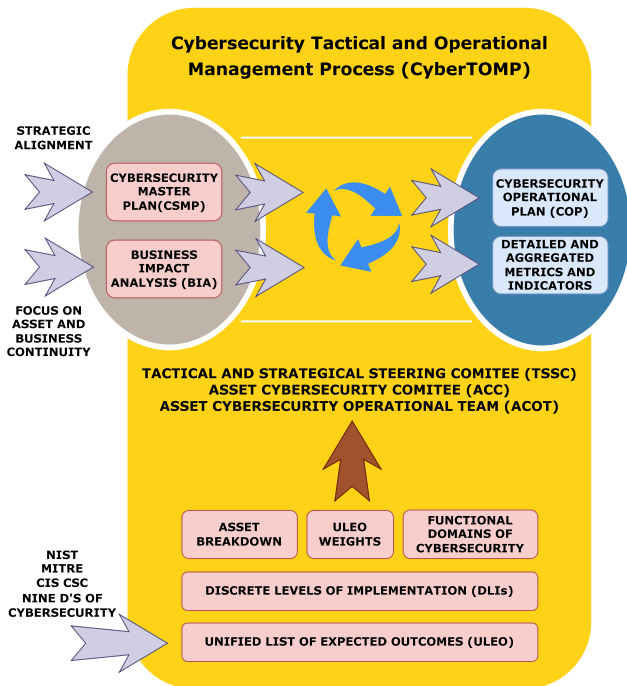


FIGURE 18. CyberTOMP high-level view.

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 because, 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 consists of eight activities, which are detailed below.

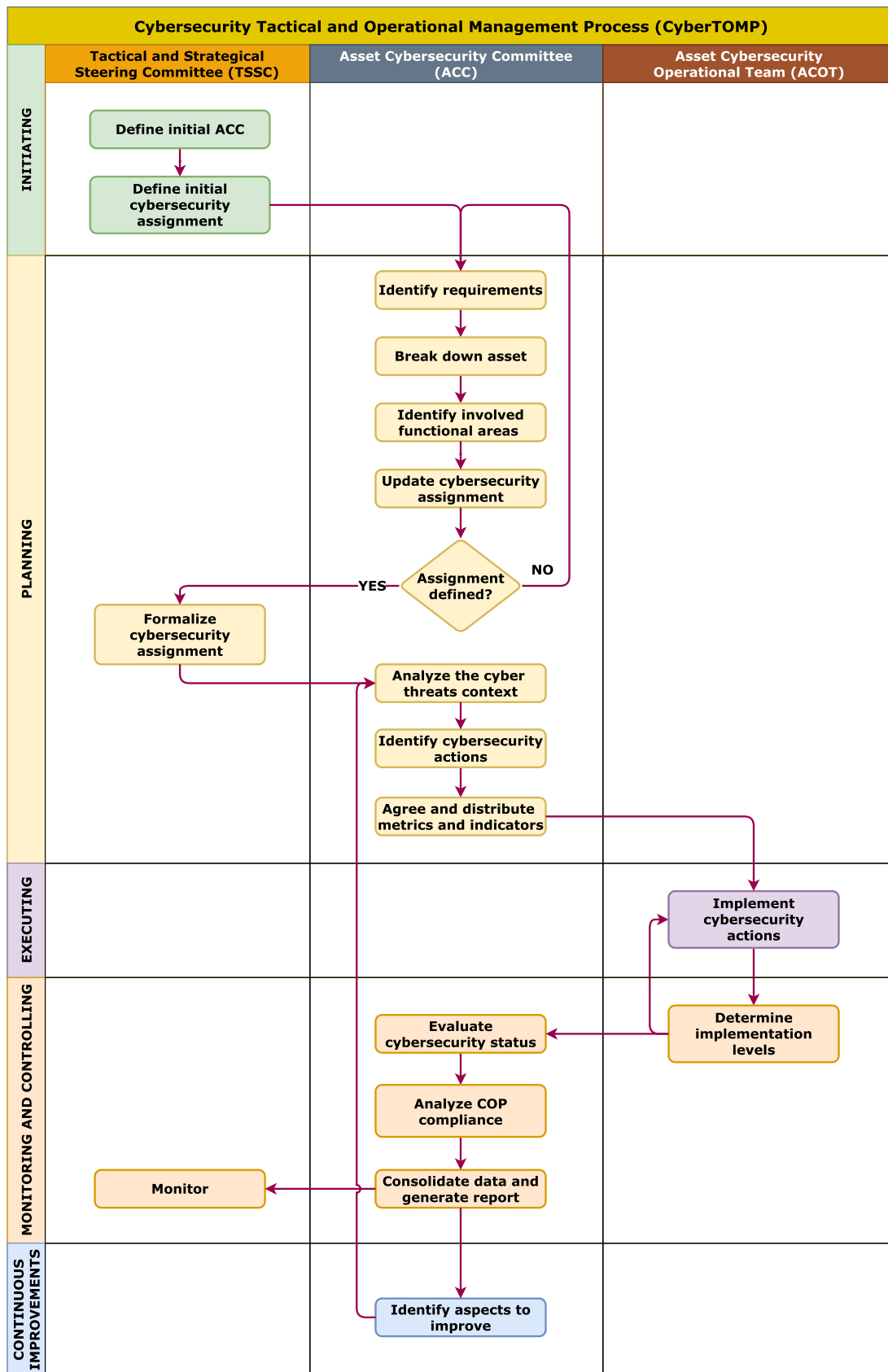


FIGURE 19. Detailed CyberTOMP steps and activities.

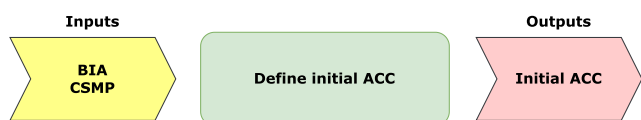


FIGURE 20. Inputs and outputs of 'Define initial ACC' activity.

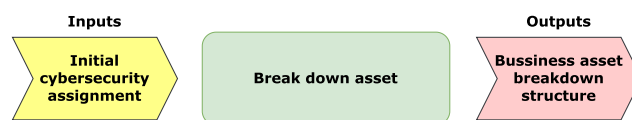


FIGURE 23. Inputs and outputs of 'Break down asset' activity.

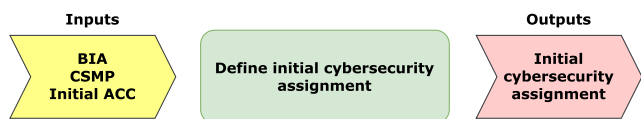


FIGURE 21. Inputs and outputs of 'Define initial cybersecurity assignment' activity'.

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.

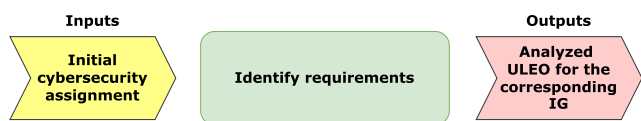


FIGURE 22. Inputs and outputs of 'Identify requirements' activity.

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

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.

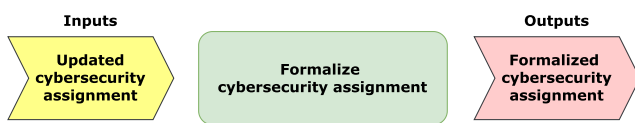


FIGURE 26. Inputs and outputs of 'Formalize cybersecurity assignment' activity.

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.

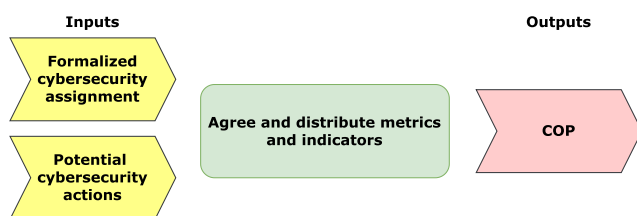


FIGURE 29. Inputs and outputs of 'Agree and distribute metrics and indicators' activity.

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 micro-management 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.

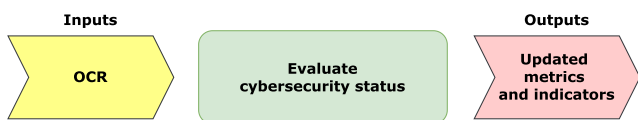


FIGURE 32. Inputs and outputs of ‘Evaluate cybersecurity status’ activity.

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

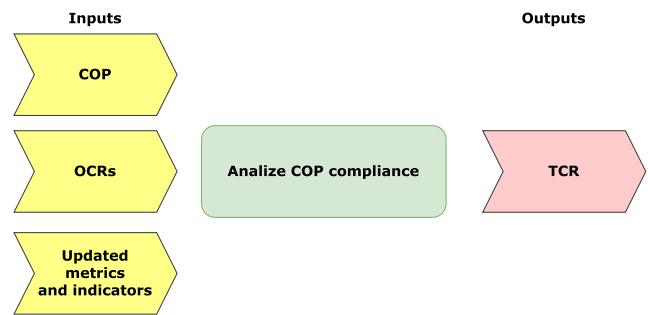


FIGURE 33. Inputs and outputs of ‘Analyze COP compliance’ activity.

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.

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.

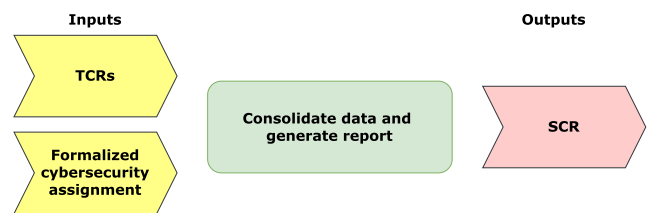


FIGURE 34. Inputs and outputs of ‘Consolidate data and generate report’ activity.

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.

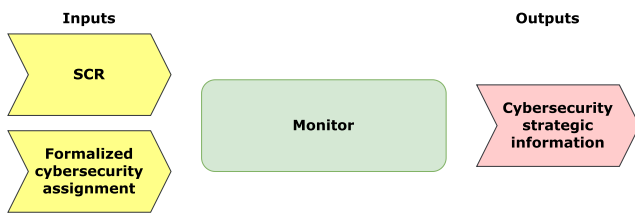


FIGURE 35. Inputs and outputs of 'Monitor' activity.

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.

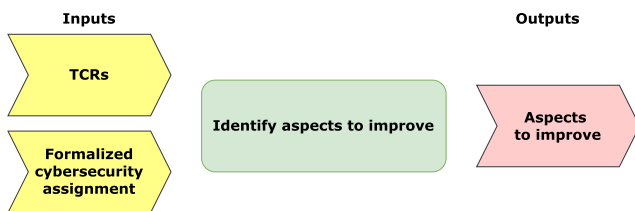


FIGURE 36. Inputs and outputs of 'Identify aspects to improve' activity.

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

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			✓

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 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

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			✓

results that serve as a hook for the expansion of the solution.

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

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

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

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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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.

<i>C</i>	<i>N_o</i>	<i>W_c</i>	<i>W_o</i>
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 - IG3

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 postgraduate 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-estic/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-adequacion-alems-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] *Acquisition 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). *Acquisition and Sustainment, CMMC 2.0 Spreadsheet and Mapping*. Accessed: Jul. 7, 2022. [Online] Available: https://www.acq.osd.mil/emmc/docs/CMMCModel_V2_Mapping.xlsx
- [54] T. Limba, T. Pléta, 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\(12\)](https://doi.org/10.9770/jesi.2017.4.4(12)).
- [55] M. Tvaronavičienė, 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. Walsler, "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](https://doi.org/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 Extremadura 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 Extremadura. 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.

...

3

SOLUCIONES ALGORÍTMICAS PARA LA OPTIMIZACIÓN

Este capítulo contiene un artículo en el cual se analizan las posibilidades de aplicación de algoritmos evolutivos de optimización multiobjetivo a problemas de gestión de la ciberseguridad. En él se hace una revisión de la literatura específica relacionada con los algoritmos evolutivos, sus posibilidades y variantes, así como también sobre casos específicos en los que este tipo de tecnologías se ha aplicado a distintos problemas de gestión en el campo de la ciberseguridad. Tras este análisis, en el artículo se desarrolla de forma íntegra un algoritmo genético de optimización multiobjetivo que, completamente imbricado en el modelo desarrollado y explicado en el apartado anterior, permite la selección rápida y eficiente de un conjunto determinado de actuaciones de ciberseguridad que permiten cumplir de forma óptima con los objetivos estratégicos de ciberseguridad holística que se definan teniendo en cuenta el conjunto de controles de ciberseguridad previamente implantados.

Este resultado de investigación corresponde al objetivo de la tesis O2, definido en el apartado 1, Objetivos y metodología de investigación.

Referencia: M. Domínguez-Dorado, D. Cortés-Polo, J. Carmona-Murillo, F. J. Rodríguez-Pérez and J. Galeano-Brajones, "*Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management*". Applied Science, vol. 13, no. 6327, 2023. <https://doi.org/10.3390/app13106327>

Factor de impacto de la publicación (JIF) en JCR 2023: 2.5

Categoría: CHEMISTRY, MULTIDISCIPLINARY. Ranking JIF: 114/230 (Q2).

Categoría: ENGINEERING, MULTIDISCIPLINARY. Ranking JIF: 44/79 (Q1).

Categoría: MATERIALS SCIENCE, MULTIDISCIPLINARY. Ranking JIF: 257/438 (Q3).




Categoría: PHYSICS, APPLIED. Ranking JIF: 87/179 (Q2).

Licencia: <https://creativecommons.org/licenses/by/4.0/>

© 2024 Los autores.

Article

Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management

Manuel Domínguez-Dorado ^{1,*}, David Cortés-Polo ², Javier Carmona-Murillo ³, Francisco J. Rodríguez-Pérez ³
and Jesús Galeano-Brajones ³

¹ Department of Information Systems and Digital Toolkit, Public Business Entity Red.es, 28020 Madrid, Spain

² Department of Signal Theory and Communications and Telematics Systems and Computing, Rey Juan Carlos University, 28933 Madrid, Spain

³ Department of Computing and Telematics Systems Engineering, University of Extremadura, 10003 Cáceres, Spain; jcarmur@unex.es (J.C.-M.); jgaleanobra@unex.es (J.G.-B.)

* Correspondence: manuel.dominguez@red.es; Tel.: +34-747756532

Featured Application: This study holds direct applicability for organizations seeking to establish comprehensive, tactical, and operational cybersecurity management, especially within the Cyber-TOMP framework. In order to achieve this objective, the concerned organization will need to achieve consensus among all functional domains involved in cybersecurity within the organization regarding the implementation of cybersecurity measures. The present proposal has been formulated with the aim of facilitating this process by devising a set of cybersecurity actions that will enable the organization to comply with its strategic cybersecurity goals upon their implementation.

Abstract: The increase in frequency and complexity of cyberattacks has heightened concerns regarding cybersecurity and created an urgent need for organizations to take action. To effectively address this challenge, a comprehensive and integrated approach is required involving a cross-functional cybersecurity workforce that spans tactical and operational levels. In this context there can be various combinations of cybersecurity actions that affect different functional domains and that allow for meeting the established requirements. In these cases, agreement will be needed, but finding high-quality combinations requires analysis from all perspectives on a case-by-case basis. With a large number of cybersecurity factors to consider, the size of the search space of potential combinations becomes unmanageable without automation. To solve this issue, we propose Fast, Lightweight, and Efficient Cybersecurity Optimization (FLECO), an adaptive, constrained, and multi-objective genetic algorithm that reduces the time required to identify sets of high-quality cybersecurity actions. FLECO enables productive discussions on viable solutions by the cross-functional cybersecurity workforce within an organization, fostering managing meetings where decisions are taken and boosting the overall cybersecurity management process. Our proposal is novel in its application of evolutionary computing to solve a managerial issue in cybersecurity and enhance the tactical–operational cybersecurity management process.

Keywords: tactical–operational cybersecurity management; process decision boosting; evolutionary computing; multi-objective genetic algorithm



Citation: Domínguez-Dorado, M.; Cortés-Polo, D.; Carmona-Murillo, J.; Rodríguez-Pérez, F.J.; Galeano-Brajones, J. Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management. *Appl. Sci.* **2023**, *13*, 6327. <https://doi.org/10.3390/app13106327>

Academic Editor: Vincent A. Cicirello

Received: 17 April 2023

Revised: 17 May 2023

Accepted: 20 May 2023

Published: 22 May 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cybersecurity has become a significant concern due to frequent and complex cyberattacks and a changing threat landscape, creating an emergency for organizations worldwide [1], such as an increase of up to 62% in cyberattacks to organization’s supply chain, and up to 75% in the number of general cyberattacks directly received by organizations [2]. To address this challenge, a holistic management approach and unity of action [3] are required, involving a cross-functional cybersecurity workforce from tactical and operational

levels, with a sense of urgency. However, in today’s organizational landscape, managing cybersecurity from a holistic perspective poses significant challenges. One of the most crucial obstacles is the lack of methodological development to manage cybersecurity at lower organizational levels, which can lead to improper organization and alignment with strategic cybersecurity goals, hindering the organization’s ability to respond quickly to changing cyber threats. While frameworks such as the Framework for Improving Critical Infrastructure Cybersecurity [4] or the International Organization for Standardization (ISO) 27000 [5,6] family of standards are commonly used at the strategic level, they fail to provide procedural foundations for tactical and operational levels. Another challenge lies in achieving holism [7] when collaborating in cross-functional internal–external teams with different chains of command at lower organizational levels, which necessitates the development of suitable mechanisms. Additionally, the absence of standardized and homogeneous cybersecurity evaluation criteria [8] at lower levels poses a significant challenge to assessing the current and expected cybersecurity status in a holistic manner.

To address this set of difficulties, CyberTOMP [9] was designed. It is a framework to manage holistic cybersecurity at tactical and operational levels. The CyberTOMP framework comprises various components that collectively provide organizations with what is necessary for the holistic management of cybersecurity at tactical and operational levels. One of these components is the Unified List of Expected Outcomes (ULEO), which is an organized list of cybersecurity actions in a four-level tree-structure format (asset level at the top, then function level, category level, and expected outcome level at the bottom). It is a common and homogeneous list that represents all the cybersecurity actions that should be implemented to protect a specific asset. Along with this, it defines a set of metrics that can be aggregated and that, together, allow for the evaluation of the current cybersecurity status of assets or their evolution over time, or the establishment of cybersecurity objectives at any level of the organization.

This list and set of metrics have been developed by combining cybersecurity actions from different de facto standards in this area [4,10,11]. None of these standards need to be implemented in the organization, but the application of CyberTOMP will allow for their implementation in a much faster and simpler way, if necessary. Furthermore, if any of these standards are already implemented in the organization, the application of CyberTOMP will already be partially achieved. Moreover, the complete list of cybersecurity actions (also called expected outcomes) are grouped in three different implementation groups (IGs) that allow organizations to apply proportionate cybersecurity actions depending on the criticality of assets (e.g., the minimum subset, the intermediate subset, or the whole list of cybersecurity actions). Each outcome has a discrete level of implementation (DLI) assigned to it [12], based on the deployment degree of the required actions to achieve the corresponding expected outcome (Figure 1). This ensures an impartial evaluation of an organization’s cybersecurity posture and avoids conflicts, bias, or misinterpretations.

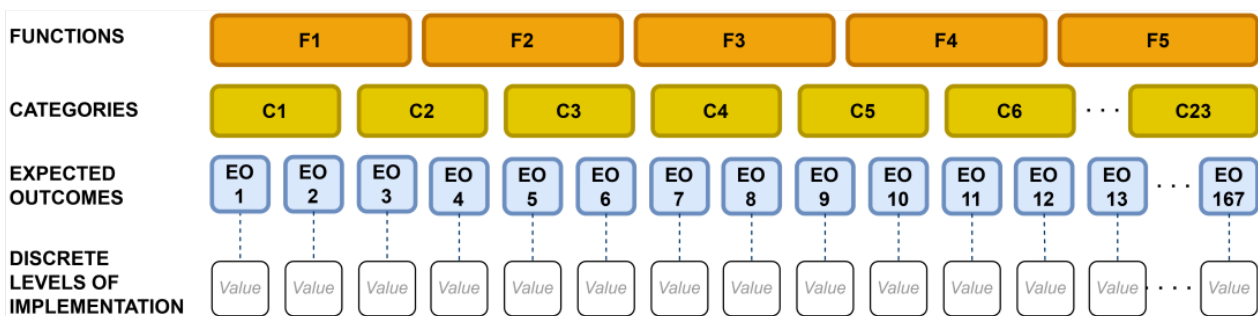


Figure 1. The ULEO breakdown from functions to expected outcomes, each assigned a DLI.

In addition to this component, CyberTOMP defines the process by which the cybersecurity workforce of the organization, consisting of different functional and multidisciplinary teams, must coordinate and work together to achieve the desired cybersecurity state in

an orchestrated, holistic, and simultaneously aligned manner with the organization's strategic objectives.

In general, the whole CyberTOMP framework has been designed in a way that guarantees that the implementation of the actions defined in the ULEO addresses a significant proportion of the current documented cyber threats [13].

The ULEO determines an asset's cybersecurity status based on the expected outcomes and their level of implementation. It also enables the assessment of cybersecurity status through hierarchical metrics and supports the establishment of strategic goals in the form of constraints for these metrics.

To comply with the strategic cybersecurity constraints, various combinations of expected outcomes, their implementation levels, and cybersecurity actions are possible and therefore must be evaluated. This is important because each expected outcome is translated into a set of required cybersecurity actions that have to be implemented. Consequently, each combination affects functional areas and can be influenced by previous or future investments in cybersecurity. Selecting a suitable combination requires determining the level of implementation for each outcome, ideally as close as possible to the current cybersecurity status. Metrics should be calculated to determine if the chosen solution meets the required constraints. If not, a new combination must be proposed. To attain the desired implementation levels, a thorough analysis of the work required must be conducted. Agreement among all functional areas is crucial, and if necessary, a new combination must be proposed to reach it.

CyberTOMP offers a guided process to coordinate cross-functional cybersecurity teams at all levels for the consecution of the expected outcomes at the desired level, achieving practical cybersecurity holism within the organization, easing the task list described in the previous paragraph. The process involves decision-makers meeting to agree on the asset's required cybersecurity status, the cybersecurity actions to be implemented, and their levels of implementation, metrics, and indicators. This is where holism is guaranteed in CyberTOMP.

In practical applications of CyberTOMP, selecting the set of cybersecurity actions and implementation levels that allows achieving a desired cybersecurity status for the asset is complex due to the vast number of potential solutions. For low criticality assets, there are 1.98×10^{28} possibilities, and for high criticality, there are 3.5×10^{100} options. Manually identifying the right combination of expected outcomes and levels of implementation is time-consuming and often unacceptable, making it challenging to reach an agreed-upon cybersecurity status during the management gatherings where decisions must be made. Meeting strategic constraints while aligning with current cybersecurity status is difficult, especially when the number of constraints increases. This results in a process that only targets the first feasible combination instead of exploring more possibilities, making it challenging to hold a productive discussion.

Natural selection is a biological concept that explains how species evolve based on their ability (or inability) to adapt to their surrounding environment. Each individual (a single specimen) within a population possesses specific characteristics that are determined by its genetic composition. A chromosome contains a defined number of genes, with each gene encoding information about a specific characteristic of the individual. The characteristics of an individual, which are defined by the alleles of each gene, are more or less beneficial to the individual depending on the specific value of the alleles. The level of adaptation of an individual within a species to their surrounding environment is determined by their particular characteristics, which are defined by the alleles of each of their genes. Individuals with better characteristics are more likely to reproduce and give rise to new individuals, while those who are less adapted are likely to become extinct without reproducing.

It is common for the offspring of well-adapted individuals to have even better characteristics, resulting in a better-adapted population through the process of reproduction and genetic exchange. Another way in which a population can evolve is through mutation.

While gene mutation in the natural world can often have fatal consequences, in certain cases, it can lead to a beneficial characteristic that enables an individual to unexpectedly prosper and become better adapted.

This natural evolutionary process has been transferred to the field of computing by designing algorithms, called genetic algorithms [14], that mimic the way nature works in order to solve complex optimization problems. To do so, a problem is usually defined as the context to which individuals (potential solutions to the problem) must adapt, and mechanisms similar to those existing in nature are applied [15]: mutation, crossover, adaptation, etc. Each individual is defined by a set of genes and alleles (variables and their respective values) that provide specific characteristics and determine their level of adaptation to the problem. In this context, being better adapted means being a better solution to the problem, while being less adapted means the opposite. Through a computationally accelerated process, genetic algorithms enable obtaining high-quality solutions to the proposed problem in a short amount of time in multiple applications.

Genetic algorithms are metaheuristic techniques useful in solving complex optimization problems [16], such as tactical–operational cybersecurity management. These problems involve a large search space and a multitude of constraints that must be satisfied simultaneously. Genetic algorithms are useful tools to manage the processes of the organization and decision-making in different areas as presented in [17], in which the authors review the operations management problems solved by genetic algorithms and suggest future research directions from the point of view of researchers and practitioners. Furthermore, [18] focuses on the application of genetic algorithms in the eight processes of supply chain management. In the field of cybersecurity, [19] presents a decision support system using a genetic algorithm to calculate uncertain cyberattack risk and determine the optimal combination of security countermeasures based on threat rates, costs, and asset impacts, whereas [20] introduces an approach to optimize cyber security investments using various methods for risk-averse organizations, aiming to reduce the cost of cyber insurance while improving self-protection. Finally, it is worth mentioning [21], which introduces a semi-automated approach based on Pareto optimality for selecting appropriate cybersecurity controls to minimize risks and address conflicting goals among stakeholders. To the best of our knowledge, there have been no prior studies employing genetic algorithms to support decision-making in the tactical and operational management of cybersecurity, specifically in the selection of cybersecurity actions applicable to business assets, from a holistic and cross-functional perspective.

By applying genetic algorithms to the exposed cybersecurity management optimization problem, organizations can improve their ability to choose faster, more accurately, and more easily the required cybersecurity actions to detect and respond to cyber threats, reduce vulnerability, and minimize risk.

This work contributes to tactical–operational cybersecurity management by means of a genetic algorithm that aids cross-functional cybersecurity teams in decision-making for the selection of the cybersecurity actions required to fulfill the strategic cybersecurity constraints/goals within the CyberTOMP framework. As a result of this, the decision-making process is boosted and made easier, leading to a reduction in the workload of cybersecurity personnel. The two most significant contributions of our study are as follows:

- An appropriate mechanism for searching feasible sets of cybersecurity actions for their application to the CyberTOMP framework.
- The demonstration of the application of evolutionary computing to decision-making in cybersecurity management.

These contributions are directly applicable to all organizations that deploy the CyberTOMP framework and are being validated by two different entities. Furthermore, they can be promptly adapted for use with other frameworks, with the National Institute of Standards and Technology (NIST) framework being particularly well-suited.

The subsequent sections of this document are organized as follows: In Section 2, a description of the relevant features and parameters of our algorithm is provided. Section 3

outlines the set of experiments that we conducted to assist decision-makers in selecting the appropriate cybersecurity actions to achieve strategic cybersecurity objectives. The results of these experiments are presented and discussed. The paper concludes with a summary and conclusions in Section 4.

2. Problem Modeling and Formulation

To achieve a comprehensive and effective cybersecurity strategy, it is essential to foster collaboration among the different functional areas that comprise the cross-functional cybersecurity workforce within an organization. In the CyberTOMP framework, this collaboration is facilitated through a series of meetings where the necessary cybersecurity safeguards required to achieve strategic cybersecurity constraints are established. However, in practice, these meetings can be ineffective as the number of possible combination of actions is too large to be manually or nearly manually identified and analyzed within a reasonable period.

The main objective of our research is to provide a technological solution to address this managerial challenge. Specifically, our study aims to develop a Fast, Lightweight, and Efficient Cybersecurity Optimization (FLECO) mechanism consisting of an adaptive, constrained and multi-objective genetic algorithm. This algorithm will enable the swift identification of high-quality solutions or sets of solutions that can be discussed among all cybersecurity participants, thus facilitating the applicability of tactical–operational cybersecurity management processes within the organization.

As stated, the field of evolutionary algorithms, and genetic algorithms in particular, has been used broadly to solve not only technical aspects, but also, often, managerial challenges in a broad range of disciplines. In this case our proposal consists of applying this approach to a cybersecurity management problem, thus contributing to enhancing the procedural basis for cybersecurity management at organizations' lower levels.

2.1. Determining Value of FLECO Parameters

In the course of designing and developing FLECO, multiple adjustments were required to ensure that the algorithm operated as intended and yielded valuable solutions. FLECO is designed for organizations that are implementing the CyberTOMP framework to manage cybersecurity at the tactical and operational levels, and to ensure its comprehensive validity, we collaborated with two organizations in the design and validation process. The first organization is a non-technological small or medium-sized enterprise (SME), consisting of fewer than 40 employees and only 2 departments. The meetings held to discuss the cybersecurity actions to be implemented include only three to five individuals. The second organization is a public entity with over 300 direct employees, 5 departments, and 11 primary functional areas. This organization has several outsourcing contracts, and its teams comprise in-house as well as external personnel. Meetings held to determine the set of cybersecurity actions involve 15–20 individuals. Both organizations are implementing CyberTOMP to varying degrees and have encountered the challenges outlined in Section 1. During the multifunctional cybersecurity workforce meetings, where the different teams must reach an agreement on which cybersecurity actions to implement and to what depth, these teams were unable to find a solution in these two companies. The main reason is the large number of existing combinations, which is unmanageable manually; a secondary reason is that the different teams were unable to search for combinations that simultaneously satisfied more than one objective: complying with the constraints defined at the strategic level related to CyberTOMP metrics; maximizing similarity with respect to the currently enforced combination to leverage previously completed work; and maximizing all the assets' global cybersecurity state. Without the possibility of finding valid combinations that maintain a balance between all objectives, the work meetings planned in CyberTOMP to ensure the required holism are meaningless. Therefore, the main motivation of our work is the design of a technological mechanism that enables the quick obtainment of solutions

that can be shared in the meetings planned in CyberTOMP, and thus, achieve the necessary holism in these organizations.

During the design phase of FLECO, we conducted hundreds of executions, most of which were unsuccessful. We made numerous modifications and decisions in collaboration with the aforementioned organizations, such as determining the value of the weights, defining strategic constraints, specifying the requirements for a solution to be deemed acceptable, and defining the genetic operators, among others [22]. At the end of the experimentation phase, these organizations participated in validating the efficacy of the proposal and testing its effectiveness in their specific use cases.

2.2. Formulation of the Multi-Objective Optimization Problem

Let P be the multi-objective optimization problem [23,24]. Let $S = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ be the set of feasible solutions for the optimization problem. Let $\vec{x} = (x_1, x_2, \dots, x_n)$ be the vector representation of an asset's cybersecurity status, where each element x_k denotes the degree to which the required cybersecurity measures have been implemented to achieve the expected outcome k . The length of the vector is determined by n , which varies depending on the cybersecurity criticality of the asset. We define $f1(\vec{x})$ as a real-valued function that quantifies the number of strategic cybersecurity constraints satisfied by the vector \vec{x} . Similarly, we define $f2(\vec{x})$ as a real-valued function that captures the similarity between the current asset's cybersecurity state and a previously recorded state. Finally, we define $f3(\vec{x})$ as a real-valued function that characterizes the overall level of cybersecurity achieved by the asset, as determined by its current cybersecurity status represented by \vec{x} .

Formally, we express $f1(\vec{x})$, $f2(\vec{x})$, and $f3(\vec{x})$ as functions that belong to the set of real numbers (\mathbb{R}), such that $0.0 \leq f1(\vec{x}), f2(\vec{x}), f3(\vec{x}) \leq 1.0$. These functions are designed to satisfy mathematical properties that allow for their effective use in the optimization process, which ensures that their values are meaningful and can be used to compare different solutions in a mathematically rigorous manner.

FLECO computes the individual fitness by means of a scalarization function, as shown in Equation (1). Specifically, the weighted sum scalarization function used is $f(\vec{x}) = \sum_{i=1}^3 f_i(\vec{x}) \cdot \omega_i$, where ω_i is the weight associated to each objective ($\sum_{i=1}^3 \omega_i = 1.0$). The values of ω_1 , ω_2 , and ω_3 were determined after an extensive analysis process. During this period, hundreds of FLECO executions were performed with different initial statuses and various strategic constraints. These executions were supervised by the organizations' decision-makers, who worked together with experts and the rest of the team to tune the weights until the convergence time of FLECO was deemed acceptable, and the generated solutions met the requirements of the organization. Finally, the values of ω_1 , ω_2 , and ω_3 were established as $\omega_1 = 0.94$, $\omega_2 = 0.05$, and $\omega_3 = 0.01$, which were deemed to be the optimal weights for the FLECO algorithm.

We define the multi-objective problem as follows:

$$\begin{aligned} & \text{maximize} && f(\vec{x}) = 0.94 \cdot f1(\vec{x}) + 0.05 \cdot f2(\vec{x}) + 0.01 \cdot f3(\vec{x}) \\ & && \\ & \text{subject to} && f1(\vec{x}) = 1.00 \quad \forall \vec{x} \in S \end{aligned} \tag{1}$$

The function denoted by $f1(\vec{x})$ serves to amalgamate the set of strategic cybersecurity constraints [25]. This approach was chosen to provide guidance to the algorithm towards generating a high-quality set of feasible solutions. Consequently, while non-feasible solutions persist within the population, they are not regarded as solutions.

2.3. Representation of Individuals

The present study considers the expected outcome level resulting from the structure of the ULEO, as depicted in Section 1, Figure 1. This expected outcome level will be

treated as a chromosome in the problem under consideration [26]. Due to the three distinct implementation groups, the expected outcomes are clustered accordingly. Hence, there are three possible chromosome lengths, as not all expected outcomes are applicable to every implementation group. Based on the cybersecurity criticality of the asset and its corresponding implementation group, the FLECO is capable of handling individuals with 47, 107, or 167 genes. Each gene represents an expected outcome from the ULEO.

In practical deployment, achieving the mentioned outcome would necessitate a set of cybersecurity actions to be implemented. Depending on the extent to which these actions are accomplished, a discrete level of implementation is assigned to each gene. These four discrete levels of implementations are the alleles in our proposal (Figure 2).

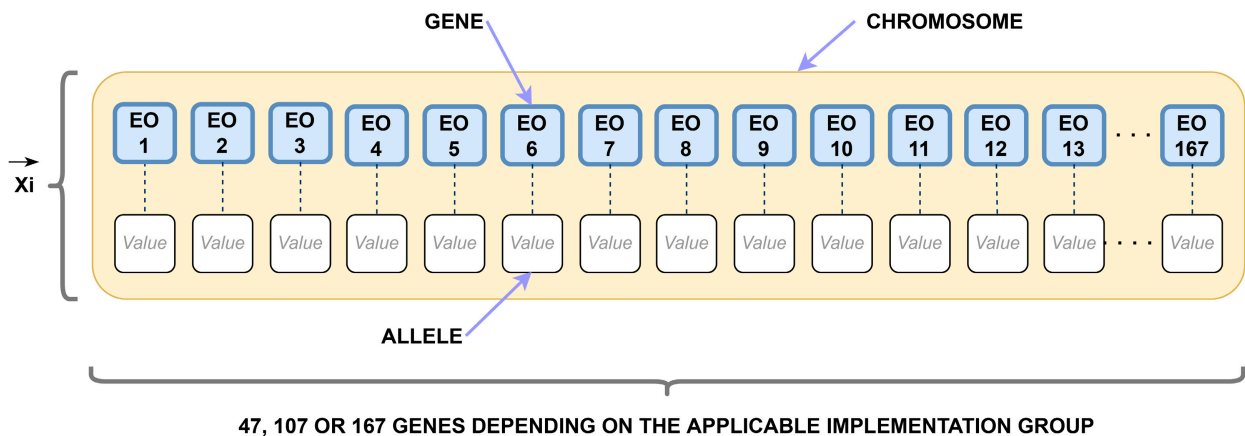


Figure 2. Chromosome definition from the ULEO.

Finally, the number of genes (decision variables) and alleles (values for those decision variables) determine the number of potential solutions that could be explored, depending on the applicable implementation group. The number of possibilities to explore for implementation group 1, 2, and 3 are 1.98070×10^{28} , 2.63281×10^{64} , and 3.4996×10^{100} , respectively, as shown in Table 1.

Table 1. Characterization of an individual in FLECO.

IG	Genes	Alleles	Combinations
1	47	4	$198,070 \times 10^{28}$
2	107	4	$263,281 \times 10^{64}$
3	167	4	$34,996 \times 10^{100}$

2.4. Crossover and Mutation Operators

Our proposal uses a standard two-point crossover operator with a crossover rate of 0.90 that was chosen based on previous ranges in the literature [27,28] and experimentation. The objective is to balance chromosome recombination with preserving genetic material from highly fit individuals. When triggered, two new offspring are generated from each set of two parents.

The mutation phase uses a predetermined rate of $1/L$, where L is the number of decision variables (the chromosome length). This rate is widely used in the related literature [29] and is known to provide significant diversity. FLECO applies this mutation rate to every gene in each chromosome, ensuring that, when applicable, the new allele is different from the current one. If the mutation is triggered for any gene, an additional new individual is generated from the corresponding chromosome.

2.5. Population and Selection Method

FLECO's initial population includes high-quality and randomly selected individuals to reach the designated population size. Subsequent populations are generated through a selection process, followed by the application of the crossover and mutation mechanisms until the population reaches the defined value. Individuals are then sorted based on fitness, and the top 30 individuals are selected to maintain the predetermined population size after each generation. A population size of 30 individuals was chosen based on an examination of various alternatives within the range provided in [30] for population size, mutation, and crossover rates. During each generation, the algorithm identifies the most suitable individuals for the reproduction phase. Twins are excluded from the population as they possess identical genetic material, which detracts from the quality of the population [31,32]. The top 1/5 (20%) of individuals are selected for reproduction, while the remainder are discarded, based on a threshold established through micro-experiments to promote FLECO's convergence time and produce feasible solutions of remarkable quality.

2.6. Algorithm Stopping Criteria

The business challenge that FLECO aims to solve, as described in Section 1, requires the swift response of a feasible solution. A feasible solution in this context must satisfy the following requirements:

- The solution is provided in a timely manner. Since the solution must be discussed in a meeting to reach agreements, it is necessary that the solution is provided to the cross-functional cybersecurity workforce by FLECO within a reasonable timeframe, no longer than 5 min. This requirement has been established by the organization's decision-maker responsible for deploying the CyberTOMP framework. Subsequently, the proposed solution can be deliberated upon amongst various functional domains, ultimately accepted upon consensus, or rejected outright.
- The solution must fulfill all the specific cybersecurity constraints, which is ultimately achieved if $f1(\vec{x}) = 1.0$ as described in Section 2.2.
- The algorithm will terminate when either of the two conditions is met.

In the event that the algorithm terminates due to time constraints (the limit of five minutes), the population may not have converged, and the resulting solutions may not be feasible. This can occur when the algorithm reaches a stagnation point and is unable to escape it, but it is more likely to happen when the strategic constraints are highly stringent or even contradictory, rendering it impossible to identify a solution that satisfies all of them.

Furthermore, in the process of designing and developing FLECO, it was determined that the algorithm must be able to run on general-purpose hardware, comparable to the ones employed in the organizations' operational setting, such as a standard laptop or desktop personal computer, rather than on specialized hardware.

2.7. Stagnation Detection and Scape

The FLECO algorithm incorporates a mechanism to detect stagnation and, if possible, escape it in order to converge towards a high-quality solution (Algorithm 1). To do so, a time threshold (2.5%) is defined as a percentage of the maximum allowed time (five minutes). At the beginning of the algorithm, the current time is recorded and updated every time the best individual fitness is improved. If there is no improvement, the time remains the same. This approach enables the computation of the consumed amount of time from the last improvement of the best chromosome's fitness. If the time reaches the defined threshold and the population has not yet converged, the stagnation warning is triggered.

Algorithm 1. Pseudo-code of the mechanism for stagnation detection and scape.

```

1:  Set default values for FLECO parameters
2:  While conditions to stop FLECO are not met
3:      Update last time the best individual's fitness changed
4:      Compute period from last time best individual's fitness changed to "now"
5:      Estimate whether FLECO seems to be in a local minimum
6:      Estimate whether FLECO is deeply stagnated
7:      If seems to be in a local minimum
8:          Apply increased mutation rate
9:          If it is deeply stagnated
10:             Remove current 50% of population's
                best individuals (soft reset)
                Regenerate the population with
                random individuals
11:          End if
12:          Increase diversity by adding extra random individuals
13:      Else
14:          Reset FLECO parameters to their default values
15:      End if
16:  End while

```

Under stagnation, the FLECO algorithm adapts dynamically to try to escape from local minimums:

- The "raw" population size, which is typically 30 in our proposal or very close to it, is enlarged up to 50% more, resulting in a total of 45 individuals [33,34]. This size adjustment aims to help the algorithm explore alternative regions of the solution space.
- Additionally, the mutation rate, usually fixed at 0.05, is dynamically increased [35] 20-fold to yield a value of 1.0, which helps the algorithm evade potential sub-optimal solutions.
- If the entrapment situation persists despite these adaptive adjustments, a secondary threshold (3.13%) is used to detect it. In this case, the top 1/2 (50%) of the best fitted individuals in the population are removed from the population and replaced by random individuals. This adjustment functions as a soft reset for the algorithm [36], preserving part of the already mature population while eliminating the most problematic individuals. This approach enables FLECO to escape from low-quality solutions in most situations and explore alternative regions of the solution space.

This parameter adjustment process implemented in FLECO to prevent stagnation improves upon its adaptive capabilities [37], enabling it to effectively respond to the evolving problem context. The activation of the jamming alert does not inherently impact the quality of the solution identified by FLECO. It serves solely as a mechanism to detect the potential occurrence of the algorithm becoming trapped in a local minimum. If such a situation arises, the alert aids in the algorithm's escape from this state and facilitates the continued exploration of the solution space for potential alternatives. Once the local minimum is successfully bypassed, the dynamic parameters are reset to their predetermined values.

3. Experiments Design and Result

The management of tactical and operational aspects of cybersecurity is of paramount importance in achieving comprehensive and effective cybersecurity. To this end, and in response to the needs of the organizations' decision-makers, our experiments were designed to assess whether FLECO could deliver a meaningful enhancement in terms of efficiency and effectiveness, thereby significantly improving the decision-making process in cybersecurity management meetings and ultimately optimizing cybersecurity outcomes.

3.1. Definition of Initial Statuses

In order to ensure uniformity in all experiments, we deemed it appropriate to utilize a set of randomly chosen chromosomes that would serve as the initial cybersecurity status

for hypothetical assets, where their criticality level necessitates the application of IG1, IG2, or IG3. To prevent any potential bias in the operation of FLECO stemming from the use of specific initial statuses, we generated 15 unique, randomized initial statuses for each implementation group, allowing for testing under diverse circumstances.

3.2. Definition of Strategic Constraints

In a manner analogous to the configuration of initial states, a series of strategic constraints were devised in order to test each scenario under equivalent conditions. The primary objective of these strategic constraints was to encompass a minimum of 10% of the metrics outlined in the CyberTOMP proposal, at all levels (i.e., asset, function, category, or expected outcome). Notably, in practical applications of CyberTOMP, average metric coverage was observed to be below 1% for all cases, as it is highly unusual for personnel operating in the strategic sphere to establish constraints that fall beneath the level of asset or cybersecurity function. Nonetheless, in order to rigorously evaluate FLECO under challenging conditions, we opted to apply four sets of constraints that were 10 times greater in scale (Table 2) to assess the effectiveness at asset, function, category, or expected outcome levels.

Table 2. Coverage provided by the synthetic set of strategic constraints depending on each IG.

Strategic Constraints	IG1	IG2	IG3	Cumulated IG1	Cumulated IG2	Cumulated IG3
Asset constraints	1	1	1	1	1	1
Function constraints	1	1	1	2	2	2
Category constraints	2	2	3	4	4	5
Expected outcomes constraints	5	11	17	9	15	22
Total constraints	9	15	22	9	15	22

The strategic objectives are established in a fixed and proportionate manner to equally influence the exploration of potential solutions, regardless of the implementation group or the length of the chromosome.

In Table 3, the strategic constraints that have been established for our experiments are presented in conjunction with their applicability to each implementation group. Each constraint has been defined as an operator and a value that references a metric that is defined in CyberTOMP.

3.3. Definition of Analysis Cases

The test suite comprises twelve combinations derived from the amalgamation of the three implementation groups and the four sets of predetermined strategic constraints at asset (A), function (F), category (C), and expected outcomes (EO) levels. The strategic constraints are clustered into four hierarchical levels, namely A, A-F, A-F-C, and A-F-C-EO levels that aggregate the corresponding constraints. These experiments focused on the evaluation of the convergence, convergence time, and solution quality, as well as the ability of FLECO to navigate the constrained region of solutions. To ensure comprehensiveness, 15 initial statuses are employed (Section 3.1) and executed 15 times for each combination of implementation group and constraint type, resulting in a set of 225 executions per combination and a total of 2700 FLECO executions.

3.4. Execution and Experiment Results

The time required by FLECO to generate solutions after executing the test suite is shown in Table 4. Every row represents a combination where 225 FLECO executions are summarized. The table shows, hence, the whole 2700 FLECO executions. The time mean, standard deviation, and median of every test case are presented in columns t , $\sigma(t)$, and \tilde{t} , respectively.

Table 3. Defined strategic constraints and their applicability to each IG.

Strategic Constraint Type	Asset	Function	Category	Expected Outcome	Operator	Value	IG1	IG2	IG3
Asset	Asset	-	-	-	>	0.65	✓	✓	✓
Function	Asset	ID	-	-	≥	0.6	✓	✓	✓
Category	Asset	RC	RC.CO	-	<	0.8			✓
Category	Asset	PR	PR.AC	-	>	0.6	✓	✓	✓
Category	Asset	ID	ID.SC	-	≥	0.5	✓	✓	✓
Expected outcome	Asset	RC	RC.CO	RC.CO-3	>	0.6			✓
Expected outcome	Asset	RS	RS.MI	RS.MI-3	≥	0.3			✓
Expected outcome	Asset	DE	DE.DP	DE.DP-5	=	0.67			✓
Expected outcome	Asset	DE	DE.AE	DE.AE-5	<	0.6			✓
Expected outcome	Asset	PR	PR.PT	9D-7	≤	0.6			✓
Expected outcome	Asset	ID	ID.BE	ID.BE-3	≥	0.7			✓
Expected outcome	Asset	ID	ID.AM	CSC-12.4	=	0.33		✓	✓
Expected outcome	Asset	ID	ID.GV	CSC-5.6	≥	0.2		✓	✓
Expected outcome	Asset	PR	PR.AC	CSC-5.6	>	0.6		✓	✓
Expected outcome	Asset	PR	PR.IP	9D-8	≥	0.3		✓	✓
Expected outcome	Asset	DE	DE.AE	DE.AE-1	=	0.67		✓	✓
Expected outcome	Asset	RS	RS.AN	RS.AN-1	<	0.6		✓	✓
Expected outcome	Asset	ID	ID.AM	CSC-3.6	≤	0.6	✓	✓	✓
Expected outcome	Asset	PR	PR.MA	CSC-4.2	≥	0.5	✓	✓	✓
Expected outcome	Asset	DE	DE.AE	DE.AE-3	=	0.33	✓	✓	✓
Expected outcome	Asset	DE	DE.CM	DE.CM-4	≥	0.2	✓	✓	✓
Expected outcome	Asset	RS	RS.MI	CSC-1.2	≥	0.2	✓	✓	✓

Table 4. Time required for each analysis case.

IG	Strategic Constraints Levels	\bar{t}	$\sigma(t)$	\tilde{t}
1	A	0.211166	0.071250	0.200270
1	A-F	0.219383	0.108698	0.223835
1	A-F-C	0.236180	0.099249	0.246635
1	A-F-C-EO	0.245545	0.192466	0.191478
2	A	0.667603	0.152436	0.677265
2	A-F	0.634475	0.171314	0.661716
2	A-F-C	0.712537	0.253927	0.760814
2	A-F-C-EO	0.388333	0.214490	0.294797
3	A	1.241601	0.322026	1.300380
3	A-F	1.291096	0.309675	1.315561
3	A-F-C	1.387193	0.308389	1.449513
3	A-F-C-EO	0.574846	0.261707	0.519179

It is noteworthy that the FLECO algorithm demonstrated a 100% convergence rate in all 2700 executions (225 per case of analysis) conducted. This is of significant importance for the practical application of the algorithm to the real-world problem it is designed to address. Notably, despite being permitted a convergence time up to five minutes, the average time required by FLECO was $\approx 1.39 \pm 0.31$ s in the worst-case scenario. However, in the majority of the analysis cases, the minimum time to obtain a feasible solution was less, reaching $\approx 0.21 \pm 0.07$ s in the most favorable case. The convergence time tends to increase with an escalation in the number of constraints in the implementation group, i.e., when the chromosomes are larger, but even in these cases it is maintained below (and far from) the defined limit. Thus, the requirement of achieving a solution in less than five minutes is greatly accomplished by FLECO, which has been demonstrated to be fast. Moreover, all the experiments have been executed in hardware below the specified requirements, achieving the mentioned values, which reveals also that FLECO is efficient in the use of resources.

Regarding the quality of the generated solutions, in Tables 5 and 6, the fitness means, $fi(\vec{x})$, for each optimization function and for the weighted function are shown, together

with the median, $\widetilde{fi(\vec{x})}$, and also the corresponding standard deviation, $\sigma(fi(\vec{x}))$, that indicates the dispersion degree of the 225 solutions for each analysis case. The average measurements of the functions $f(\vec{x})$, $f1(\vec{x})$, $f2(\vec{x})$, and $f3(\vec{x})$, along with the corresponding disaggregated measurements, exhibit close proximity to the solution anticipated by the decision-makers of the organizations. These measurements align with the requirements of FLECO for recognizing a solution as feasible, where $f1(\vec{x}) = 1.0$, and, moreover, the observation of closely similar values across the various scenarios tested is indicative of FLECO’s ability to obtain solutions of comparable quality, regardless of the situation.

Table 5. Fitness evaluation of the three objective functions.

IG	Strategic Constraints Levels	$f1(\vec{x})$	$\sigma(f1(\vec{x}))$	$\widetilde{f1(\vec{x})}$	$f2(\vec{x})$	$\sigma(f2(\vec{x}))$	$\widetilde{f2(\vec{x})}$	$f3(\vec{x})$	$\sigma(f3(\vec{x}))$	$\widetilde{f3(\vec{x})}$
1	A	1.00	0.00	1.00	0.804147	0.009005	0.801489	0.669295	0.017062	0.665523
1	A-F	1.00	0.00	1.00	0.817820	0.041293	0.801489	0.667423	0.015376	0.662577
1	A-F-C	1.00	0.00	1.00	0.814755	0.035440	0.801489	0.669001	0.016742	0.663130
1	A-F-C-EO	1.00	0.00	1.00	0.811145	0.016723	0.801489	0.662561	0.011586	0.659791
2	A	1.00	0.00	1.00	0.803195	0.011234	0.800561	0.660704	0.010372	0.658164
2	A-F	1.00	0.00	1.00	0.803958	0.012015	0.800561	0.660461	0.009044	0.658408
2	A-F-C	1.00	0.00	1.00	0.808690	0.022809	0.800561	0.659015	0.008397	0.656217
2	A-F-C-EO	1.00	0.00	1.00	0.820165	0.022698	0.809813	0.654826	0.005065	0.653115
3	A	1.00	0.00	1.00	0.807198	0.024698	0.800419	0.657923	0.006619	0.656296
3	A-F	1.00	0.00	1.00	0.803646	0.013384	0.800359	0.659479	0.009102	0.656734
3	A-F-C	1.00	0.00	1.00	0.802865	0.010542	0.800359	0.659695	0.009007	0.657471
3	A-F-C-EO	1.00	0.00	1.00	0.841527	0.028920	0.839940	0.653301	0.003522	0.652164

Table 6. Fitness evaluation of the scalarization function.

IG	Strategic Constraints Levels	$f(\vec{x})$	$\sigma(f(\vec{x}))$	$\widetilde{f(\vec{x})}$
1	A	0.986900	0.000467	0.986783
1	A-F	0.987565	0.002054	0.986796
1	A-F-C	0.987428	0.001752	0.986874
1	A-F-C-EO	0.987183	0.000835	0.986812
2	A	0.986767	0.000559	0.986670
2	A-F	0.986803	0.000595	0.986680
2	A-F-C	0.987025	0.001132	0.986647
2	A-F-C-EO	0.987557	0.001130	0.987106
3	A	0.986939	0.001223	0.986627
3	A-F	0.986777	0.000664	0.986639
3	A-F-C	0.986740	0.000527	0.986625
3	A-F-C-EO	0.988609	0.001446	0.988549

The computed standard deviation for each case is kept around 10^{-3} for all analysis cases, which denotes that FLECO is able to reach solutions with similar quality regarding the surrounding conditions. The test suite was purposefully designed and implemented to validate FLECO, incorporating diverse conditions for each run. These conditions include variations in starting points, restrictions on metrics, implementation groups, random populations, and other factors. As a result, we have been able to gather results from a total of 2700 executions. Although each execution possesses unique characteristics, they all exhibit a similar level of quality and completion time. This achievement is attributed to the meticulous fine-tuning of various algorithm parameters, guided by decision-makers from different domains from the collaborating companies. Weeks of testing have facilitated the enhancement of FLECO’s capability to effectively explore the solution space and discover high-quality solutions. This serves as a positive indication of the algorithm’s efficacy and consistency in generating solutions, and its ability to comply with the requirement of generating valuable solutions for the cybersecurity workforce to discuss.

Regarding FLECO's ability to explore the solution space, Figure 3 presents 12 charts, each corresponding to an analysis case where 225 solutions are displayed (2700 in total).

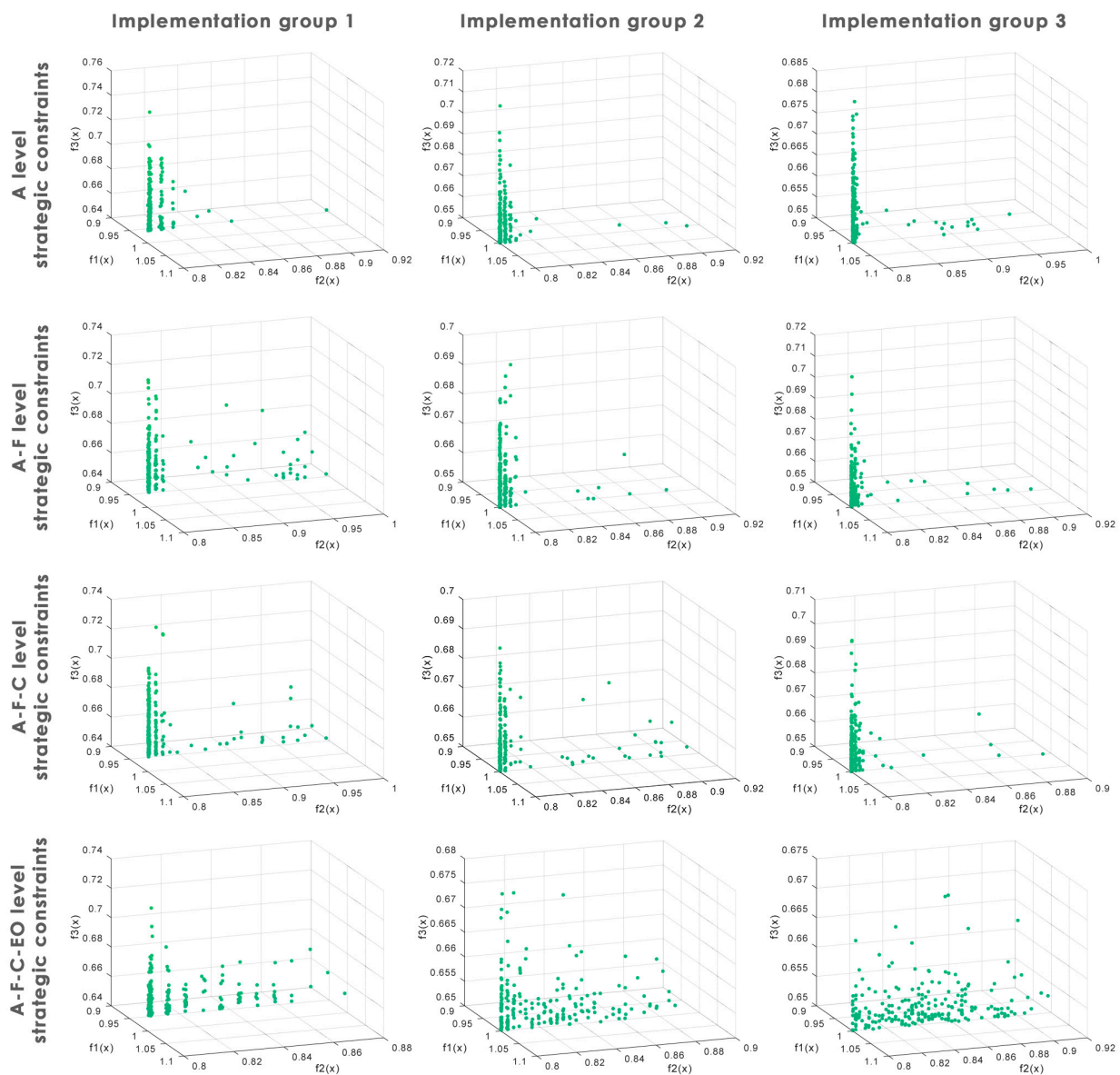


Figure 3. Approximation achieved by FLECO of the constrained solutions space. Each green dot is a feasible, high-quality solution found by FLECO.

These charts depict the impact of applying constraints to the problem and its consequent effect on the constrained solution space. The results indicate that the feasible solution space becomes more fragmented as the number of decision variables is increased (which is the same as increasing the corresponding IG) and when more constraints are imposed on the problem, ranging from 1 to 22 in the designed experiments. Nonetheless, what is noteworthy is that the FLECO algorithm managed to explore these narrow segments of the constrained solutions space, in search of solutions, at an adequate level.

4. Conclusions and Future Work

In this research work, we address the potential of evolutionary computation for solving an optimization problem related to cybersecurity management. To this end, we have developed FLECO, a multi-objective, constrained, and adaptive genetic algorithm that assists the cybersecurity workforce in selecting the set of actions that must be implemented

to comply with the cybersecurity restrictions required from the strategic sphere. The multidisciplinary cybersecurity teams, consisting of 3–5 and 15–20 members, respectively, from the collaborating companies in this study encountered difficulties in finding feasible combinations of cybersecurity actions without the aid of FLECO. These combinations were essential for their discussions and the achievement of comprehensive agreements as mandated by the CyberTOMP framework. Despite numerous attempts over the course of a month while the design of FLECO was in progress, the teams were unsuccessful in identifying a feasible set of cybersecurity actions that met the requirements within the specified timeframe of less than 5 min, as stipulated by the decision-makers of these companies. In fact, they were unable to find a suitable set even after dedicating significant additional time. Addressing this need, FLECO provides feasible sets of cybersecurity actions that fulfill the multiple established objectives in a significantly shorter time than what is required by the decision-makers of the participating companies. This capability has enabled them to conduct tactical–operational management meetings, explore different combinations, and achieve holistic cybersecurity starting from the lower levels of the organization. The specific contributions of our work to this scenario are as follows:

1. An effective mechanism, as it discovers solutions that comply with all business-level constraints.
2. A rapid mechanism, as it achieves this within a timeframe of less than 5 min, facilitating the smooth implementation of the CyberTOMP framework.
3. An efficient mechanism, as it operates using general-purpose hardware similar to the workstations commonly found in contemporary companies.
4. A predictable mechanism, as it exhibits stable behavior regardless of search conditions, consistently delivering solutions of comparable quality.
5. The practical demonstration of the application of evolutionary computing to decision-making in cybersecurity management.

The algorithm has been designed based on the specifications of the CyberTOMP framework, which makes it useful and directly applicable to organizations that are using this framework for tactical and operational cybersecurity management. However, it is easily modifiable to adapt to similar frameworks, the NIST framework being particularly well-suited. Furthermore, the set of test cases designed to validate FLECO has also aimed to minimize bias and the influence that the participation of two specific organizations may have on the results.

FLECO has demonstrated its speed, efficiency, and effectiveness in finding solutions in a wide variety of contexts, meeting the expectations set by decision-makers in the participating organizations regarding the quality of the solutions provided, the speed with which those solutions are generated, and the positive effect this has on the holistic, tactical–operational cybersecurity management process and meetings that CyberTOMP foresees to discuss and jointly agree on cybersecurity actions to execute.

In summary, we can say that evolutionary computation in general, and genetic algorithms such as FLECO in particular, can positively make a difference in decision-making in a poorly explored area such as tactical–operational cybersecurity management.

As part of our research we have also identified some lines for future work we deem necessary to expose. Firstly, although we have made every effort to design both the algorithm and experiments to avoid bias, it is difficult to eliminate it completely given the subjectivity inherent in defining a solution as good or bad for each organization and its reflection in the weights and ratios that serve as a parameter for the algorithm. For that reason, we intend to address this by conducting further tests with different types of organizations focused on increasing the validity of FLECO in any situation. We also believe that it is important to explore alternatives that require less intervention by decision-makers for their final adjustment, such as algorithms based on Pareto dominance. Secondly, while FLECO represents a qualitative and quantitative leap in the application of the principles indicated by the CyberTOMP framework, we believe that this contribution could be much greater if optimization functions were defined that covered more complex business objectives and

whose outcome was to minimize the human effort required to select the set of cybersecurity actions. As a consequence, we plan to expand the solution by including economic or effort aspects required for each expected cybersecurity outcome, which could significantly enhance the assistance that FLECO provides to the teams responsible for selecting and designing cybersecurity actions.

Author Contributions: All authors of this article have contributed equally to the conception, design, execution, and interpretation of the research. Each author has played an integral part in drafting and revising the manuscript and has approved the final version for submission. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by TED2021-131699B-I00AEI/10.13039/501100011033/ Unión Europea NextGenerationEU/PRTR and by the Spanish Ministry of Science and Innovation [PID2020-112545RB-C54, PDC2022-133900-I00]. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available in the article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. ENISA. *ENISA Threat Landscape 2022*; European Union Agency for Cybersecurity: Heraclión, Greece, 2022; Available online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022> (accessed on 21 May 2023).
2. CCN-CERT. *Ciberamenazas y tendencias-Edición 2022*; CCN: Madrid, Spain, 2022; Available online: <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html> (accessed on 21 May 2023).
3. van Kranenburg, R.; Le Gars, G. The Cybersecurity Aspects of New Entities Need a Cybernetic, Holistic Perspective. *Int. J. Cyber Forensic Adv. Threat. Investig.* **2021**, *1*, 2. [CrossRef]
4. NIST. *Framework for Improving Critical Infrastructure Cybersecurity v1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. Available online: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (accessed on 21 May 2023).
5. *ISO/IEC JTC 1/SC 27; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*. ISO/IEC: Geneva, Switzerland, 2022.
6. *ISO/IEC JTC 1/SC 27b; Information Security, Cybersecurity and Privacy Protection—Information Security Controls*. ISO/IEC: Geneva, Switzerland, 2022.
7. Tisdale, S.M. Architecting a cybersecurity management framework. *Issues Inf. Syst.* **2016**, *17*, 227–236.
8. Axon, L.; Arnau, E.; van Rensburg, A.J.; Nurse, J.R.C.; Goldsmith, M.; Creese, S. Practitioners' Views on Cybersecurity Control Adoption and Effectiveness. In Proceedings of the ARES 21: Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021.
9. Domínguez-Dorado, M.; Carmona-Murillo, J.; Cortés-Polo, D.; Rodríguez-Pérez, F.J. CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels. *IEEE Access* **2022**, *10*, 122454–122485.
10. *CIS, CIS Critical Controls(R). Version 8*; Center for Internet Security: New York, NY, USA, 2021.
11. Wilson, K.S.; Kiy, M.A. Some Fundamental Cybersecurity Concepts. *IEEE Access* **2014**, *2*, 116–124. [CrossRef]
12. *Center for Internet Security, CIS Community Defense Model v2.0*; CIS: New York, NY, USA, 2021.
13. MITRE, MITRE ATT&CK. Available online: <https://attack.mitre.org/> (accessed on 3 March 2023).
14. Katoch, S.; Chauhan, S.S.; Kumar, V. A review on genetic algorithm: Past, present, and future. *Multimed. Tools Appl.* **2021**, *80*, 8091–8126. [CrossRef] [PubMed]
15. Alhijawi, B.; Awajan, A. Genetic algorithms: Theory, genetic operators, solutions, and applications. *Evol. Intell.* **2023**. [CrossRef]
16. Alorf, A. A survey of recently developed metaheuristics and their comparative analysis. *Eng. Appl. Artif. Intell.* **2023**, *117*, 105622. [CrossRef]
17. Lee, K. A review of applications of genetic algorithms in operations management. *Eng. Appl. Artif. Intell.* **2018**, *76*, 1–12. [CrossRef]
18. Jauhar, S.K.; Pant, M. Genetic algorithms in supply chain management: A critical analysis of the literature. *Sādhanā* **2016**, *41*, 993–1017. [CrossRef]
19. Rees, L.P.; Deane, J.K.; Rakes, T.R.; Baker, W.H. Decision support for Cybersecurity risk planning. *Decis. Support Syst.* **2011**, *51*, 493–505. [CrossRef]

20. Uganbayar, G.; Yautsiukhin, A.; Martinelli, F.; Massacci, F. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Comput. Secur.* **2021**, *101*, 102121. [[CrossRef](#)]
21. Mollaeefar, M.; Ranise, S. Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR. *Comput. Secur.* **2023**, *129*, 103206. [[CrossRef](#)]
22. Deb, K.; Agrawal, S. Understanding interactions among genetic algorithm parameters. *Found. Genet. Algorithms* **1999**, *5*, 265–286.
23. Falcón-Cardona, J.G.; Gómez, R.H.; Coello, C.A.; Tapia, M.G. Parallel Multi-Objective Evolutionary Algorithms: A Comprehensive Survey. In *Swarm and Evolutionary Computation*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 67, pp. 1–23.
24. Konak, A.; Coit, D.W.; Smith, A.E. Multi-objective optimization using genetic algorithms: A tutorial. *Reliab. Eng. Syst. Saf.* **2006**, *91*, 992–1007. [[CrossRef](#)]
25. Liang, J.; Ban, X.; Yu, K.; Qu, B.; Qiao, K.; Yue, C.; Chen, K.; Tan, K.C. A Survey on Evolutionary Constrained Multi-objective Optimization. *IEEE Trans. Evol. Comput.* **2022**, *27*, 1–20.
26. Zainuddin, F.A.; Abd Samad, M.F.; Tunggal, D. A Review of Crossover Methods and Problem Representation of Genetic Algorithm in Recent Engineering Applications. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 759–769.
27. Srinivas, M.; Patnaik, L. Genetic algorithms: A survey. *Computer* **1994**, *27*, 17–26. [[CrossRef](#)]
28. Hassanat, A.; Almohammadi, K.; Alkafaween, E.; Abunawas, E.; Hammouri, A.; Prasath, V.B.S. Choosing Mutation and Crossover Ratios for Genetic Algorithms—A Review with a New Dynamic Approach. *Information* **2019**, *10*, 390. [[CrossRef](#)]
29. Galeano-Brajones, J.; Luna-Valero, F.; Carmona-Murillo, J.; Cano, P.H.Z.; Valenzuela-Valdés, J.F. Designing problem-specific operators for solving the Cell Switch-Off problem in ultra-dense 5G networks with hybrid MOEAs. *Swarm Evol. Comput.* **2023**, *78*, 1–17. [[CrossRef](#)]
30. Mirjalili, S. Genetic Algorithm. In *Evolutionary Algorithms and Neural Networks. Studies in Computational Intelligence*; Springer: Cham, Switzerland, 2018; Volume 780, pp. 43–55.
31. Higgs, T.; Stantic, B.; Hoque, T.; Sattar, A. Refining Genetic Algorithm twin removal for high-resolution protein structure prediction. In Proceedings of the 2012 IEEE Congress on Evolutionary Computation, Brisbane, QLD, Australia, 10–15 June 2012.
32. Imani, M.; Pakizeh, E.; Saraee, M. Improving genetic algorithm with the help of novel twin removal method. In Proceedings of the Tenth IASTED International Conference on Artificial Intelligence and Applications, Innsbruck, Austria, 15 February 2010.
33. Arabas, J.; Michalewicz, Z.; Mulawka, J. GAVaPS—a genetic algorithm with varying population size. In Proceedings of the First IEEE Conference on Evolutionary Computation. IEEE World Congress on Computational Intelligence, Orlando, FL, USA, 27–29 June 1994.
34. Lobo, F.G.; Lima, C.F. A review of adaptive population sizing schemes in genetic algorithms. In Proceedings of the 7th Annual Workshop on Genetic and Evolutionary Computation (GECCO '05), New York, NY, USA, 25–29 June 2005.
35. Libelli, S.M.; Alba, P. Adaptive mutation in genetic algorithms. *Soft Comput.* **2000**, *4*, 76–80. [[CrossRef](#)]
36. Ribas, P.C.; Yamamoto, L.; Polli, H.L.; Arruda, L.; Neves-Jr, F. A micro-genetic algorithm for multi-objective scheduling of a real world pipeline network. *Eng. Appl. Artif. Intell.* **2013**, *26*, 302–313. [[CrossRef](#)]
37. Zafer, B. Adaptive genetic algorithms applied to dynamic multiobjective problems. *Appl. Soft Comput.* **2007**, *7*, 791–799.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

4

SOLUCIONES TECNOLÓGICAS PARA FACILITAR LA IMPLANTACIÓN PRÁCTICA

Esta sección incluye un artículo en el cual se analizan y describen dos soluciones software desarrolladas en el marco de la tesis haciendo uso del algoritmo genético de optimización multiobjetivo comentado en el apartado anterior. Este software incluye el desarrollo de una librería para ser integrada en software de terceros y también una aplicación gráfica, para su uso directo por parte de aquellas organizaciones que hayan implantado y estén usando el marco de trabajo para la gestión holística de la ciberseguridad en el sector público. Este software facilita la toma de decisiones al permitir definir sobre ella el estado actual de ciberseguridad de los activos de negocio, definir también los objetivos estratégicos de ciberseguridad holística deseados y hacer uso del algoritmo genético previamente desarrollado para identificar uno o varios conjuntos de controles de ciberseguridad que habría que implantar para conseguir dichos objetivos. Esta solución agiliza la elección de dicho conjunto de controles de semanas o meses, dependiendo del caso, a segundos, minimizando los conflictos en los equipos multidisciplinares encargados de diseñar las acciones de ciberseguridad que permiten cumplir con los objetivos estratégicos marcados por la organización o alertando de forma inmediata cuando no exista ninguna combinación factible que permita su consecución.

Este resultado de investigación corresponde al objetivo de la tesis O3, definido en el apartado 1, Objetivos y metodología de investigación.

Referencia: M. Domínguez-Dorado, F. J. Rodríguez-Pérez, J. Galeano-Brajones, J. Calle-Cancho, and D. Cortés-Polo, “*Fleco: A tool to boost the adoption of holistic cybersecurity management*”, *Software Impacts*, volume 19. p. 100614, 2024. <https://doi.org/10.1016/j.simpa.2024.100614>

Factor de impacto de la publicación (JIF) en JCR 2023: 1.3

Categoría: COMPUTER SCIENCE, SOFTWARE ENGINEERING. Ranking JIF: 92/131 (Q3).

Licencia: <http://creativecommons.org/licenses/by/4.0/>

© 2024 Los autores.

Contents lists available at [ScienceDirect](https://www.sciencedirect.com)

Software Impacts

journal homepage: www.journals.elsevier.com/software-impacts

Original software publication

FLECO: A tool to boost the adoption of holistic cybersecurity management

Manuel Domínguez-Dorado ^{a,*}, Francisco J. Rodríguez-Pérez ^b, Jesús Galeano-Brajones ^b,
Jesús Calle-Cancho ^c, David Cortés-Polo ^b

^a Department of Information Systems and Digital Toolkit, Public Business Entity Red.es, 28020 Madrid, Spain

^b Department of Computing and Telematics Systems Engineering, University of Extremadura, 10003 Cáceres, Spain

^c Extremadura Research Center for Advanced Technologies (CETA-CIEMAT), Calle Sola 1, 10200 Trujillo, Spain

ARTICLE INFO

Keywords:

Cybersecurity
FLECO
Functional areas
Holistic approach
Strategic objectives

ABSTRACT

The implementation of a holistic cybersecurity approach involves engaging multiple functional areas within the organization, each assigned specific actions to achieve strategic cybersecurity objectives. These actions – there can be numerous permutations of them – have associated costs, expertise requirements. Selecting the right combinations requires careful analysis and consideration, leading to time-consuming deliberations and potential conflicts. Identifying inadequate combinations that fail to meet strategic goals also requires significant effort. To streamline this process, we developed FLECO (Fast, Lightweight, and Efficient Cybersecurity Optimization), an adaptable multi-objective genetic algorithm that enables near-instantaneous identification of feasible cross-functional combinations. It serves as a foundation for the cybersecurity workforce to reach a consensus.

Code metadata

Current code version	v1.2
Permanent link to code/repository used for this code version	https://github.com/SoftwareImpacts/SIMPAC-2023-502
Permanent link to reproducible capsule	https://codeocean.com/capsule/5432749/tree/v1
Legal code license	GNU Lesser General Public License v3.0 or later (LGPL-3.0-or-later)
Code versioning system used	git
Software code languages, tools and services used	Java 11
Compilation requirements, operating environments and dependencies	OpenJDK 11 or later Maven
If available, link to developer documentation/manual	https://github.com/manolodd/fleco/blob/fleco-1.2/README.md
Support email for questions	fleco@manolodominguez.com

1. Introduction

In response to the current cybersecurity landscape, organizations need a comprehensive approach involving coordination across various functional areas to achieve optimal cybersecurity levels and protect business assets [1] following specific cybersecurity standards. The CyberTOMP framework was designed to orchestrate tactical-operational cybersecurity efforts towards strategic goals, addressing challenges in

reaching a consensus on specific cybersecurity actions from a holistic perspective [2]. Despite its support, the multitude of possible action combinations makes consensus difficult; this is not a unique feature of CyberTOMP, on the contrary, it is common for almost every model based on a fixed set of controls/safeguards from which the cybersecurity team have to agree the ones to be implemented, such as the National Institute of Standards and Technology (NIST) cybersecurity framework [3], the Center for Internet Security (CIS) Critical

The code (and data) in this article has been certified as Reproducible by Code Ocean: (<https://codeocean.com/>). More information on the Reproducibility Badge Initiative is available at <https://www.elsevier.com/physical-sciences-and-engineering/computer-science/journals>.

* Corresponding author.

E-mail addresses: manuel.dominguez@red.es (M. Domínguez-Dorado), fjrodri@unex.es (F.J. Rodríguez-Pérez), jgaleanobra@unex.es (J. Galeano-Brajones), jesusmanuel.calle@ciemat.es (J. Calle-Cancho), dcorpol@unex.es (D. Cortés-Polo).

<https://doi.org/10.1016/j.simpa.2024.100614>

Received 7 December 2023; Accepted 9 January 2024

2665-9638/© 2024 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

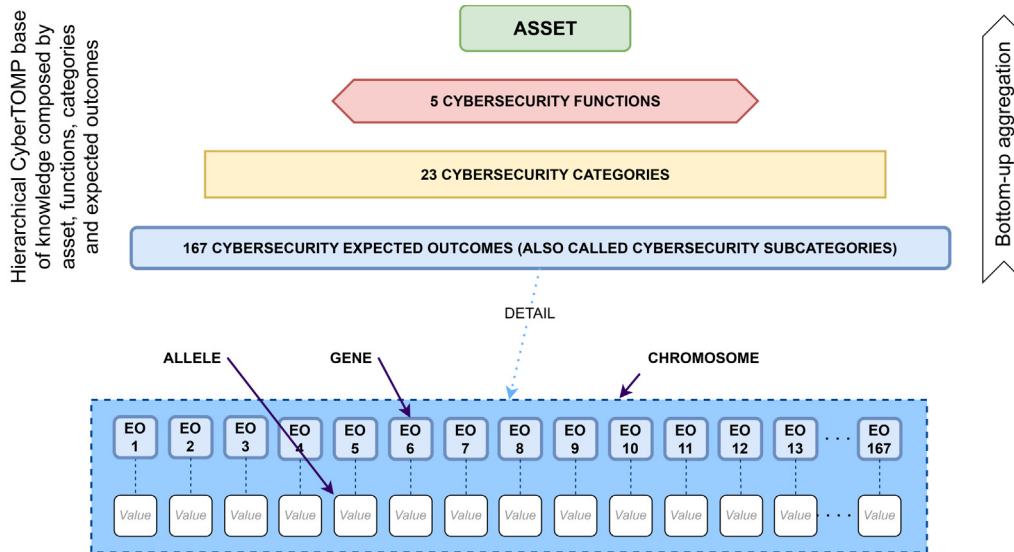


Fig. 1. CyberTOMP framework's hierarchical base of knowledge are translated into genetics concepts. Solutions are then represented as chromosomes composed by genes and alleles and the cybersecurity problem is turned into an optimization one.

Security Controls (CSC) [4], or the CIS Community Defense Model 2.0 (CDM) [5]. This challenge led to the development of FLECO, a constrained, adaptive, multi-objective genetic algorithm that swiftly identifies feasible cybersecurity action combinations; It eliminates the necessity for manually rejecting vast quantities of impractical solutions [6], allowing the cross-functional cybersecurity workforce to focus on cooperation regarding the computed feasible set of cybersecurity actions. Genetic algorithms, known for solving complex optimization problems [7–11], are applied in tactical-operational cybersecurity management for the first time in our development, specifically in the selection of cybersecurity actions for business assets from a holistic perspective. The collaborative development of FLECO involved two organizations, contributing to its fine-tuning and validation through thousands of simulations. These simulations demonstrated FLECO's capability to enhance the implementation of a comprehensive cybersecurity approach within any organization, considering diverse conditions, parameterizations, and strategic cybersecurity goals for various business assets.

In this work, we release FLECO as an open-source tool, providing an opportunity for researchers in cybersecurity management and organizations interested in implementing comprehensive cybersecurity to contribute, enhance, and utilize the tool.

2. Description

The primary function of FLECO is to autonomously identify a set of cybersecurity actions from a vast array of potential combinations. These actions, once implemented by the cross-functional cybersecurity workforce, allow achieving the defined strategic cybersecurity goals. However, manual collaboration among team members has proven challenging in reaching a consensus on these actions. To address this, we developed the FLECO algorithm, released under the GNU Lesser General Public License 3.0 as a Java library and also as a Graphic User Interface (GUI) standalone application [12].

FLECO utilizes optimization techniques, specifically genetic algorithms, to offer its functionalities. It transforms the cybersecurity problem into an optimization challenge, recognizing that the cybersecurity status of a business asset – whether current or desired – can be represented as a set of predefined cybersecurity actions, each with its implementation level. In genetic algorithm terms, this translates to defining the cybersecurity status as a chromosome, each applicable cybersecurity action as a gene, and the implementation level of each

action as an allele. In simplifying matters, FLECO encodes the cybersecurity condition of the evaluated asset in a manner conducive to the application of genetic algorithm techniques. Simultaneously, due to the hierarchical organization of cybersecurity actions in a tree-like structure, various metrics can be formed and acquired at distinct levels (Fig. 1).

FLECO/FLECO Studio software delivers various key functionalities tailored for holistic cybersecurity management. Through parameterization, it adapts seamlessly to diverse needs and use cases with different complexity in both public and private sectors. The system efficiently identifies cybersecurity actions and their deployment levels to achieve strategic goals within seconds, using standard hardware commonly found in office settings. Implementing proportional cybersecurity, the approach clusters potential actions into three groups based on asset criticality, allowing for tailored responses to different asset importance levels. The system employs a multi-objective genetic algorithm, simultaneously maximizing three goals: meeting strategic cybersecurity objectives, maintaining continuity with current actions, and enhancing overall cybersecurity status. FLECO/FLECO Studio provides flexible usage options, serving as a library for integration into existing systems (or executing massive batch test with research purposes), as shown in Fig. 2, or as a standalone GUI application for independent use. With its user-friendly GUI, it enables cross-functional cybersecurity professionals to easily incorporate it into their daily management tasks (Fig. 3). Additionally, the system allows context saving and management, facilitating the continuous development of cybersecurity management activities. In summary, FLECO/FLECO Studio offers an efficient and user-friendly solution for holistic cybersecurity management, empowering organizations to enhance their cybersecurity posture and streamline daily cybersecurity tasks. It also serves as a valuable resource for researchers specializing in the holistic management of tactical-operational cybersecurity.

3. Impact overview

The creation of FLECO addresses a crucial need in the practical application of a holistic cybersecurity management model, particularly at tactical and operational levels, such as the CyberTOMP framework. Holistic management involves collective decision-making on cybersecurity actions in meetings at these levels to achieve strategic objectives. However, this is not an easy process due to the fact that the selected set of actions has impact on economic, effort-related, and company-specific factors and on different functional areas, leading to challenges

```

public class SimpleExample {
    public static void main(String[] args) {
        int initialPopulation = 30;
        int maxSeconds = 5 * 60;
        float crossoverProbability = 0.90f;
        ImplementationGroups IG = ImplementationGroups.IG3;

        Chromosome initialStatus = new Chromosome(IG);
        initialStatus.randomizeGenes();

        StrategicConstraints SCs = new StrategicConstraints(IG);
        SCs.addConstraint(new Constraint(ComparisonOperators.GREATER, 0.65f));
        SCs.addConstraint(Functions.IDENTIFY, new Constraint(ComparisonOperators.GREATER_OR_EQUAL, 0.6f));
        SCs.addConstraint(Categories.RC_CO, new Constraint(ComparisonOperators.LESS, 0.8f));
        SCs.addConstraint(Genes.PR_PT_9D_7, new Constraint(ComparisonOperators.LESS_OR_EQUAL, 0.6f));
        SCs.addConstraint(Genes.ID_BE_ID_BE_3, new Constraint(ComparisonOperators.GREATER_OR_EQUAL, 0.7f));

        FLECO fleco;
        fleco = new FLECO(initialPopulation, maxSeconds, crossoverProbability, IG, initialStatus, SCs);
        fleco.setProgressEventListener(new DefaultProgressEventListener());
        fleco.evolve();
        fleco.getBestChromosome().print();
    }
}

```

Fig. 2. A simple Java snippet to show the basic usage of FLECO in library mode. Additional complete examples are included in the project's source code tree.

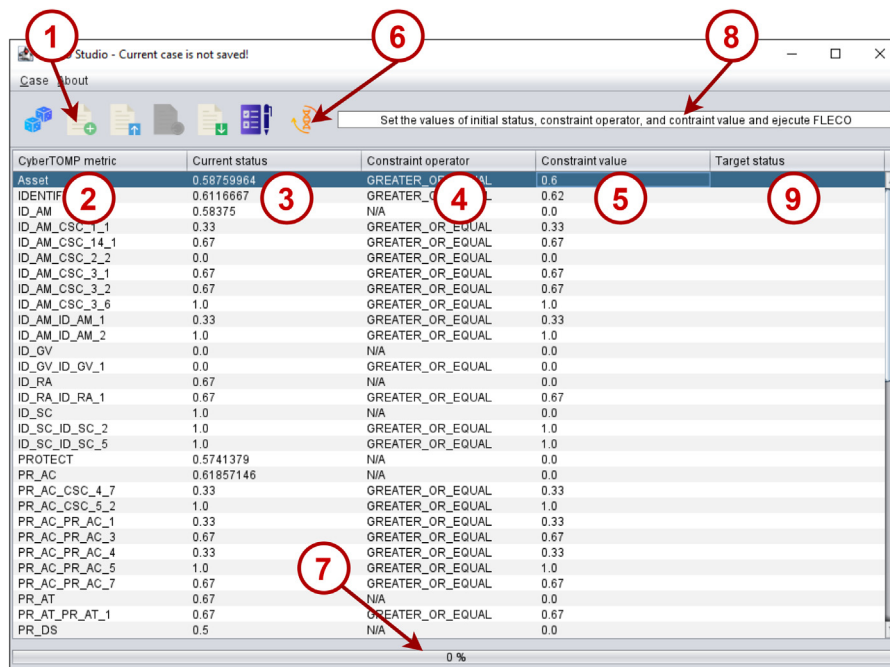


Fig. 3. Basic workflow in FLECO Studio: create a new case (1), read the CyberTOMP metrics (2) and set their current value (3), choose whether apply a constraint/goal to each CyberTOMP metric (4) and set the corresponding value (5). Launch FLECO execution (6) that will progress (7) until the end, making it visible in the message box (8). When computed, FLECO will show the required implementation status for every cybersecurity action (9) in order to fulfil the defined strategic constraints/goals.

for multidisciplinary cybersecurity teams. FLECO, developed and publicly available, offers a solution by facilitating the identification of a comprehensive set of actions, contributing to a more viable and straightforward implementation of holistic tactical-operational cybersecurity. The adaptability of FLECO to models beyond CyberTOMP is straightforward, involving modifications to its knowledge bases.

Within our research endeavours focused on holistic tactical-operational cybersecurity management, FLECO has played a significant role. It has been directly applied to cases, contributing to both the advancement of research in this domain and making an impact in industrial settings for organizations utilizing it. Two instances exemplifying research papers supported by the application of FLECO include:

- A research on a mechanism to drastically improve the selection of cybersecurity actions to enhance the implementation of holistic cybersecurity management, published in [6].

- A research to implement a holistic approach to cybersecurity in the public sector through the outsourcing of a Wide-Scope CyberSOC, published in [13].

In any case, great care was taken during the development of FLECO to ensure that it would be a useful tool not only for the specific companies that participated somehow in its designing, definition or validation, but also for any organization with similar needs.

4. Further development

FLECO is utilized in the day-to-day operations of the multidisciplinary cybersecurity team, whether supported by specialized external personnel or not. However, this diverse team, consisting of individuals from tactical and operational levels, may not always possess the necessary background to comprehend and apply holistic cybersecurity. In our collaborative research with various public and private entities,

an interesting opportunity has been identified. It involves expanding the functionalities of FLECO/FLECO Studio to not only assist the cybersecurity team in deciding the set of cybersecurity actions but also to enhance their situational awareness in cybersecurity [14]. This transformation positions FLECO not just as an optimization tool but also as a cybersecurity training tool.

As a result of this discovery, FLECO Studio is currently undergoing expansion, and an experimental cybersecurity training program is being conducted to validate its benefits. However, it is important to note that this research is still ongoing.

Funding statement

This research was funded in part by TED2021-131699B-I00/ MCIN/AEI/10.13039/501100011033/ and by European Union NextGenerationEU/PRTR. The funding sources had no involvement in study design; in the collection, analysis and interpretation of data; in the writing of the report; and in the decision to submit the article for publication.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

- [1] R. van Kranenburg, G. Le Gars, The cybersecurity aspects of new entities need a cybernetic, holistic perspective, *Int. J. Cyber Forensic Adv. Threat Investig.* 1 (63–68) (2021) 2.
- [2] M. Domínguez-Dorado, J. Carmona-Murillo, D. Cortés-Polo, F.J. Rodríguez-Pérez, CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels, *IEEE Access* 10 (2022) 122454–122485.
- [3] NIST, Framework for Improving Critical Infrastructure Cybersecurity V1.1, National Institute of Standards and Technology, Gaithersburg, 2018.
- [4] CIS, CIS Critical Controls(R). Version 8, Center for Internet Security, New York, 2021.
- [5] Center for Internet Security, CIS Community Defense Model V2.0, CIS, New York, 2021.
- [6] M. Domínguez-Dorado, D. Cortés-Polo, J. Carmona-Murillo, F.J. Rodríguez-Pérez, J. Galeano-Brajones, Fast, lightweight, and efficient cybersecurity optimization for tactical–operational management, *MDPI Appl. Sci.* 13 (6327) (2023).
- [7] L. Jing, B. Xuanxuan, Y. Kunjie, Q. Boyang, Q. Kangjia, Y. Caitong, C. Ke, C.T. Kay, A survey on evolutionary constrained multi-objective optimization, *IEEE Trans. Evol. Comput.* 27 (2) (2022) 202–221.
- [8] A. Alorf, A survey of recently developed metaheuristics and their comparative analysis, *Eng. Appl. Artif. Intell.* 117 (A) (2023) 105622.
- [9] C.K. Lee, A review of applications of genetic algorithms in operations management, *Eng. Appl. Artif. Intell.* 76 (1) (2018) 1–12.
- [10] L.P. Rees, J.K. Deane, T.R. Rakes, W.H. Baker, Decision support for cybersecurity risk planning, *Decis. Support Syst.* 51 (1) (2011) 493–505.
- [11] G. Uuganbayar, A. Yautsiukhin, F. Martinelli, F. Massacci, Optimisation of cyber insurance coverage with selection of cost effective security controls, *Comput. Secur.* 101 (102121) (2021).
- [12] M. Domínguez-Dorado, Manolodd/fleco: fleco-1.2, 2023, <http://dx.doi.org/10.5281/zenodo.8092451>, [Online]. Available.
- [13] M. Domínguez-Dorado, F.J. Rodríguez-Pérez, J. Carmona-Murillo, D. Cortés-Polo, J. Calle-Cancho, Boosting holistic cybersecurity awareness with outsourced wide-scope CyberSOC: A generalization from a spanish public organization study, *MDPI Inf.* 14 (586) (2023) 1–31.
- [14] F. Ulrik, B. Joel, Cyber situational awareness – a systematic review of the literature, *Comput. Secur.* 46 (2014) 18–31.

5

EXTENSIONES METODOLÓGICAS PARA LA CIBERSEGURIDAD DE LA CADENA DE SUMINISTRO

En esta sección se incluye un artículo en el que se abordan las especificidades de las organizaciones públicas que les dificultan, de una forma acentuada particular, la adopción de un modelo de gestión holístico de la ciberseguridad, especialmente en los niveles organizacionales inferiores. En este trabajo en primer lugar se hace una revisión exhaustiva de aquellos aspectos previamente identificados en el modelo de gestión holística de la ciberseguridad explicado en el capítulo 2, pero con un enfoque específico sobre la literatura existente que analice dichos aspectos en el contexto de las organizaciones públicas. En el trabajo se analizan en detalle distintas temáticas como los fundamentos de la ciberseguridad holística, la gestión de la fuerza de trabajo táctico-operativa de la ciberseguridad, el desarrollo, gestión y retención del talento en ciberseguridad, la subcontratación en el sector público o la externalización de servicios de ciberseguridad gestionada o centros de operaciones de ciberseguridad. Posteriormente, el artículo aborda, con la colaboración de una entidad del Sector Público, un análisis de fortalezas y debilidades para la implantación de un modelo de ciberseguridad holística y el diseño de las estrategias asociadas (mediante extensiones metodológicas) para maximizar las posibilidades de éxito en esta implantación. Durante los trabajos, se sigue un proceso estructurado conducente a la generalización de las características de este caso de uso particular a todas las entidades del sector público. Como resultado, se proponen extensiones al modelo propuesto que permiten identificar de forma precisa las habilidades y capacidades necesarias para una ciberseguridad holística efectiva, así como los requisitos exigibles a la cadena de suministros para que pueda contribuir a la ciberseguridad global de la organización. Tanto en la externalización de servicios de centros de operaciones de ciberseguridad, como en la adquisición de capacidades de terceros para el establecimiento de equipos multidisciplinares mixtos público-privados. Y permiten aumentar la concienciación del personal propio respecto a la necesidad de contribución a la ciberseguridad desde su área de conocimiento individual.

Este resultado de investigación corresponde al objetivo de la tesis O4, definido en el apartado 1, Objetivos y metodología de investigación.

Referencia: M. Domínguez-Dorado, F. J. Rodríguez-Pérez, J. Carmona-Murillo, D. Cortés-Polo and J. Calle-Cancho, "*Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study*". *Information*, vol. 14, no. 586, pp. 1-31, 2023. <https://doi.org/10.3390/info14110586>.

Factor de impacto de la publicación (JIF) en JCR 2023: 2.4

Categoría: COMPUTER SCIENCE, INFORMATION SYSTEMS. Ranking JIF: 126/249 (Q3).

Licencia: <https://creativecommons.org/licenses/by/4.0/>

© 2024 Los autores.

Article

Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study

Manuel Domínguez-Dorado ^{1,*} , Francisco J. Rodríguez-Pérez ², Javier Carmona-Murillo ² , David Cortés-Polo ² 
and Jesús Calle-Cancho ³

¹ Department of Domains, Information Systems and Digital Toolkit, Public Business Entity Red.es., 28020 Madrid, Spain

² Department of Computing and Telematics Systems Engineering, University of Extremadura, 10003 Cáceres, Spain

³ Extremadura Research Center for Advanced Technologies (CETA-CIEMAT), 10200 Trujillo, Spain

* Correspondence: manuel.dominguez@red.es; Tel.: +34-747-756-532

Abstract: Public sector organizations are facing an escalating challenge with the increasing volume and complexity of cyberattacks, which disrupt essential public services and jeopardize citizen data and privacy. Effective cybersecurity management has become an urgent necessity. To combat these threats comprehensively, the active involvement of all functional areas is crucial, necessitating a heightened holistic cybersecurity awareness among tactical and operational teams responsible for implementing security measures. Public entities face various challenges in maintaining this awareness, including difficulties in building a skilled cybersecurity workforce, coordinating mixed internal and external teams, and adapting to the outsourcing trend, which includes cybersecurity operations centers (CyberSOCs). Our research began with an extensive literature analysis to expand our insights derived from previous works, followed by a Spanish case study in collaboration with a digitization-focused public organization. The study revealed common features shared by public organizations globally. Collaborating with this public entity, we developed strategies tailored to its characteristics and transferrable to other public organizations. As a result, we propose the “Wide-Scope CyberSOC” as an innovative outsourced solution to enhance holistic awareness among the cross-functional cybersecurity team and facilitate comprehensive cybersecurity adoption within public organizations. We have also documented essential requirements for public entities when contracting Wide-Scope CyberSOC services to ensure alignment with their specific needs, accompanied by a management framework for seamless operation.

Keywords: cyberSOC outsourcing; holistic cybersecurity; public sector cyber-resilience; tactical-operational cybersecurity management; wide-scope cyberSOC



Citation: Domínguez-Dorado, M.; Rodríguez-Pérez, F.J.; Carmona-Murillo, J.; Cortés-Polo, D.; Calle-Cancho, J. Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study. *Information* **2023**, *14*, 586. <https://doi.org/10.3390/info14110586>

Academic Editors: Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 12 September 2023

Revised: 17 October 2023

Accepted: 23 October 2023

Published: 25 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A multitude of definitions exist for the concept of cybersecurity. One of the wider definitions can be located in the work of Domínguez-Dorado et al. [1], which is closely intertwined with the notion of cyberspace. Cyberspace, defined as a network comprising interconnected information systems facilitated by communication networks, serves as the arena where individuals and entities interact and carry out their activities. This environment possesses distinct attributes, including high dynamism, common ground where each organization exercises control over a portion, a substantial reliance on third parties, and a necessity to prioritize not only information, but also the continuity of business processes and assets. Furthermore, it demands a focus on cyber resilience, among other considerations. Within this context, cybersecurity emerges as the discipline entrusted with the responsibility of managing and mitigating the threats, risks, and circumstances originating from this intricate cyberspace. A cyberattack, one of the most common of the mentioned

cyber threats, encompasses any deliberate endeavor aimed at illicitly acquiring, disclosing, modifying, incapacitating, or annihilating data, applications, or other assets by means of unauthorized access to a network, computer system, or digital device. Furthermore, it is worth noting that attackers need not always gain access to any element within the organization's infrastructure. A mere misinformation campaign can suffice to tarnish the organization's reputation and trustworthiness. It is widely recognized that in the 21st Century, cybersecurity must be approached holistically. However, many organizations still struggle to effectively implement this approach due to a lack of alignment with traditional information security standards and practices. While an information security approach permits handling the cybersecurity aspects in many cases, it might be insufficient, alone, to address some of the risks and threats that emerge from cyberspace and for that reason, it is sometimes recommended to adopt a more suitable cybersecurity approach as explained in von Solms and van Niekerk [2], and Reid and van Niekerk [3]. Therefore, achieving true holism and effective cybersecurity in practice remains a challenge for many organizations.

In various instances, the obstacles in achieving holistic cybersecurity deployment stem from issues tied to the cross-functional cybersecurity workforce and their capacity to establish a holistic approach to address the ever-evolving cyber threats landscape. This will be further elucidated in the forthcoming sections. For instance, one of the reasons that public sector organizations often outsource their cybersecurity needs, such as managed cybersecurity services or CyberSOC services, is the difficulty in recruiting and retaining civil servants with the necessary cybersecurity skills as stated in works as Furnell [4], De Zan [5], Reeder and Alan [6], or DeCrosta [7]. This is a problem faced by organizations across the public and private sectors, but it is particularly acute in the public sector for which we recommend the studies of Shava and Hofisi [8], Ngwenyama et al. [9], or Nizich [10], where the high demand and high salaries for cybersecurity professionals in the private sector can make it difficult to attract and retain talent. Additionally, when it comes to externalized CyberSOC contracts, these contracts must be renewed on a periodic basis, which can make it difficult to retain talent even when outsourcing these services. As a result, public sector organizations may struggle to maintain a consistent and effective approach to cybersecurity.

Relying heavily on outsourced services for their operational needs is also an impediment to focusing on a holistic framework, Reh Lee et al. [11]. Public sector entities often have a large number of highly skilled managers at various levels, but the hands-on work is frequently carried out by personnel from outsourced services providers. As a result, tactical-operational teams in these organizations are often composed of a mix of in-house staff and personnel from external service providers. These outsourced services are typically focused on specific areas, such as communications, software development, legal advising, human resources, or facilities management, and are typically only available to the specific area that contracted them. This fragmented approach creates obstacles to achieving holistic cybersecurity. Nevertheless, when a decision has been made to outsource a CyberSOC, this situation can be tapped as the foundation for building a truly holistic approach to cybersecurity, particularly in public sector organizations. To achieve this goal, the CyberSOC should be able to propose cybersecurity actions that can be implemented across the organization to achieve the necessary level of holism. This requires a cross-functional vision, as the nature of cybersecurity is inherently holistic. At the same time, the tactical-operational teams responsible for implementing these cybersecurity measures must be skilled in their respective areas of expertise to effectively design and implement cybersecurity safeguards in the "last mile". Unfortunately, it is often the case that neither the CyberSOC is adequately equipped to prescribe cybersecurity actions across all domains, nor are tactical-operational teams trained to apply their expertise to cybersecurity holistically, Onwibiko and Ouazzane [12].

Taking the aforementioned considerations into account, in this work, we address the enhancement of the organization's cybersecurity workforce capabilities to implement and maintain holistic cybersecurity. Our study commences with the necessity of implementing a model for managing holistic cybersecurity from the lower levels of a Spanish public organization. To attain this objective, we initiated a thorough examination of the existing

literature, aiming to identify aspects highlighted in a prior work [1] and potential requisites for its practical application within the context of public sector. Subsequently, we conducted an in-depth analysis of the participating entity, which agreed to serve as a case study that could be generalized aid similar organizations. In this sense, the participating public entity contributed not only by providing information for analysis at the beginning of the study, but also actively participated in defining the solution presented in this paper. They shared their firsthand expertise and played a crucial role in identifying and addressing early implementation issues, adding substantial value to the research effort. The purpose of this analysis was to confirm the presence of insights we had identified as common during our examination of the existing literature, within the studied public organization. If these insights are indeed present, the same strategies devised for our specific use case should prove advantageous for public sector entities on a broader scale.

As a result of our investigation in cooperation with the participating entity, and in order to couple with the features of public sector organizations, we suggest introducing a new category of outsourced CyberSOC, which we refer to as the Wide-Scope CyberSOC. This innovative CyberSOC not only needs to incorporate a holistic cybersecurity approach into its daily operations, but also must possess the capability to convey this perspective and knowledge to every member of the cross-functional, diverse cybersecurity team, thereby empowering them to actively engage in this collaborative approach. As part of our study, we identify the key elements and requirements that a public organization should demand from the provider offering such a Wide-Scope CyberSOC service. This ensures that it facilitates the improvement of worker capabilities in the context of holistic cybersecurity.

As part of this endeavor, we draw upon existing frameworks and prior knowledge, such as the CyberTOMP framework and previous research on outsourcing and workforce training, among others. By amalgamating these resources with additional components, we streamline the process of implementing comprehensive cybersecurity measures within public organizations.

The remainder of this document is organized as follows: In Section 2, a review of research relevant for our proposal are carried out. Section 3 provides a detailed description of the methodology and steps employed in our study, including a literature review as an expanded and detailed version of the introduction. Section 4 presents the key findings obtained throughout the research and Section 5 summarizes the most significant conclusions of our study and presents the future lines of work that arise from it.

2. Analysis of the State of the Art

Starting at this juncture, we initiated an analysis of the existing literature. Our aim was to select relevant works that could facilitate an expansion of our knowledge, particularly regarding insights derived from one of our prior studies [1]. Additionally, we sought to identify any unique requirements or specific needs that might surface when applying the aforementioned work to a public sector organization. At this stage, our primary objective was to pinpoint common features, requirements, or needs that were shared by public organizations on a global scale. Table 1 provides a comprehensive overview of the collection of works we analyzed. However, a detailed contextualization of these works is provided in the subsequent paragraphs.

In recent decades, there has been a growing consensus regarding the meaning of cybersecurity and how it differs from previous approaches such as technology security and information security, represented by the works of Schatz et al. [2,13]. Cybersecurity emerges from the concept of cyberspace, which is a network of interconnected information services that allows people and organizations to conduct their activities and businesses beyond the physical boundaries of traditional organizations. As a result, much of the ecosystem in which organizations operate falls outside of their control, and the dependence of business activities on this “uncontrolled” part has increased over time. This new environment gives rise to new threats, risks, and countermeasures that must be properly addressed; Ghelani addresses this problem in [14].

Table 1. Studies examined to ascertain whether the identified characteristics could be extrapolated to the entire Public Sector.

Topic	Analyzed Source
Holistic cybersecurity foundations and cybersecurity context in public sector	[2,3,13,15–34]
Tactical-operational cybersecurity workforce management	[1,35–47]
Cybersecurity talent development and retention	[4–10,48–66]
Outsourcing in public sector	[11,67–88]
Outsourcing CyberSOC services	[89–95]

Slowly but surely, organizations are beginning to adopt practical approaches to cybersecurity management. However, these efforts are often limited to the strategic level and rely on information security standards rather than specific cybersecurity frameworks, as analyzed by Sulistyowati et al. in [15]. There has been relatively little progress in applying cybersecurity management to lower levels, which are crucial for achieving effective cybersecurity.

The situation in the public sector is even more challenging. Private companies are often early adopters of new technologies and approaches, while public sector organizations are typically slower to adopt these innovations due to a variety of constraints such as regulatory frameworks, contracting timeframes, hiring restrictions, career development opportunities, and excessive bureaucracy; Srinivas et al. goes deep in this topic in [16]. As a result, public sector entities may struggle to adapt nimbly to changes in the cybersecurity landscape. In many cases, they resort to outsourcing services in order to alleviate these challenges.

2.1. The Importance of a Holistic Approach to Cybersecurity

Cybersecurity differs from previous approaches in several ways, with the main differences stemming from the emergence of a new environment: the cyberspace. As a critical component in every digitized organization, cyberspace poses unique challenges since organizations cannot have complete control over it but have near complete dependency. As mentioned in the introduction “*a mere misinformation campaign can suffice to tarnish the organization’s reputation and trustworthiness*”. The threats and risks that emerge from this environment require unity of action and a broader holistic approach as studied in Ahmed et al. [17], and while some research has been conducted in this area as described by Atoum et al. in [18], much more work remains to achieve an acceptable level of holism, something that is covered by Kranenburg and Le Gars [19], and to cover those specific threats emanating from cyberspace for which an information security approach does not fit well. Recent studies also suggest the need to extend this holism not only within the organization itself, but also to its network of collaborators, civil organizations, government entities, and citizens, in order to provide the necessary unity of action to effectively respond to threats and risks, as investigated in [20] by Del-Real and Díaz-Fernández.

In order to effectively respond to risks and threats emanating from cyberspace, a holistic approach to cybersecurity must involve all functional areas of the organization. This requires a cross-functional approach that considers the unique perspectives and challenges of each area in order to develop comprehensive and effective cybersecurity strategies and, of course, it requires that the involved cross-functional cybersecurity workforce poses a high level of awareness regarding their potential contribution to the overall cybersecurity. Moreover, holism should not be a merely theoretical concept but had better instead to focus on practical implementation. While there have been some advances in achieving this holism in practice, most of these efforts have focused on the strategic level, with less attention given to bringing holism down to the tactical and operational levels of the organization. It is at these lower levels that the necessary safeguards for effective cybersecurity are implemented, though, and thus, it is essential to address the obstacles that prevent organizations from achieving true holism in their tactical-operational approach to cybersecurity.

2.2. Tactical-Operational Cybersecurity Workforce Management

There are several works that address cybersecurity management from different points of view: Rothrock et al. examine it from the board of director's perspective in [45]; the municipalities' points of view are reviewed by Preis and Susskind in [41]; the work by Limba et al. in [46] is centered in critical infrastructures; Yigit et al. focus on the assessment of cybersecurity capabilities in [37]; Rajan et al. focused on cross-functional collaboration in [38]; etc. All of these are very useful studies that have made possible several advances in cybersecurity. However, none of them are comprehensive models that can be used within an organization to handle cybersecurity at tactical and operational levels with a managerial approach. From our perspective, holism can only be achieved by designing and applying managerial techniques not only to lower levels, but also from lower levels, from those who must cooperate in the short and medium term to execute and design cybersecurity safeguards in the last mile, as considered by Axon et al. in [39].

While there are a few existing works that address holism at different levels, including the tactical and operational levels, there is still a need for further research and development in this area in order to effectively manage cybersecurity at these levels.

In [40], a work by Antunes et al., a good analysis is carried out after a practical implementation of an information security and a cybersecurity program in small and medium-size enterprises (SMEs) in Portugal. It takes into account the required controls and their degree of implementation, and profiles SMEs to apply proportional security measures. However, it does not provide details on the coordination mechanism for the multidisciplinary cybersecurity workforce and is based on the ISO 27001 standard for information security rather than cybersecurity. The authors themselves recognize this as a limitation. This analysis focuses on characterizing the participating SMEs in order to align the various safeguards with their specific needs.

The work developed by Domínguez-Dorado et al. in [1] proposed a more comprehensive set of procedural elements that explicitly enable cybersecurity management at the tactical and operational levels is defined as CyberTOMP framework. It is based on the most important cybersecurity frameworks and initiatives, and its authors have created a unified list of potential cybersecurity actions. These actions, also called "expected outcomes", are clustered into three implementation groups that can be applied to business assets with different cybersecurity needs, making it easier to select the appropriate cybersecurity controls, a selection of controls mechanism that is also covered by Breier and Hudec in [47].

While this framework is designed specifically for managing cybersecurity at the tactical and operational levels, it also allows for alignment with strategic cybersecurity goals through the use of the business impact analysis, that, according to Quinn et al. in [36], is a good tool to inform risk prioritization, and the cybersecurity master plan as hooks, which allows unifying cybersecurity and business continuity in a single framework, something described in [43] by Phillips and Tanner. This approach allows organizations to maintain a focus on their overall cybersecurity objectives while also addressing the specific challenges and needs at the tactical and operational levels and this allows the framework to be independent of the strategic standard chosen by the organization, while still providing complementary support. The study of Domínguez-Dorado et al. in [1] follows a practical approach and provides step-by-step processes, procedures, and guidance for identifying cybersecurity actions through a collaborative process that engages all functional areas of the organization. It is additionally supported by tools that facilitate the attainment of agreements on the necessary set of cybersecurity actions [35]. This approach allows for the development of holistic cybersecurity actions that are agreed upon and assigned to the functional areas involved in cybersecurity. The focus of this framework on business assets, which are understood as manageable and understandable units of cybersecurity, is a growing trend in the field as can be extracted from the works of Clark et al. [42] and Kure and Islam [44].

Nonetheless, although this framework provides a useful approach for managing cybersecurity at the tactical and operational levels, there is room to improve. For instance,

it can be enhanced to identify the skills and training required by different functional areas of the organization in order to effectively carry out their cybersecurity tasks. Without the necessary skills and training, it is difficult for organizations to fully implement this framework and achieve the desired results.

Summarizing, to ensure the effectiveness of tactical and operational cybersecurity management, it is essential to develop mechanisms that can provide the necessary capabilities and expertise at these levels. This can be achieved through training programs, hiring qualified personnel, and implementing systems and processes that support the effective management of cybersecurity at the tactical and operational levels, or it can be achieved by acquiring this knowledge from specialized third parties. By taking these steps, organizations can better prepare themselves to effectively manage cybersecurity risks and threats and ensure that their overall cybersecurity efforts are successful.

2.3. Cybersecurity Talent Development and Retention

The development and retention of cybersecurity talent is a pressing issue in today's world. The rapid expansion of the cyberspace and the growing dependence of organizations on it have led to a shortage of cybersecurity professionals. The pandemic of COVID-19 has exacerbated this situation, as organizations have had to provide remote access and services to their employees, making them more vulnerable to cyber-attacks. This has motivated an increased demand for cybersecurity specialists, as organizations strive to protect themselves against these threats.

The shortage of cybersecurity talent has an indirect effect on organizations: in high-demand conditions, organizations are less able to retain cybersecurity-skilled personnel because many companies are competing for the same talent.

Training the existing workforce is an option, but it comes with the risk of losing skilled personnel due to the high demand for cybersecurity professionals. Despite this, providing training to the existing workforce can be beneficial in the short term, as it allows organizations to develop the skills of their employees and improve their ability to manage cybersecurity risks and threats. However, it is important for organizations to carefully consider their training strategies, as they need to ensure that they can retain their trained personnel in the long term. It is likely that more educated, motivated, and well-paid public employees will be easier for organizations to retain, as identified by Dahlstöm et al. [64].

There is an increasing number of research works that address this situation from different perspectives; for instance, in [4], the authors present evidence of the cybersecurity workforce shortage and the different forms of qualification that are available to meet the needs. The work presented in [5] shows that this shortage is due in part to the high demand for cybersecurity specialists, as well as the limited availability of relevant training programs and qualifications. In response to this problem, some public organizations have turned to national skills competitions to create interest in cybersecurity and attract qualified personnel. In a work by Ahmad et al. [62], the authors propose to use incident management as a way to improve organizational learning in cybersecurity topics. This approach focuses on using real-life incidents to provide practical experience and training for cybersecurity personnel, with the aim of increasing their knowledge and expertise. The research carried out in [56] by Ahmad et al. highlights the need for interdisciplinary cybersecurity education and proposes a curriculum roadmap that integrates cybersecurity across technical and non-technical curricula. This approach seeks to address the current shortage of cybersecurity talent by providing a more comprehensive education on the subject. The research presented in [6] proposes three promising approaches to identify, recruit, and develop cybersecurity talent from both technical and non-technical personnel. These approaches aim to address the shortage of skilled cybersecurity professionals and improve organizations' ability to retain their talent. In [57], Chowdhury and Gkioulos identify cybersecurity training offerings for critical infrastructure protection and the key performance indicators that allow evaluating their effectiveness. In research by Noche [58], a comprehensive review of empirical studies aimed at developing the cybersecurity workforce is presented. Gamification

is proposed as a method to improve the cybersecurity training of individuals responsible for protecting critical infrastructure in [54] by Ashley et al. In [60], a study by Kävrestad and Nohlberg, a review of evaluation strategies for cybersecurity training is presented with the aim of minimizing the impact of human factors on cyberattacks. In an investigation by Hulatt and Stavrou [59], the authors present the need for a multidisciplinary cybersecurity workforce that includes professionals from various backgrounds beyond traditional ones such as computing and Information Technology (IT). The authors of [55], Justice et al., analyze the future needs of the cybersecurity workforce. In [61], Maurer et al. identify the specific cybersecurity and professional skills required by those responsible for cybersecurity. These skills are necessary to ensure the effectiveness of tactical and operational cybersecurity management. Finally, in [7], the study analyses the quantitative and qualitative factors that contribute to the current shortage of cybersecurity professionals.

Overall, the shortage of cybersecurity talent is a growing concern for organizations, as it reduces their ability to effectively manage cybersecurity risks and protect against potential threats. This shortage is particularly acute at the tactical and operational levels, where hands-on skills are essential. Intense competition for skilled personnel has made it difficult for organizations to attract and retain the talent they need, leading to further declines in their ability to manage cybersecurity effectively. In order to address this issue, organizations must develop effective strategies to attract and retain cybersecurity talent, particularly at the tactical and operational levels. This will require a comprehensive approach that includes training programs, hiring qualified personnel, and implementing systems and processes that support effective cybersecurity management.

2.4. Outsourcing in Public Sector

There are various forms of potential collaboration in public service delivery, as Kekez et al. analyze in [85], with outsourcing being one of the most common. The decision to outsource is often driven by a desire to reduce costs, as investigated by Santos and Fontana in [71] and improve efficiency. By transferring certain business processes or functions to an external provider, a company can benefit from their expertise and specialized capabilities. Additionally, outsourcing can provide access to a global talent pool, allowing companies to tap into a wider range of skills and knowledge. In addition to cost savings and access to specialized skills, outsourcing can also help a business to focus on its core competencies and drive growth. As such, this is a strategy that is often considered by public organizations looking to streamline their operations and improve their public services.

Although there are some differences between public and private outsourcing, which is explored in [87] by Burnes and Anastasiadis, the motivations for outsourcing are similar across both public and private sectors, with cost control and reduction, focus on core capabilities, and access to supplier expertise and technologies being among the key drivers as supported by works carried out by Marco-Simó and Pastor-Collado [74] or Bogoviz et al. [77], but also to face exceptional situations like the pandemic of COVID-19 as analyzed in [75] by van der Wal. Public organizations are generally well-equipped with individuals who have the necessary skills and expertise to manage tasks and processes effectively. However, they frequently face challenges when it comes to staffing the most technical and operational tasks, which require specialized knowledge and expertise. As a result, these organizations may struggle to effectively perform these tasks, leading to reduced efficiency and performance.

In order to overcome these challenges, many public organizations turn their strategic plans to outsourcing through public-private contracts, as examined in Pavelko et al. [70]. These contracts provide a legal framework for defining the roles and responsibilities of each party, as well as the terms of the relationship between the public and private sectors. They also help to ensure that the activities and services provided under the contract are organized and carried out in a manner that is consistent with the parties' respective rights and obligations, something studied in the research of Bloomfield et al. [78]. The accurate definition of service requirements within these contracts is a key factor for Proscovia in [79] to successful outsourcing, which will later depend on managing the outsourcing

relationship well after the decision is made, which is evaluated in [69] by Heikkilä and Cordon. The lack of service requirements definitions when outsourcing in public sector led to a falling quality of the provided public services.

Outsourcing is a controversial topic. There are many interesting works that discuss the pros and cons of outsourcing in the public sector under different circumstances such as those carried out by Tayauova, Lobao et al., Aswini, Sánchez, Rizwan and Bhatti, Johansson and Siverbo, and Andersson et al. in [76,81–83,86,88] or [80], respectively, among others. Although this debate is outside the scope of our study, we mention them here to highlight the significance of the outsourcing approach for public sector entities.

While outsourcing can have a slight negative effect on the performance and perception of in-house employees [11], it is often necessary in order to ensure that tactical-operational teams have the necessary skills and expertise. But as a result of outsourcing, tactical-operational teams in the public sector are often composed of a mix of public sector employees and outsourced or insourced personnel.

It is also important to note that by outsourcing any service, the outsourcing organization is expanding its supply chain, which can lead to additional risks, including in the realm of cybersecurity. Some of these topics are covered in Nasrulddin et al. [72] and Repetto et al. [73].

2.5. Outsourcing CyberSOC Services

A CyberSOC, is a specialized unit that is focused on monitoring, detecting, and responding to cyber threats in real time. Among the main duties of a CyberSOC the following are included, as determined in Saraiva and Mateus-Coelho [90]:

- Continuous monitoring of an organization's networks and systems for signs of potential cyber threats;
- Detection of cyber threats through the use of advanced technology and analysis of security data;
- Response to detected threats, including implementing countermeasures to prevent or mitigate the impact of the threat;
- Communication with relevant stakeholders, such as the organization's leadership and other security teams, about detected threats and response efforts;
- Ongoing analysis of security data to identify patterns and trends that can help improve the organization's overall security posture.

In addition to these core duties, a CyberSOC may also be responsible for providing training and education to the organization's staff on cybersecurity best practices, as well as collaborating with other security teams and external partners to share information and coordinate efforts to defend against cyber threats. Overall, the role of a CyberSOC is essential in helping organizations protect themselves from the constantly evolving threat landscape of the digital world, as analyzed in [91] by Shutock and Dietrich, and assess their readiness level, something evaluated in [92] by Georgiadou et al.

From our perspective, this set of capabilities and responsibilities, especially the non-core ones, can be tapped by the organization to turn the CyberSOC into the cornerstone over which develop real holistic cybersecurity. Although in public administration, where outsourcing is something very common, this possibility cannot be extrapolated directly, due to the existence of cross-functional tactical and operational teams composed by employees and outsourced workforce.

From a cybersecurity perspective, the presence of mixed multidisciplinary in-house/outsourced tactical and operational teams, which experience high levels of turnover every few years, is not necessarily a problem, but it does present a challenging situation that must be managed carefully in order to ensure effective holistic cybersecurity across the organization.

The above could be even more challenging if the CyberSOC service itself is outsourced, which is also a common practice in public sector and involves roles with high cybersecurity skills, as questioned in Nugraha [94]. Although outsourcing also has advantages, as mentioned in previous paragraphs, the cons are relevant in this case, according to Ti Dun et al. [93], and several efforts have to be made to enhance the communication

between the public entity's manager and the provider of CyberSOC services, which is analyzed in [95] by Kokulu et al. In view of the above, we are of the opinion that one potential disadvantage of outsourcing a CyberSOC is the loss of control over the security of the organization's systems and data. When a CyberSOC is managed by an external provider, the organization loses the ability to directly oversee and manage the security measures in place to protect its systems and data. This can make it difficult to ensure that the necessary security protocols are being followed and can increase the risk of security breaches or other incidents. Another disadvantage is the potential for reduced flexibility and responsiveness. When a CyberSOC is outsourced, the organization is reliant on the external provider for the timely detection and response to security threats. If the provider is unable to respond quickly or effectively, this can leave the organization vulnerable to security breaches or other incidents. Lastly, assigning an outsourced CyberSOC to prescribe cybersecurity tasks for all of the organization's functional areas that are also partially outsourced can lead to conflicts and a lack of coordination between service providers. This can potentially be challenging to resolve and can impact the organization's cybersecurity strategy.

As previously mentioned, there are several situations in which public sector organizations may need to outsource their CyberSOC services. In order for these outsourced CyberSOCs to be able to provide cybersecurity recommendations for all of the organization's functional areas and support their implementation, the outsourcing public entity must put in some effort upfront to identify the necessary capabilities of the CyberSOC and include them as requirements in the related technical specifications. However, these public organizations are often outsourcing their CyberSOC services due to a lack of knowledge and skills, making it difficult for them to identify the necessary requirements. It is necessary to simplify this process in order to ensure that the requirements for the service provider of an outsourced CyberSOC align with the needs of the public organization to develop effective, comprehensive cybersecurity.

2.6. Insights after Reviewing the State of the Art

After conducting a thorough review to identify the unique circumstances and issues that prevent the achievement of effective, comprehensive cybersecurity in public sector organizations, we found that:

- The role of tactical-operational cross-functional teams in cybersecurity management is crucial, as they are responsible for implementing the actual cybersecurity countermeasures within the organization and provide the corresponding holism. There is a dearth of research studies that examine this specific niche from a managerial standpoint, thereby creating a void that hampers the implementation of a comprehensive cybersecurity management approach. It is imperative that such an approach be undertaken at these levels to prevent the formation of isolated units, both within the public and private sectors;
- Currently, there is a shortage of cybersecurity professionals that is expected to continue in the short and medium term. This shortage is particularly acute in public sector organizations, which often have personnel capable of managing at all levels but lack technical staff with hands-on expertise. Therefore, it is imperative to undertake certain actions aimed at raising awareness among the cross-functional cybersecurity workforce regarding the implications of their specific areas of expertise in the broader realm of cybersecurity. This will enable them to become personnel who possess the necessary expertise and managerial acumen to effectively confront the prevailing cyber threats;
- Public sector entities heavily rely on the practice of outsourcing. One of the reasons for that is to gain access to technical staff with hands-on expertise, trying to avoid the mentioned workforce shortage. As a result, their cross-functional tactical-operational teams are often composed of a mix of employees and outsourced workers, which are frequently replaced as their outsourcing contracts come to an end. It is common for public organizations to also outsource CyberSOC services. Although outsourcing appears to be a necessary step in many instances, it is crucial that it is executed in a manner that ensures the service provider aligns with the cybersecurity requirements

of the business. Specifically, it must be capable of facilitating the implementation of a comprehensive tactical-operational cybersecurity management approach.

3. Method

The present research is driven by the real need of a public sector entity, at its own initiative, to undertake an ambitious program to implement a tactical-operational management model for cybersecurity, providing the required holism to tackle current cyber threats. The mentioned organization is a Spanish public organization, which is involved in promoting technology in all spheres of society. It employs approximately 300 individuals and comprises five departments along with sixteen primary functional areas. Exploiting this need and in mutual agreement with the involved organization, we conducted a research project aimed at providing a series of valuable contributions not only to that organization, but also to other public entities with similar needs.

We undertook the research employing a business analysis methodology, evaluating the capacities of the public entity to effectively implement a comprehensive tactical-operational cybersecurity management approach, which holds the potential to foster a substantial transformation in the cybersecurity culture. Our study was divided into four phases grouped in two stages:

- Stage 1. Pre-study of public sector requirements and context
 - Phase 1. In this phase, after a systematic analysis of the existing literature was carried out, the corresponding insights were analyzed and organized to detect whether the features, requirements, and impediments to deploy a truly holistic cybersecurity management model are shared by different public sector organizations worldwide; this phase corresponds to the work described in Section 2.
 - Phase 2. During this phase, a series of meetings were conducted with the participating organization to discuss the prerequisites for implementing a comprehensive cybersecurity management model. These discussions aimed to enable the organization to assess challenges and barriers that could impede the adoption of such a model. Additionally, the organization shared anonymously, and whenever possible, information about other public entities it is related to, which allowed gathering relevant insight both directly and indirectly. This phase focused on determining the organization's capability to fulfill the model's requirements and identify potential obstacles. Continuing with our work, the information retrieved in the mentioned meetings was channelized using the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis technique described by Benzaghta et al. in [96] to analyze deeply and systematically the current circumstances of the participating public entity. We also determine at this point whether the resulting insights coincide with the common features identified for public organizations in a wider context.
 - Phase 3. At this stage, we identified a specific set of actionable strategies that we understood as universally applicable to all public sector entities due the fact that they share common root characteristics as determined in Phase 1 and Phase 2. These strategies were aimed at the successful implementation of a comprehensive tactical-operational cybersecurity management model. This model takes into consideration the distinctive attributes of the public organizations identified in the previous phase and we use the Threats, Opportunities, Weaknesses, and Strengths (TOWS) matrix technique, described in Pasaribu et al. [97], to analyze the external opportunities and threats and compare them to the organization's strengths and weaknesses, resulting in a set of actionable strategies. The combined use of SWOT-TOWS analysis is common to analyze and interpret systems, especially to develop strategies; the work of Hattangadi in [98] analyzes them together.
- Stage 2. Model development.
 - Phase 4. Finally, we carried out our proposal to develop the identified strategies, that would allow public entities to seamlessly adopt a holistic management model

of cybersecurity, taking into account and incorporating the previously identified peculiarities and facing the existing specific challenges of public entities. Throughout the duration of this phase, the research team benefited from the active engagement of the participating public entity. Their involvement enriched the solutions devised by providing insights from the perspective of the recipient institution.

3.1. Stage 1: Pre-Study of Public Sector Requirements and Context

During this stage, encompassing all tasks within phases 1, 2, and 3, we conducted a comprehensive preliminary study to systematically analyze the context surrounding public sector entities. This analysis extended to the international perspective through a state-of-the-art review and to our specific Spanish case study. The overarching objective at this stage was to acquire an in-depth understanding of the requirements and characteristics unique to public sector organizations, enabling them to effectively address the challenges faced by the cross-functional cybersecurity workforce in implementing holistic cybersecurity. Armed with this knowledge, we aimed to identify the most advantageous strategies for any model seeking to address these challenges and seamlessly integrate with public sector entities. We leveraged these identified strategies in the subsequent development of our proposal.

In phase 2, several meetings were held with the participating organization, aimed at discussing the requirements that need to be met to implement a holistic cybersecurity management model. The main purpose of these meetings was to analyze its specific context, gathering relevant information about its strengths and weaknesses, as well as the existing opportunities and threats in relation to the implementation of a holistic cybersecurity model. Moreover, throughout the entire process, the participating organization provided anonymous information concerning other similar public entities with which it had relationships, pertaining to the same aspects being analyzed in its case. As a result, the study incorporates direct information provided by the organization itself, as well as secondary information concerning third parties, provided by the organization but in an indirect way, thus necessitating a more in-depth subsequent analysis. Based on these, and with the gathered information, a SWOT analysis was conducted, which succinctly represented the characteristics of the organization and its starting conditions to address the process of deploying a holistic model that enables the enhancement of its cybersecurity (Table 2).

Table 2. SWOT analysis based on the information provided by the participating entity regarding its own strengths, weaknesses, opportunities, and threats, as well as those of third-party public entities.

		Strengths	Weakness
Internal		<ul style="list-style-type: none"> • Their personnel are highly skilled as managers; • Have much experience in outsourcing processes and can contract the required skilled service providers if needed; <ul style="list-style-type: none"> • Can provide long term stable employment; • They are not necessarily under the pressure of a profit goal but driven by the vocation of public utility. 	<ul style="list-style-type: none"> • Have difficulty to retain and develop the career of cybersecurity personnel; <ul style="list-style-type: none"> • Lack of personnel skilled in hands-on tasks; • Their teams are often composed by in-house and outsourced personnel; • They are silo-based organizations where cross-domain collaboration is difficult.
		Opportunities	Threats
External		<ul style="list-style-type: none"> • There is an increasing interest that public organizations enhance their cybersecurity capabilities; • Can partner with private sector organizations to leverage their expertise and technology to improve cybersecurity; • Those public organizations able to offer cyber-resilient services will be more valued; • More funding is available for public organization to modernize in terms of cybersecurity. 	<ul style="list-style-type: none"> • Private sector can attract potential employees more effectively; • Regulations hinder to contract the same service providers continuously; • The number of cyber criminals seeking to target public sector organizations is increasing; • Cyber threats are constantly evolving, and the public sector may struggle to keep up with the latest threats and technologies. This can lead to a reactive approach to cybersecurity rather than a proactive one.
		Positive	Negative

From this phase, we obtained a comprehensive understanding of the organization's potential to implement the intended model. The positive aspects can be summarized as a high capacity for management and expertise in outsourcing, coupled with a growing interest and allocation of budget towards enhancing cybersecurity in the public sector. The negative aspects primarily revolve around the public entity's challenges in developing and retaining technical cybersecurity talent, as well as difficulties in adapting to highly dynamic changes or implementing a collaborative internal working system.

In conclusion of this stage, we have come to the realization that the common characteristics we found in the analysis of the state of the art are also present in the participating entity and the rest of entities we analyzed indirectly. Extensive literature exists that describes similar circumstances in public organizations worldwide. Henceforth, we possessed sufficient confidence to perceive this situation as a widespread phenomenon within public sector organizations aspiring to implement a comprehensive tactical-operational cybersecurity management approach. At this point in our study, we had gathered sufficient evidence to suggest that the participating organization exhibited similar characteristics to other public entities worldwide in terms of their potential to implement a holistic cybersecurity management model. This encouraged us to believe that the solution we were developing for the participating entity could also be beneficial to other organizations with similar profiles.

Finally, in the third phase, we employed the prior analysis as an input to a TOWS matrix with the objective of translating the insights from Phase 1 and Phase 2 into actionable strategies. The resulting strategies were:

- Strengths and Opportunities (SO) strategies, commonly referred to as the "Maxi-Maxi Strategy", encompass the utilization of strengths to optimize opportunities. In a TOWS analysis, this type of strategy is considered highly proactive and has a higher likelihood of yielding success. In our case, the public organization could leverage its expertise, skills, and capabilities in public procurement and outsourcing to effectively utilize the available funding. By establishing public-private contracts, the organization can transform itself into a resilient entity in the field of cybersecurity and provide better and more secure public services;
- Strengths and Threats (ST) strategies, commonly referred to as the "Maxi-Mini Strategy", involve leveraging strengths to mitigate threats. In our study, by leveraging the growing allocation of funds for cybersecurity enhancements and the heightened focus on modernizing and fortifying public entities and services, the public organization can seize the opportunity to engage public sector companies. This strategic move aims to facilitate the organization's adaptation to the dynamic, challenging, and rapidly evolving contexts of cybersecurity and cyber threats;
- Weakness and Opportunities (WO) strategies, commonly referred to as the "Mini-Maxi Strategy", encompass the approach of minimizing weaknesses by capitalizing on available opportunities. In our work, the growing allocation of funds for cybersecurity enhancements, coupled with the heightened emphasis on modernizing and fortifying public entities and services, presents an opportunity for the public organization to utilize outsourced personnel, augment the cybersecurity skills and career progression of its existing employees, and establish methodological foundations to foster true holism;
- Weaknesses and Threats (WT) strategies, also recognized as the "Mini-Mini Strategy", are employed to minimize weaknesses and evade threats. Within a TOWS analysis, this type of strategy is considered highly reactive/defensive and may not be as reliable in generating success. Due to this rationale, this strategy is not deemed conducive to steering the advancement of our proposal.

In summary, our objective in this research was to find a mechanism that would facilitate the development of the described strategies, namely, the SO, ST, and WO strategies. Essentially, this mechanism should be based on the outsourcing of services, leveraging existing resources and the interest in cybersecurity within the context of public sector entities. Its purpose would be to enhance the cybersecurity skills of various functional areas within the organization, improve its talent retention capabilities, implement a holistic

model, and establish a cybersecurity management context that seamlessly orchestrates all these elements.

3.2. Stage 2: Model Development

The second stage of our research began with the inputs from stage 1, namely, the strategies required for a model aiming to address the challenges of deploying holistic cybersecurity by the cross-functional cybersecurity workforce in public sector organizations. In this specific context, the strategies previously defined were adjusted to accommodate the unique characteristics of public entities, ensuring that the resulting model would be well-suited to their needs.

Throughout Phase 4, we formulated our proposal to execute the strategies delineated in the preceding stage. Following thorough deliberations, we made the strategic choice to harness the outsourcing capabilities of public sector entities and establish a novel type of outsourced CyberSOC. This strategic decision was aimed at bolstering the cybersecurity proficiency of the cross-functional workforce while aligning with the specific contextual considerations, strengths, and weaknesses unique to public sector organizations. The outcome of this phase, as detailed in the following sections, are the results of our research: a novel concept called the “Wide-Scope CyberSOC” along with the essential documentation and procedural elements for its easy and efficient implementation within public sector organizations.

As mentioned, our proposal involves the utilization of an outsourced CyberSOC service, equipped with specialized capabilities that serve as the foundation for fostering a holistic approach to cybersecurity management within the organization. We designated this novel CyberSOC type as “Wide-Scope CyberSOC”.

In order to materialize this Wide-Scope CyberSOC, we deemed it imperative to consider several pivotal aspects, as depicted in Figure 1:

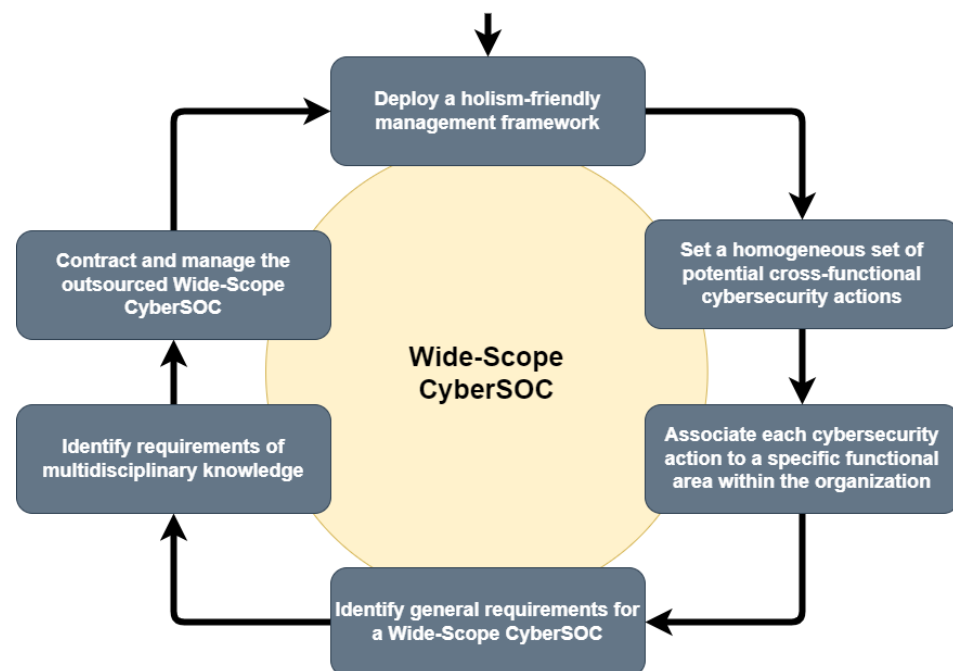


Figure 1. Key aspects to be taken into consideration to seamlessly integrate a Wide-Scope CyberSOC into the organization, enabling a holistic management of cybersecurity.

- The establishment of a cybersecurity management framework that can deliver the necessary holism at lower organizational levels is imperative. Contracting a Wide-Scope CyberSOC to assist the organization in overcoming silos and adopting a holistic approach would be futile if the procedural foundations to support such an extended CyberSOC have not been put in place. Consequently, based on the reasons outlined in Section 2.2, we opted for the CyberTOMP framework.

- Since the Wide-Scope CyberSOC is intended to provide guidance and assistance in designing and implementing multidisciplinary cybersecurity measures, it is essential to pre-identify the potential set of such cybersecurity actions. This enables us to contractually demand support for each of these actions. As our proposal is based on CyberTOMP, this set of actions is already identified within this framework. The Unified List of Expected Outcomes (ULEO) of CyberTOMP (Table 3) precisely represents a compilation of potential cybersecurity actions. There, every unified expected outcome is represented together with its corresponding function and category from the cybersecurity framework of National Institute of Standards and Technology (NIST). Each expected outcome in the ULEO has its own identifier. Expected outcomes from [99] are identified with the prefix “9D”, those from [100] are identified with the prefix “CSC”, and the remainder are identified using the original terminology from [101]. Furthermore, the associated Implementation Groups (IGs), to which the unified expected outcome should be applied, are determined. This enables the development of a proportionate cybersecurity approach, as lower IGs define the unified expected outcomes applicable to assets of lower criticality, while higher IGs pertain to assets with greater criticality. Additionally, leveraging this list for our proposal allows us to utilize the associated set of metrics concerning its implementation and the cybersecurity status of each asset to which they are applied.

Table 3. A fragment of the ULEO, as defined in the CyberTOMP framework, included for informational purposes.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3
Protect	PR.PT	9D-4		✓	✓
Protect	PR.PT	CSC-4.12			✓
.
.
.
Protect	PR.PT	PR.PT-5	✓	✓	✓

- It is also crucial to identify which functional area should be responsible for each of these cybersecurity actions, ensuring that the contribution of each functional area to overall cybersecurity enables genuine holistic cybersecurity. Furthermore, this allows the Wide-Scope CyberSOC to focus its efforts on supporting each area in developing specific cybersecurity actions from the perspective of its specialized field. During our research efforts, we conducted a detailed analysis of the various functional areas involved in cybersecurity, as defined in CyberTOMP (Table 4). We also examined the specific scope of each cybersecurity action and established the association between functional areas and corresponding actions in all cases, as described in [99,100,102]. The comprehensive results of our investigation can be found in Appendix A.

Table 4. Functional areas of the organization involved in holistic cybersecurity, as defined in the reference framework used in our proposal.

Area ID	Area’s Main Cybersecurity Responsibilities
FA1	In charge of the security of Internet of Things (IoT) devices.
FA2	Implementation of active defense measures, vulnerabilities management, threat hunting, Security Information and Event Management (SIEM) operation, activities within a CyberSOC, and incident response.
FA3	Human resources preparation regarding cybersecurity threats through continuous training and its reinforcement, as well as the design and execution of practical cybersecurity exercises

Table 4. Cont.

Area ID	Area's Main Cybersecurity Responsibilities
FA4	Analysis of internal and external threats, exchange of threat intelligence with third parties, and preparation and incorporation of Indicators of Compromise (IoCs).
FA5	Surveillance of the applicable regulation and its incorporation into cybersecurity. Key Performance Indicators (KPI) monitoring, establishment of strategies, policies, standards, processes, procedures, and corporate instructions.
FA6	Risk treatment, business continuity management, crisis management, establishing the organization's position regarding cyber risks, insurance contracting, risk registration, auditing, definition of groups of risk management, and definition of those responsible and owners of the processes and assets.
FA7	Cybersecurity risk analysis, vulnerability scanning, supply chain risk identification and analysis, asset inventory, risk monitoring, penetration testing of infrastructure, people, or information systems.
FA8	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 and the static or dynamic analysis of the code.
FA9	Management, development, implementation, and verification of compliance with the standards and regulations defined at the corporate level for cybersecurity: CIS controls [100], CIS Community Defense Model [103], MITRE matrix [104,105], NIST framework [101] for the improvement of cybersecurity of critical infrastructures or the family of standards ISO27000, CyberTOMP.
FA10	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 and the establishment of secure reference configurations.
FA11	Promote study, education and training, attendance at conferences and participation in related professional groups, training, or certification.
FA12	Internal and external corporate communication, social networks management, marketing and the establishment and maintenance of institutional relationship with interested third parties with whom the organization maintains some type of contact.

- Given that the Wide-Scope CyberSOC is going to be outsourced to third parties, it is highly advisable to establish a set of general requirements that clearly distinguish what is being contracted as a Wide-Scope CyberSOC and not merely a technologically focused CyberSOC. This is important because many service providers tend to offer traditional, technology-focused CyberSOC services by default. In the context of a public entity that has outsourced some of its workforce and has an external CyberSOC, we define a Wide-Scope CyberSOC as a CyberSOC with the following general requirements:
 - o Must possess the necessary skills and capabilities to understand, design, prescribe, advise, and monitor cybersecurity actions that can be executed by every functional area within an organization that can contribute to the organization's strategic common effort, with a particular focus on those functional areas that fall outside of the realm of computing or information technologies;
 - o Must be capable of positioning itself within the context of each organization's functional areas, and from this vantage point, be able to understand the implications (including what, how, where, when, and who) of these areas of expertise with regards to cybersecurity. In fact, a Wide-Scope CyberSOC must be an expert in all fields of knowledge that are relevant to cybersecurity. Not only in the most technological ones;
 - o Must be aware that those functional areas that do not typically participate in cybersecurity may not be conscious of the fact that they can significantly contribute to improving the overall state of cybersecurity from within their own areas of expertise. As such, a Wide-Scope CyberSOC must also act as a mentor to enhance

the awareness of these functional areas and develop their cybersecurity skills from the perspective of their areas of expertise;

- o Must be able to understand the organizational context and address circumstances where the functional areas with which it engages in cybersecurity may be partially outsourced and frequently renewed. Its mode of operation must be adapted to this situation in a seamless manner.

Drawing upon the characteristics of public entities that we have identified, and supported by the body of research we have examined and presented in Table 1, we have proposed the preceding paragraphs as general requirements for public entities when engaging a service provider for CyberSOC outsourcing.

This approach allows us to leverage the existing presence of an outsourced, technology-focused CyberSOC to offer a more comprehensive perspective on cybersecurity. Simultaneously, it enhances the awareness of the cybersecurity workforce regarding its potential contributions to the overall cybersecurity posture of the organization. While there may be alternative approaches, we believe that ours takes into account factors already prevalent in public organizations, which we have directly and indirectly analyzed in previous phases. These factors include the widespread adoption of outsourcing, the existence of mixed operational teams comprising both in-house and outsourced personnel, the challenges associated with acquiring cybersecurity talent, and the imperative need to augment cybersecurity skills to address the shortage in the cybersecurity workforce, among others. In our conception of a Wide-Scope CyberSOC, it must be proficient enough to serve as the cybersecurity reference unit within the organization and train cross-functional personnel applying a learning-by-doing approach, as explained in [106] by Deng et al., and also providing mentorship and coaching as needed, following the guidelines of [107–110] by Hamburg, Burrell, Ndueso et al., and Corradini, respectively. It is also necessary that the outsourced Wide-Scope CyberSOC has the ability of enhancing the cybersecurity awareness of workers, as in [65,66]. It should serve as a facilitating element that enables the continuous enhancement of cybersecurity capabilities and knowledge within each functional area involved in corporate cybersecurity, rather than solely designing and implementing these measures firsthand.

While it is not mandatory, it is advisable for the Wide-Scope CyberSOC to be viewed as a collective asset of the entire cross-functional cybersecurity workforce. Given that this new CyberSOC will be more deeply involved in the daily cybersecurity activities of various functional areas, we recommend positioning it within the organization in a way that minimizes the potential for any functional area to perceive conflicts of interest or biases, something identified by Monzelo and Nunes [111] or Badhwar [112], as shown in Figure 2.

- As a preliminary step before contracting the Wide-Scope CyberSOC service, it is also essential to turn the desired multidisciplinary capabilities, skills, and knowledge into explicit requirements for the service that any potential service provider must meet. These requirements will enable them to effectively mentor and provide the necessary support to the various functional areas contributing to cybersecurity. As part of our study, we have conducted this analysis and defined the necessary prerequisites, which can be directly incorporated into the technical specifications of the Wide-Scope CyberSOC. The specific knowledge requirements can be found in Appendix A;
- Finally, after addressing all the relevant points explained in this section, the public entity will be able to outsource the Wide-Scope CyberSOC service using its expertise in public procurement. Once the service is contracted, it should be managed using the existing procedures in the selected model, CyberTOMP. Figure 3 illustrates the specific activities of the tactical-operational cybersecurity management process defined in CyberTOMP, where the Wide-Scope CyberSOC should play a key role by contributing its expertise and acting as a cohesive element among the various functional areas of the organization. Furthermore, aside from the aforementioned aspect, which pertains exclusively to the set of steps/tasks delineated in the CyberTOMP proposal, the Wide-Scope CyberSOC must also undertake the activities typically associated with a

traditional CyberSOC. These activities may encompass actions within the realms of identify, protect, detect, respond, and recover approaches, as is customary.

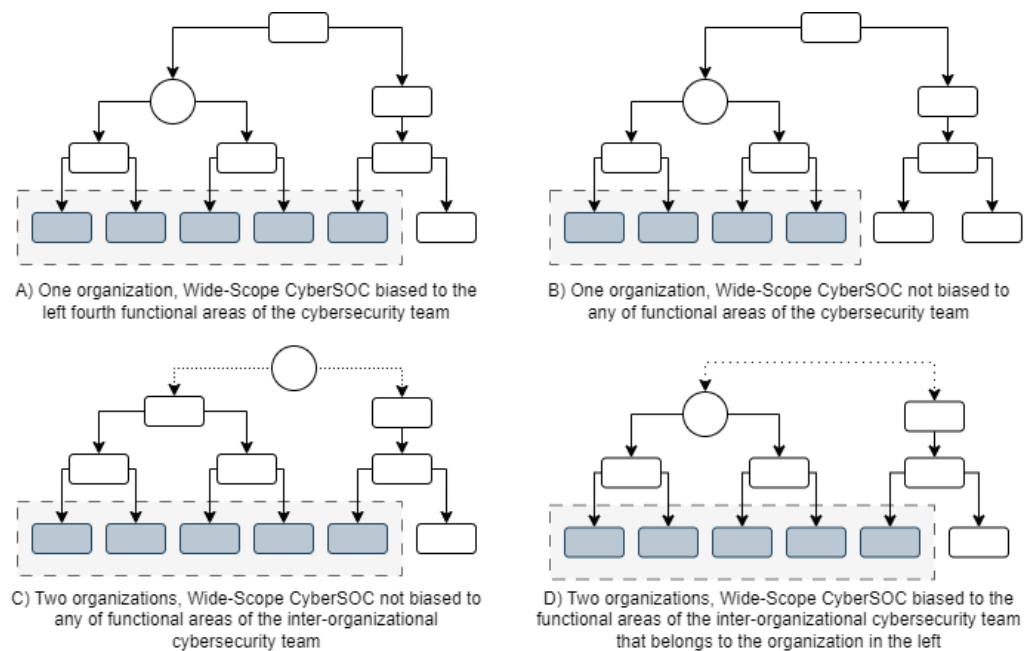


Figure 2. Here are four examples of organizational structures. In (B,C), the Wide-Scope CyberSOC (represented by a circle) is less likely to be perceived as biased, as every functional area involved in cybersecurity (shown in gray) that makes up the multidisciplinary cybersecurity team (enclosed by a dashed rectangle) has direct access to it, even if they belong to different organizations. Conversely, this is not the case in scenarios (A,D).



Figure 3. Tasks defined within the CyberTOMP framework in which the Wide-Scope CyberSOC can assume a significant role.

3.3. *Assessing the Wide-Scope CyberSOC Effect on the Deployment of Holistic Cybersecurity*

The core objective of our proposal is to ease the implementation of holistic cybersecurity by enhancing the capabilities of the cross-functional cybersecurity workforce, which includes individuals from both the public and private sectors. Our aim is to empower them to better comprehend and apply their roles, leveraging their specific expertise to contribute effectively to the overall organizational cybersecurity strategy.

To achieve this goal, we advocate for the adoption of the innovative Wide-Scope CyberSOC. It is crucial to underscore that our ultimate objective is to fortify the cybersecurity situational awareness of the personnel involved. To this end, we believe that evaluating and measuring the situational awareness of the cybersecurity cross-functional team over time, post-implementation of the Wide-Scope CyberSOC within the organization, serves as a robust means of validating the effectiveness of the Wide-Scope CyberSOC in simplifying the deployment of holistic cybersecurity.

To facilitate this measurement, we propose the utilization of structured questionnaires tailored to assess personnel's situational awareness skills across four key areas, in line with the requirements we recommend imposing on the Wide-Scope CyberSOC:

1. Grasping the holistic nature of cybersecurity and the extensive spectrum of potential, applicable cybersecurity actions;
2. Recognizing the responsibilities associated with each functional area and appreciating the critical importance of collective engagement in achieving the highest cybersecurity standards;
3. Understanding the imperative need for proportional cybersecurity measures, aligned with the criticality of assets;
4. Acknowledging that various approaches can be employed to attain the same objectives, thus enabling the distribution of cybersecurity efforts and resources throughout the organization to foster collaborative equilibrium.

Given that situational awareness training is inherently an ongoing process, it may take a substantial amount of time before conclusive results are obtained. Nevertheless, successive measurements should exhibit an upward trend in these skills among the cross-functional cybersecurity workforce.

4. Results and Discussion

The current research project addresses a genuine need of a Public Sector entity engaged in defining and implementing a holistic cybersecurity management model: the necessity to attain a comprehensive level of cybersecurity awareness among their personnel. With the collaboration of this organization, we undertook this work with the intention of ensuring that the outcomes, tools, and elements developed could also be applicable to other public sector entities. Our motivation lies not only in a sense of public service but also in the potential for collaboration and further evolution of the proposal.

To ensure this, we conducted our work adhering to the standard formal or semi-formal methods as described: We conducted an analysis of a relevant set of research works found in the current literature. Our goal was to identify requirements stemming from one of our previous studies and the need emerging from its applicability to a public sector entity. Subsequently, through interviews and work sessions, we assessed the entity's situation and specific characteristics regarding the adoption of a holistic model for cybersecurity management. Concurrently, we indirectly gathered information on similar characteristics in other public organizations from the same organization. We employed SWOT analysis technique, to systematically organize and categorize these attributes, to confirm these characteristics were similar to the common ones, we analyzed scrutinizing the international literature. This was crucial to develop a proposal applicable to all public organizations, not just the study participant. The outcome confirmed shared characteristics, and for that reason, we assumed they share a common scenario and could benefit from our proposal. Using a TOWS analysis technique, we identified successful strategies, guiding a coherent approach in our proposal's design. To implement the identified strategies, and taking into

account the features of public sector organizations, we designed an extended-capabilities CyberSOC that facilitates the adoption of the holistic model tactically and operationally by increasing the holistic cybersecurity awareness level of the cybersecurity workforce.

To the best of our knowledge, and after extensive periods of research, we have not encountered a study that addresses the development of holistic cybersecurity capabilities at the lower levels of the organization while also considering the specificities of public sector entities and their operational methods. Our proposal specifically targets this gap within public organizations.

As a contribution resulting from this study, we coined the new concept, “Wide-Scope CyberSOC”, which defines such a CyberSOC with extended capabilities. This CyberSOC can be easily outsourced, thanks to our identification of a well-structured, common, and multidisciplinary set of cybersecurity actions that has been also associated with each organization’s functional area involved in cybersecurity. We then transformed this set into directly applicable requirements when drafting technical specifications for the procurement of such services. As a result of this process, the outsourced Wide-Scope CyberSOC is managed and evaluated consistently, seamlessly integrated into a specific framework for the holistic, tactical-operational management of cybersecurity. These contributions can be found, summarized, and organized, in Appendix A.

The Wide-Scope CyberSOC will be capable of actively participating in and facilitating the tactical-operational cybersecurity team in various activities. These activities include identifying cybersecurity requirements, breaking down business assets, identifying functional areas involved in their cybersecurity, analyzing the cyber threat landscape, and adapting the organization accordingly. Additionally, the CyberSOC will be instrumental in designing and implementing cross-functional cybersecurity measures. This empowered CyberSOC will serve as a cornerstone, expediting the adoption of a multidisciplinary approach to cybersecurity management within the public organization.

As part of our study, in cooperation with the participating public entity, we have designed its first Wide-Scope CyberSOC. It underwent a public tender process, with various security service providers submitting their offers. The organization has since implemented and is currently managing its first Wide-Scope CyberSOC based on the guidelines outlined in this study. In the meanwhile, we are assessing the effect of introducing the Wide-Scope CyberSOC in this public sector organization following the method described in Section 3.3. Initial measurements show promise, but further data collection and maturation are required before presenting the results to the general public, which will take a considerable amount of time.

We devoted a substantial amount of effort to carefully plan our research approach, ensuring that the results would not only be beneficial for the participating public organization, but also applicable to other public sector organizations internationally. While we are confident that it aligns well with the Spanish case study, we conducted and took the necessary precautions to facilitate its applicability to a broader range of public organizations, and we acknowledge that no research is immune to the possibility of unintentional biases or errors. We have identified two potential areas where these unlikely events could occur:

- The generalization process in our research was built upon the presence of common features and circumstances identified in the global literature pertaining to public sector organizations, along with the parallel existence of these same insights within the public organization participating in our study. This alignment allowed us to establish a connection that led us to recognize that the insights from our case study are applicable to other public organizations worldwide. To ensure the reliability of our approach, we deliberately selected a comprehensive array of research works for the analysis of current literature concerning public sector organizations. This approach was taken specifically to reduce the risk of selecting only a few sources that might not accurately represent these public organizations. Nonetheless, despite our efforts, there is a slight possibility that our selection of research works may have been influenced by unconscious bias;

- On the other hand, we have introduced a method to evaluate the effectiveness of our proposal, which we are currently applying to the participating organization in our study. The initial results appear promising, but they require extended assessment over time to thoroughly ascertain the model's benefits. Furthermore, since this is a generalization based on a single case study, the only application thus far has been the one conducted as part of our research. Additional applications will offer valuable data to refine our proposal if necessary.

While we have not identified any of the situations mentioned, and despite our vigilance and awareness, we acknowledge that these could be two points where additional checks could be beneficial to strengthen our work. Therefore, we encourage third parties to independently analyze the generalization process we conducted and implement the model in other public organizations to verify the results or propose enhancements that contribute to the body of knowledge related to holistic cybersecurity management in public sector organizations.

5. Conclusions and Future Work

As highlighted in the introduction, organizations across various sectors, both public and private, are becoming increasingly reliant on cyberspace, a realm beyond complete control, rendering them susceptible to dynamic cyber threats. This vulnerability exposes organizations to potential risks, including business disruptions and sensitive data breaches. For public entities, such risks translate into an inability to deliver essential public services and a failure to safeguard citizens' data and privacy. To address this challenge effectively, an enhanced cybersecurity awareness among the cybersecurity workforce is essential. We have identified common characteristics among public sector organizations, enabling us to propose a comprehensive solution that equips them to navigate cyberspace securely. Our proposal introduces a novel outsourced CyberSOC, the Wide-Scope CyberSOC, designed to facilitate the development of holistic cybersecurity skills within the workforce and streamline holistic cybersecurity management in public sector organizations. This work offers a valuable framework applicable to any public entity, particularly those heavily engaged in digital citizen services, where the exposure to the expanding cyber threats landscape is significant. Additionally, we have outlined the comprehensive set of requirements that public organizations should request from Wide-Scope CyberSOC service providers to ensure the fulfillment of necessary functionalities. As part of future work, we are exploring the development of specific tools to simplify the operations of Wide-Scope CyberSOCs and enhance the holistic cybersecurity awareness of cross-functional cybersecurity teams.

Author Contributions: Conceptualization, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; methodology, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; software, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; validation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; formal analysis, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; investigation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; resources, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; data curation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; writing—original draft preparation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; writing—review and editing, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; visualization, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; supervision, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; project administration, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; funding acquisition, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by TED2021-131699B-I00/ MCIN/AEI/10.13039/501100011033/ European Union NextGenerationEU/PRTR.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

Table A1. Knowledge Requirements to Contract Wide-Scope CyberSOC Services.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: “The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in . . .”
Identify	ID.AM	CSC-1.1	✓	✓	✓	FA7	Establishing and maintaining a detailed enterprise asset inventory with the potential to store or process data.
Identify	ID.AM	CSC-12.4		✓	✓	FA10	Establishing and maintaining architecture diagrams.
Identify	ID.AM	CSC-14.1	✓	✓	✓	FA3	Establishing and maintaining a security awareness program.
Identify	ID.AM	CSC-2.2	✓	✓	✓	FA8	Ensuring that only authorized, supported software is used.
Identify	ID.AM	CSC-3.1	✓	✓	✓	FA5	Establishing and maintaining a process for data management
Identify	ID.AM	CSC-3.2	✓	✓	✓	FA10	Establishing and maintaining a data inventory.
Identify	ID.AM	CSC-3.6	✓	✓	✓	FA10	Identifying data on end-user devices that has encryption requirements.
Identify	ID.AM	CSC-3.7		✓	✓	FA9	Establishing and maintaining a data classification scheme
Identify	ID.AM	ID.AM-1	✓	✓	✓	FA7	Establishing and maintaining detailed inventory of physical devices and systems.
Identify	ID.AM	ID.AM-2	✓	✓	✓	FA8	Inventorying all software platforms and applications within the organization.
Identify	ID.AM	ID.AM-3		✓	✓	FA8	Mapping organizational communication and data flows.
Identify	ID.BE	9D-1		✓	✓	FA7	Analyzing the business environment to determine potential ways of deterring attacks.
Identify	ID.BE	ID.BE-1			✓	FA6	Identifying and communicating the organization’s role in the supply chain.
Identify	ID.BE	ID.BE-2			✓	FA6	Identifying and communicating the organization’s place in critical infrastructure and its industry sector.
Identify	ID.BE	ID.BE-3			✓	FA5	Establishing and communicating priorities for organizational mission, objectives, and activities.
Identify	ID.BE	ID.BE-4			✓	FA5	Establishing dependencies and critical functions for delivery of critical services.
Identify	ID.BE	ID.BE-5			✓	FA5	Establishing resilience requirements to support delivery of critical services for all operating states.
Identify	ID.GV	CSC-17.4		✓	✓	FA5	Establishing, maintaining an incident response process.
Identify	ID.GV	ID.GV-1	✓	✓	✓	FA5	Establishing and communicating organizational cybersecurity policy.
Identify	ID.GV	ID.GV-2		✓	✓	FA9	Coordinating and aligning cybersecurity roles and responsibilities with internal roles and external partners.
Identify	ID.GV	ID.GV-3			✓	FA5	Understanding and managing legal and regulatory requirements regarding cybersecurity.

Table A1. Cont.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Identify	ID.GV	ID.GV-4			✓	FA5	Ensuring governance and risk management processes address cybersecurity risks.
Identify	ID.RA	9D-1		✓	✓	FA7	Ensuring that the organization understands the risk of vulnerabilities and the necessity of deterring their exploitation.
Identify	ID.RA	CSC-18.2		✓	✓	FA7	Conducting periodic external penetration tests in order to enhance understanding of cyber risks.
Identify	ID.RA	CSC-18.5			✓	FA7	Conducting periodic internal penetration tests in order to enhance understanding of cyber risks.
Identify	ID.RA	CSC-3.7		✓	✓	FA9	Assessing the current validity of the data classification scheme in relation to existing risks.
Identify	ID.RA	ID.RA-1	✓	✓	✓	FA7	Identifying and documenting assets vulnerabilities.
Identify	ID.RA	ID.RA-2			✓	FA4	Ensuring cyber threat intelligence is received from information sharing forums and sources.
Identify	ID.RA	ID.RA-3			✓	FA4	Identifying and document threats, both internal and external.
Identify	ID.RA	ID.RA-4			✓	FA6	Identifying potential business impacts and likelihoods.
Identify	ID.RA	ID.RA-6			✓	FA6	Identifying and prioritizing risk responses.
Identify	ID.RM	9D-8		✓	✓	FA2	Comprehending the potential risks that necessitate redirecting attackers to alternative targets.
Identify	ID.RM	ID.RM-1			✓	FA6	Ensuring risk management processes are established, managed, and agreed to by organizational stakeholders.
Identify	ID.RM	ID.RM-2			✓	FA6	Determining and clearly expressing organizational risk tolerance.
Identify	ID.RM	ID.RM-3			✓	FA6	Informing the organization's risk tolerance by its role in critical infrastructure and sector specific risk analysis.
Identify	ID.SC	ID.SC-1		✓	✓	FA5	Identifying, establishing, assessing, and managing cyber supply chain risk management processes.
Identify	ID.SC	ID.SC-2	✓	✓	✓	FA5	Identifying, prioritizing, and assessing third party partners of information systems, components, and services, using a cybersecurity supply chain risk assessment process.
Identify	ID.SC	ID.SC-3		✓	✓	FA9	Ensuring contracts with suppliers and third-party are designed to meet the goals of an organization's cybersecurity program and cybersecurity supply chain management plan.
Identify	ID.SC	ID.SC-4			✓	FA6	Auditing, testing, and evaluating suppliers and third-party partners to confirm they are meeting their contractual obligations.
Identify	ID.SC	ID.SC-5	✓	✓	✓	FA9	Conducting response and recovery planning and testing with suppliers and third-party providers.
Protect	PR.AC	CSC-12.5		✓	✓	FA10	Centralizing network authentication, authorization, and auditing.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: “The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . .”
Protect	PR.AC	CSC-12.6		✓	✓	FA10	Employing secure network management and communication protocols.
Protect	PR.AC	CSC-13.4		✓	✓	FA10	Conducting traffic filtering between network segments
Protect	PR.AC	CSC-4.7	✓	✓	✓	FA10	Managing default accounts on enterprise assets and software.
Protect	PR.AC	CSC-5.2	✓	✓	✓	FA10	Using unique passwords for all enterprise assets.
Protect	PR.AC	CSC-5.6		✓	✓	FA10	Centralizing account management.
Protect	PR.AC	CSC-6.8			✓	FA10	Deploying and maintaining Role-Based Access Control (RBAC)
Protect	PR.AC	PR.AC-1	✓	✓	✓	FA10	Ensuring identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
Protect	PR.AC	PR.AC-2			✓	FA7	Ensuring physical access to assets is managed and protected.
Protect	PR.AC	PR.AC-3	✓	✓	✓	FA10	Ensuring remote access is managed.
Protect	PR.AC	PR.AC-4	✓	✓	✓	FA10	Ensuring access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
Protect	PR.AC	PR.AC-5	✓	✓	✓	FA10	Ensuring network integrity is protected.
Protect	PR.AC	PR.AC-6			✓	FA10	Ensuring identities are proofed and bound to credentials and asserted in interactions.
Protect	PR.AC	PR.AC-7	✓	✓	✓	FA10	Ensuring users, devices, and other assets are authenticated commensurate with the risk of the transaction.
Protect	PR.AT	CSC-14.9		✓	✓	FA3	Conducting role-specific security awareness and skills training.
Protect	PR.AT	CSC-15.4		✓	✓	FA5	Ensuring service provider contracts include security requirements.
Protect	PR.AT	PR.AT-1	✓	✓	✓	FA3	Ensuring all users are informed and trained.
Protect	PR.AT	PR.AT-2		✓	✓	FA3	Ensuring privileged users understand their roles and responsibilities.
Protect	PR.DS	9D-6			✓	FA8	Dispersing protective measures throughout the payload to safeguard the data.
Protect	PR.DS	CSC-3.4	✓	✓	✓	FA10	Enforcing data retention in accordance with the risk strategy.
Protect	PR.DS	PR.DS-1		✓	✓	FA10	Ensuring data-at-rest is protected.
Protect	PR.DS	PR.DS-2		✓	✓	FA10	Ensuring data-in-transit is protected.
Protect	PR.DS	PR.DS-3	✓	✓	✓	FA10	Ensuring assets are formally managed throughout removal, transfers, and disposition.
Protect	PR.DS	PR.DS-4			✓	FA10	Adjusting capacity to ensure availability is maintained.
Protect	PR.DS	PR.DS-5			✓	FA10	Ensuring protections against data leaks are implemented.
Protect	PR.DS	PR.DS-6		✓	✓	FA10	Ensuring integrity checking mechanisms are used to verify software, firmware, and information integrity.

Table A1. Cont.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Protect	PR.DS	PR.DS-7		✓	✓	FA10	Ensuring the development and testing environment(s) are separate from the production environment.
Protect	PR.DS	PR.DS-8			✓	FA10	Ensuring integrity checking mechanisms are used to verify hardware integrity.
Protect	PR.IP	9D-3		✓	✓	FA2	Enhancing the difficulty of accessing the protected information beyond the attacker's skills.
Protect	PR.IP	9D-5		✓	✓	FA2	Investigating the threat in depth in order to prevent access to protected information using a multi-layered approach.
Protect	PR.IP	9D-8		✓	✓	FA2	Implementing measures to divert attackers in order to protect the information.
Protect	PR.IP	9D-9	✓	✓	✓	FA2	Implementing measures in depth that become increasingly challenging and less visible as they approach the asset.
Protect	PR.IP	CSC-11.1	✓	✓	✓	FA10	Establishing and maintaining a process for data recovery.
Protect	PR.IP	CSC-16.1		✓	✓	FA8	Establishing and maintaining a secure application development process.
Protect	PR.IP	CSC-16.14			✓	FA4	Undertaking comprehensive threat modelling.
Protect	PR.IP	CSC-18.4			✓	FA7	Validating the security measures deployed to protect information following each penetration test.
Protect	PR.IP	CSC-2.5		✓	✓	FA5	Creating an allow list of authorized software in order to protect information.
Protect	PR.IP	CSC-2.6		✓	✓	FA5	Creating an allow list of authorized libraries in order to protect information.
Protect	PR.IP	CSC-2.7			✓	FA5	Creating an allow list of authorized scripts in order to protect information.
Protect	PR.IP	CSC-4.3	✓	✓	✓	FA10	Configuring automatic session locking on enterprise assets to protect the information.
Protect	PR.IP	PR.IP-1	✓	✓	✓	FA5	Ensuring a baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.
Protect	PR.IP	PR.IP-10		✓	✓	FA5	Ensuring response and recovery plans are tested.
Protect	PR.IP	PR.IP-11	✓	✓	✓	FA11	Incorporating cybersecurity into human resources practices for information handling.
Protect	PR.IP	PR.IP-12		✓	✓	FA7	Developing and implementing a vulnerability management plan.
Protect	PR.IP	PR.IP-2		✓	✓	FA10	Implementing a system development life cycle to manage systems.
Protect	PR.IP	PR.IP-3			✓	FA5	Designing a configuration change control process.
Protect	PR.IP	PR.IP-4	✓	✓	✓	FA10	Ensuring backups of information are conducted, maintained, and tested.
Protect	PR.IP	PR.IP-5			✓	FA5	Ensuring policy and regulations regarding the physical operating environment for organizational assets are met.

Table A1. Cont.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . ."
Protect	PR.IP	PR.IP-6	✓	✓	✓	FA10	Ensuring data is destroyed according to policy.
Protect	PR.IP	PR.IP-7		✓	✓	FA5	Ensuring protection processes are improved.
Protect	PR.IP	PR.IP-8			✓	FA2	Ensuring effectiveness of protection technologies is shared.
Protect	PR.IP	PR.IP-9	✓	✓	✓	FA5	Ensuring response plans and recovery plans are in place and managed.
Protect	PR.MA	9D-5		✓	✓	FA2	Conducting maintenance activities on all layers of the asset.
Protect	PR.MA	9D-9		✓	✓	FA2	Carrying out maintenance tasks to ensure depth of defense.
Protect	PR.MA	CSC-12.1	✓	✓	✓	FA10	Carrying out maintenance to ensure the network infrastructure is up to date.
Protect	PR.MA	CSC-12.3		✓	✓	FA10	Managing the network infrastructure with a security-oriented approach.
Protect	PR.MA	CSC-13.5		✓	✓	FA10	Carrying out maintenance actions to ensure assets remotely connecting to enterprise resources comply with the organization's requirements.
Protect	PR.MA	CSC-16.13			✓	FA2	Performing root cause analysis on security vulnerabilities.
Protect	PR.MA	CSC-18.3		✓	✓	FA10	Remediating penetration test findings.
Protect	PR.MA	CSC-4.2	✓	✓	✓	FA5	Carrying out tasks to securely configure the network infrastructure in accordance with established processes.
Protect	PR.MA	CSC-4.6	✓	✓	✓	FA10	Carrying out security maintenance tasks on enterprise assets and software.
Protect	PR.MA	CSC-4.8		✓	✓	FA10	Uninstalling or disabling unnecessary services on enterprise assets and software.
Protect	PR.MA	CSC-4.9		✓	✓	FA10	Configuring trusted DNS servers on enterprise assets.
Protect	PR.MA	CSC-7.3	✓	✓	✓	FA10	Performing automated operating system patch management.
Protect	PR.MA	CSC-8.1	✓	✓	✓	FA5	Establishing and maintaining an audit log management process.
Protect	PR.MA	CSC-8.10		✓	✓	FA10	Retaining audit logs.
Protect	PR.MA	CSC-8.3	✓	✓	✓	FA10	Ensuring adequate audit log storage.
Protect	PR.MA	CSC-8.9		✓	✓	FA10	Centralizing audit log collection and retention.
Protect	PR.MA	PR.MA-1			✓	FA10	Ensuring maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
Protect	PR.PT	9D-4		✓	✓	FA2	Implementing differentiated protections to address each threat specifically.
Protect	PR.PT	9D-7			✓	FA2	Employing decoys to distract attackers.
Protect	PR.PT	CSC-4.12			✓	FA10	Separating enterprise workspaces on mobile end-user devices
Protect	PR.PT	CSC-4.4	✓	✓	✓	FA10	Implementing and managing a firewall on servers

Table A1. Cont.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Protect	PR.PT	CSC-4.5	✓	✓	✓	FA10	Implementing and managing a firewall on end-user devices
Protect	PR.PT	CSC-9.5		✓	✓	FA10	Implementing DMARC.
Protect	PR.PT	PR.PT-1	✓	✓	✓	FA10	Ensuring audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
Protect	PR.PT	PR.PT-2	✓	✓	✓	FA10	Ensuring removable media is protected and its use restricted according to policy.
Protect	PR.PT	PR.PT-3			✓	FA10	Ensuring the principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
Protect	PR.PT	PR.PT-4			✓	FA10	Ensuring communications and control networks are protected.
Protect	PR.PT	PR.PT-5	✓	✓	✓	FA10	Ensuring mechanisms are implemented to achieve resilience requirements in normal and adverse situations.
Detect	DA.AE	CSC-8.12			✓	FA10	Collecting service provider logs to detect anomalies.
Detect	DA.AE	DE.AE-1		✓	✓	FA10	Establishing and maintaining a baseline of operations and expected data flows for users and systems.
Detect	DA.AE	DE.AE-2		✓	✓	FA2	Analyzing detected events to understand attack targets and methods.
Detect	DA.AE	DE.AE-3	✓	✓	✓	FA2	Collecting and correlating event data correlated from multiple sources and sensors.
Detect	DA.AE	DE.AE-4			✓	FA2	Determining impact of events.
Detect	DA.AE	DE.AE-5			✓	FA2	Establishing incident alert thresholds.
Detect	DE.CM	CSC-13.1		✓	✓	FA2	Centralizing security event alerting
Detect	DE.CM	CSC-13.5		✓	✓	FA10	Monitoring access control for assets remotely connecting to enterprise resources.
Detect	DE.CM	CSC-3.14			✓	FA10	Logging access to sensitive data.
Detect	DE.CM	DE.CM-1		✓	✓	FA2	Ensuring the network is monitored to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-2			✓	FA1	Ensuring the physical environment is monitored to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-3			✓	FA10	Ensuring personnel activity is monitored to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-4	✓	✓	✓	FA2	Detecting malicious code.
Detect	DE.CM	DE.CM-5			✓	FA2	Detecting unauthorized mobile code.
Detect	DE.CM	DE.CM-6			✓	FA2	Monitoring external service provider activity to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-7	✓	✓	✓	FA2	Monitoring for unauthorized personnel, connections, devices, and software.
Detect	DE.CM	DE.CM-8		✓	✓	FA7	Conducting periodic vulnerability scans
Detect	DE.DP	CSC-17.1	✓	✓	✓	FA5	Designating personnel, including key and backup, to manage incident handling.

Table A1. Cont.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Detect	DE.DP	CSC-17.4		✓	✓	FA5	Testing the incident response process to ensure it includes awareness of anomalous events.
Detect	DE.DP	CSC-17.5		✓	✓	FA5	Assigning key cross-functional roles and responsibilities in relation to incident response.
Detect	DE.DP	DE.DP-2			✓	FA2	Ensuring detection activities comply with all applicable requirements.
Detect	DE.DP	DE.DP-3			✓	FA10	Testing detection processes.
Detect	DE.DP	DE.DP-5			✓	FA5	Continuously improving detection processes.
Respond	RS.AN	CSC-17.9			✓	FA5	Establishing and maintaining security incident thresholds to ensure effective response.
Respond	RS.AN	RS.AN-1		✓	✓	FA2	Ensuring notifications from detection systems are investigated.
Respond	RS.AN	RS.AN-2			✓	FA2	Ensuring the impact of the incident is understood.
Respond	RS.AN	RS.AN-3			✓	FA2	Ensuring forensics are performed.
Respond	RS.AN	RS.AN-5		✓	✓	FA5	Ensuring processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources.
Respond	RS.CO	CSC-17.4	✓	✓	✓	FA5	Communicating the incident response process.
Respond	RS.CO	CSC-17.5		✓	✓	FA5	Communicating key cross-functional roles and responsibilities in relation to incident response.
Respond	RS.CO	RS.CO-5			✓	FA4	Ensuring voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Respond	RS.IM	RS.IM-1		✓	✓	FA5	Ensuring response plans incorporate lessons learned.
Respond	RS.IM	RS.IM-2		✓	✓	FA5	Response strategies are updated.
Respond	RS.MI	CSC-1.2	✓	✓	✓	FA10	Ensuring that a process is in place to address unauthorized assets.
Respond	RS.MI	CSC-4.10		✓	✓	FA10	Enforcing remote wipe capability on portable end-user devices
Respond	RS.MI	CSC-7.7		✓	✓	FA10	Remediating detected vulnerabilities and weakness.
Respond	RS.MI	RS.MI-1			✓	FA2	Containing incidents.
Respond	RS.MI	RS.MI-2			✓	FA2	Mitigating incidents.
Respond	RS.MI	RS.MI-3			✓	FA2	Mitigating newly identified vulnerabilities or documenting them as accepted risks.
Respond	RS.RP	CSC-17.6		✓	✓	FA5	Defining mechanisms for communicating during incident response.
Respond	RS.RP	RS.RP-1			✓	FA2	Ensuring a response plan is executed during or after an incident.
Recover	RC.CO	RC.CO-1			✓	FA12	Managing public relations.
Recover	RC.CO	RC.CO-2			✓	FA12	Repairing the reputation after an incident.
Recover	RC.CO	RC.CO-3			✓	FA12	Communicating recovery activities to internal and external stakeholders as well as executive and management teams.

Table A1. Cont.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: “The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in . . .”
Recover	RC.IM	RC.IM-1			✓	FA5	Ensuring recovery plans incorporate lessons learned.
Recover	RC.IM	RC.IM-2			✓	FA5	Ensuring recovery strategies are updated.
Recover	RC.RP	RC.RP-1			✓	FA2	Ensuring a recovery plan is executed during or after a cybersecurity incident.

References

- Domínguez-Dorado, M.; Carmona-Murillo, J.; Cortés-Polo, D.; Rodríguez-Pérez, F.J. CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels. *IEEE Access* **2022**, *10*, 122454–122485. [\[CrossRef\]](#)
- von Solms, R.; van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [\[CrossRef\]](#)
- Reid, R.; van Niekerk, J. From information security to cyber security cultures. In Proceedings of the Information Security for South Africa, Johannesburg, South Africa, 13–14 August 2014.
- Furnell, S. The cybersecurity workforce and skills. *Comput. Secur.* **2012**, *100*, 102080. [\[CrossRef\]](#)
- De Zan, T. Mitigating the Cyber Security Skills Shortage: The Influence of National Skills Competitions on Cyber Security Interest. Ph.D. Thesis, Department of Education and Centre for Doctoral Training in Cyber Security, Linacre College, University of Oxford, Oxford, UK, 2021.
- Reeder, F.; Alan, P. *What Works in Finding Elite Cybersecurity Talent: Promising Practices for Chief Information Officers*; CIO.org: Newport, UK, 2021.
- DeCrosta, J. Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage. Ph.D. Thesis, Utica College, Utica, NY, USA, 2021.
- Shava, E.; Hofisi, C. Challenges and Opportunities for Public Administration in the Fourth Industrial Revolution. *Afr. J. Public Aff.* **2017**, *9*, 203–215.
- Ngwenyama, O.; Henriksen, H.Z.; Hardt, D. Public management challenges in the digital risk society: A Critical Analysis of the Public Debate on Implementation of the Danish NemID. *Eur. J. Inf. Syst.* **2023**, *32*, 108–126. [\[CrossRef\]](#)
- Nizich, M. Preparing the Cybersecurity Workforce of Tomorrow. In *The Cybersecurity Workforce of Tomorrow (The Future of Work)*; Emerald Group Publishing Limited: Bingley, UK, 2023; pp. 117–146.
- Lee, G.R.; Lee, S.; Malatesta, D.; Fernández, S. Outsourcing and Organizational Performance: The Employee Perspective. *Am. Rev. Public Adm.* **2019**, *49*, 973–986. [\[CrossRef\]](#)
- Onwubiko, C.; Ouazzane, K. Challenges towards Building an effective Cyber Security Operations Centre. *Int. J. Cyber Situational Aware.* **2019**, *4*, 11–39. [\[CrossRef\]](#)
- Schatz, D.; Bashroush, R.; Wall, J. Towards a More Representative Definition of Cyber Security. *J. Digit. Forensics Secur. Law* **2017**, *12*, 53–74.
- Ghelani, D. Cyber Security, Cyber Threats, Implications and Future. *Am. J. Sci. Eng. Technol.* **2022**, *3*, 12–19.
- Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *Int. J. Inform. Vis.* **2020**, *4*, 225–230. [\[CrossRef\]](#)
- Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. [\[CrossRef\]](#)
- Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [\[CrossRef\]](#)
- Atoum, I.; Ootom, A.; Ali, A.A. A holistic cyber security implementation framework. *Inf. Manag. Comput. Secur.* **2014**, *22*, 251–264. [\[CrossRef\]](#)
- van Kranenburg, R.; Le Gars, G. The Cybersecurity Aspects of New Entities Need a Cybernetic, Holistic Perspective. *Int. J. Cyber Forensic Adv. Threat Investig.* **2021**, *1*, 2. [\[CrossRef\]](#)
- Del-Real, C.; Díaz-Fernández, A.M. Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *Int. Cybersecur. Law Rev.* **2022**, *3*, 313–343. [\[CrossRef\]](#)
- Oruj, Z. Cyber security: Contemporary cyber threats and national strategies. *Distance Educ. Ukr. Innov. Norm.-Leg. Pedagog. Asp.* **2023**, *1*, 100–116.
- Sharikov, P. Contemporary Cybersecurity Challenges. In *The Implications of Emerging Technologies in the Euro-Atlantic Space*; Palgrave Macmillan: Cham, Switzerland; Basel, Switzerland, 2023; pp. 143–157.
- Cavelty, M.D.; Smeets, M. Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *J. Eur. Public Policy* **2023**, *30*, 1330–1352. [\[CrossRef\]](#)
- Kosseff, J. Upgrading Cybersecurity Law. *Houst. Law Rev. Forthcom.* **2023**, 1–33. [\[CrossRef\]](#)

25. Creemers, R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy. *J. Contemp. China* **2023**, *1–16*. [[CrossRef](#)]
26. Mijwil, M.M.; Filali, Y.; Aljanabi, M.; Bounabi, M.; Al-Shahwani, H. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 1–6.
27. Abazi, B. Establishing the National Cybersecurity (Resilience) Ecosystem. *IFAC-PapersOnLine* **2022**, *55*, 42–47. [[CrossRef](#)]
28. ENISA. *ENISA Threat Landscape 2022*; European Union Agency for Cybersecurity: Heraclión, Greece, 2022.
29. Hinkley, S. *Technology in the Public Sector and the Future of Government Work*; UC Berkeley Labor Center: Berkeley, CA, USA, 2022.
30. Norris, D.F.; Mateczun, L.K.; Forno, R.F. What the Literature Says About Local Government Cybersecurity. In *Cybersecurity and Local Government*; Wiley Data and Cybersecurity: Hoboken, NJ, USA, 2022; pp. 47–66.
31. CCN-CERT. *Ciberamenazas y Tendencias: Eidición 2022*; Centro Criptológico Nacional: Madrid, Spain, 2022.
32. Farrand, B.; Carrapico, H. Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *Eur. Secur.* **2022**, *31*, 435–453. [[CrossRef](#)]
33. Al Mehairi, A.; Zgheib, R.; Abdellatif, T.M.; Conchon, E. Cyber Security Strategies While Safeguarding Information Systems in Public/Private Sectors. In *Electronic Governance with Emerging Technologies, Proceedings of the EGETC 2022, Tampico, Mexico, 12–14 September 2022*; Communications in Computer and Information Science; Springer: Cham, Switzerland, 2022; pp. 49–63.
34. Blondin, D.; Boin, A. Cooperation in the Face of Transboundary Crisis: A Framework for Analysis. *Perspect. Public Manag. Gov.* **2020**, *3*, 197–209. [[CrossRef](#)]
35. Domínguez-Dorado, M.; Cortés-Polo, D.; Carmona-Murillo, J.; Rodríguez-Pérez, F.J.; Galeano-Brajones, J. Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management. *Appl. Sci.* **2023**, *13*, 6327. [[CrossRef](#)]
36. Quinn, S.; Ivy, N.; Barrett, M.; Feldman, L.; Topper, D.; Witte, G.; Gardner, R.K. *Using Business Impact Analysis to Inform Risk Prioritization and Response*; NIST Interagency Report NIST IR 8286D; NIST: Gaithersburg, MD, USA, 2022.
37. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.* **2021**, *1*, 119–139. [[CrossRef](#)]
38. Rajan, R.; Rana, N.P.; Parameswar, N.; Dhir, S.; Sushil; Dwivedi, Y.K.K. Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technol. Forecast. Soc. Change* **2021**, *170*, 120872. [[CrossRef](#)]
39. Axon, L.; Erola, A.; van Rensburg, A.J.; Nurse, J.R.C.; Goldsmith, M.; Creese, S. Practitioners’ Views on Cybersecurity Control Adoption and Effectiveness. In *Proceedings of the ARES 2021: The 16th International Conference on Availability, Reliability and Security*, Vienna, Austria, 17–20 August 2021; ACM ICPS. ACM: New York, NY, USA, 2021; pp. 1–10.
40. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [[CrossRef](#)]
41. Preis, B.; Susskind, L. Municipal Cybersecurity: More Work Needs to be Done. *Urban Aff. Rev.* **2020**, *58*, 614–629. [[CrossRef](#)]
42. Clark, M.; Espinosa, J.; Delone, W. Defending Organizational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*, Maui, HI, USA, 7–10 January 2020; pp. 4283–4292.
43. Phillips, R.; Tanner, B. Breaking down silos between business continuity and cyber security. *J. Bus. Contin. Emerg. Plan.* **2019**, *12*, 224–232.
44. Kure, H.I.; Islam, S. Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 332–340. [[CrossRef](#)]
45. Rothrock, R.A.; Kaplan, J.; Van Der Oord, F. The Board’s Role in Managing Cybersecurity Risks. *MIT Sloan Manag. Rev.* **2018**, *59*, 12–15.
46. Limba, T.; Plèta, T.; Agafonov, K.; Damkus, M. Cyber security management model for critical infrastructure. *Entrep. Sustain. Issues* **2017**, *4*, 559–573. [[CrossRef](#)]
47. Breier, J.; Hudec, L. On Selecting Critical Security Controls. In *Proceedings of the 2013 International Conference on Availability, Reliability and Security*, Regensburg, Germany, 2–6 September 2013; IEEE: New York, NY, USA, 2013; pp. 1–7.
48. Almoughem, K.A.B.M. The Future of Cybersecurity Workforce Development. *Acad. J. Res. Sci. Publ.* **2023**, *4*, 37–48. [[CrossRef](#)]
49. Shah, A.; Ganesan, R.; Jajodia, S.; Cam, H.; Hutchinson, S. A Novel Team Formation Framework based on Performance in a Cybersecurity Operations Center. *IEEE Trans. Serv. Comput. Early Access* **2023**, *16*, 2359–2371. [[CrossRef](#)]
50. Adetoye, B.; Fong, R.C.-W. Building a Resilient Cybersecurity Workforce: A Multidisciplinary Solution to the Problem of High Turnover of Cybersecurity Analysts. In *Cybersecurity in the Age of Smart Societies*; Springer: Cham, Switzerland, 2023; pp. 61–87.
51. Balon, T.; Baggili, I. Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Educ. Inf. Technol.* **2023**, *28*, 11759–11791. [[CrossRef](#)]
52. Nadua, F.-D.-L.; Escandor, L.; Bangayan, M.; Vigonte, F.; Abante, M.V. Identifying Incentives to Address Attrition in the Government Cybersecurity Workforce. 2023; pp. 1–21. Available online: <https://ssrn.com/abstract=4382110> (accessed on 16 October 2023).
53. Fisk, N.; Kelly, N.M.; Liebrock, L. Cybersecurity Communities of Practice: Strategies for Creating Gateways to Participation. *Comput. Secur.* **2023**, *132*, 103188. [[CrossRef](#)]
54. Ashley, T.D.; Kwon, R.; Gourisetti, S.N.G.; Katsis, C.; Bonebrake, C.A.; Boyd, P.A. Gamification of Cybersecurity for Workforce Development in Critical Infrastructure. *IEEE Access* **2022**, *10*, 112487–112501. [[CrossRef](#)]

55. Justice, C.; Sample, C.; Loo, S.M.; Ball, A.; Hampton, C. Future Needs of the Cybersecurity Workforce. In Proceedings of the 17th International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022; Academic Conferences International Limited: South Oxfordshire, UK, 2022; Volume 17, pp. 81–91.
56. Ahmad, N.; Laplante, P.A.; DeFranco, J.F.; Kassab, M. A Cybersecurity Educated Community. *IEEE Trans. Emerg. Top. Comput.* **2022**, *10*, 1456–1463. [[CrossRef](#)]
57. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. *Comput. Sci. Rev.* **2021**, *40*, 100361. [[CrossRef](#)]
58. Noche, E.B. A Literature Review of Empirical Studies on Cyber Security Workforce Development. *Asian J. Multidiscip. Stud.* **2021**, *4*, 65–73.
59. Hulatt, D.; Stavrou, E. The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation. In *Human Aspects of Information Security and Assurance, Proceedings of the 15th IFIP WG 11.12 International Symposium, HAISA 2021*; Virtual, 7–9 July 2021, Springer: Cham, Switzerland, 2021; pp. 138–147.
60. Kävrestad, J.; Nohlberg, M. Evaluation Strategies for Cybersecurity Training Methods: A Literature Review. In *Human Aspects of Information Security and Assurance, Proceedings of the 15th IFIP WG 11.12 International Symposium, HAISA 2021*; Virtual, 7–9 July 2021, Springer: Cham, Switzerland, 2021; pp. 102–112.
61. Maurer, C.; Summer, M.; Mazzola, D.; Pearson, K.; Jacks, T. The Cybersecurity Skills Survey: Response to the 2020 SIM IT Trends Study. In Proceedings of the SIGMIS-CPR'21: 2021 on Computers and People Research Conference, Virtual, 30 June 2021; ACM: Hamburg, Germany, 2021; pp. 35–37.
62. Ahmad, K.C.A.; Desouza, S.B.; Manyard, H.N.; Baskerville, R.L. How integration of cyber security management and incident response enables organizational learning. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 939–953. [[CrossRef](#)]
63. McNulty, M.; Kettani, H. On Cybersecurity Education for Non-technical Learners. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; IEEE: New York, NY, USA, 2020; pp. 413–416.
64. Dahlström, C.; Nistotskaya, M.; Tyrberg, M. Outsourcing, bureaucratic personnel quality and citizen satisfaction with public services. *Public Adm.* **2018**, *96*, 218–233. [[CrossRef](#)]
65. Affan, Y.; Lin, L.; Rubia, F.; Wang, J. Improving software security awareness using a serious game. *IET Softw. Spec. Issue Gamification Persuas. Games Softw.* **2019**, *13*, 159–169.
66. Rubia, F.; Affan, Y.; Lin, L.; Wang, J. Strategies for counteracting social engineering attacks. *Comput. Fraud. Secur.* **2022**, *2022*, 15–19. [[CrossRef](#)]
67. Aragão, J.P.S.; Fontana, M.E. Guidelines for public sector managers on assessing the impact of outsourcing on business continuity strategies: A Brazilian case. *J. Glob. Oper. Strateg. Sourc.* **2023**, *16*, 118–141. [[CrossRef](#)]
68. Gowun, P.; Brunjes, B.M. Engaging Citizens in Government Contracting: A Theoretical Approach for the Role of Social Service Nonprofits. *Perspect. Public Manag. Gov.* **2022**, *5*, 317–329.
69. Heikkilä, J.; Cordon, C. Outsourcing: A core or non-core strategic management decision? *Brief. Entrep. Financ.* **2022**, *11*, 183–193. [[CrossRef](#)]
70. Pavelko, O.; Lazaryshyna, I.; Dukhnovska, L.; Sharova, S.; Oliinyk, T.; Donenko, I. Construction Development and Its Impact on the Construction Enterprises Financial Results. *Stud. Appl. Econ.* **2021**, *39*, 1–11. [[CrossRef](#)]
71. Aragão, J.P.S.; Fontana, M.E. Outsourcing Strategies in Public Services under Budgetary Constraints: Analysing Perceptions of Public Managers. *Public Organ. Rev.* **2021**, *22*, 61–77. [[CrossRef](#)]
72. Latif, M.N.A.; Aziz, N.A.A.; Hussin, N.S.N.; Aziz, Z.A. Cyber security in supply chain management: A systematic review. *LogForum* **2021**, *17*, 49–57. [[CrossRef](#)]
73. Repetto, M.; Carrega, A.; Rapuzzi, R. An architecture to manage security operations for digital service chains. *Future Gener. Comput. Syst.* **2021**, *115*, 251–266. [[CrossRef](#)]
74. Marco-Simó, J.M.; Pastor-Collado, J.A. IT Outsourcing in the Public Sector: A Descriptive Framework from a Literature Review. *J. Glob. Inf. Technol. Manag.* **2020**, *23*, 25–52. [[CrossRef](#)]
75. van der Wal, Z. Being a Public Manager in Times of Crisis: The Art of Managing Stakeholders, Political Masters, and Collaborative Networks. *Public Adm. Rev.* **2020**, *80*, 759–764. [[CrossRef](#)] [[PubMed](#)]
76. Rizwan, H.; Bhatti, S.N. Impacts of Outsourcing on Quality: A Case Study of an Electronics Sector. *Bahria Univ. J. Manag. Technol.* **2020**, *2*, 16–23.
77. Bogoviz, A.V.; Berezhnoi, A.V.; Mezhev, I.S.S.; Titova, O.V.; Kryukova, O.G. Decision Making in Modern Business Systems by the Principles of Outsourcing. In *Specifics of Decision Making in Modern Business Systems*; Emerald Publishing Limited: Leeds, UK, 2019; pp. 141–148.
78. Bloomfield, K.; Williams, T.; Bovis, C.; Merali, Y. Systemic risk in major public contracts. *Int. J. Forecast.* **2019**, *35*, 667–676. [[CrossRef](#)]
79. Proscovia, S. The impact of new public management through outsourcing on the management of government information: The case of Sweden. *Rec. Manag. J.* **2019**, *29*, 134–151.
80. Andersson, F.; Jordahl, H.; Josephson, J. Outsourcing Public Services: Contractibility, Cost, and Quality. *CESifo Econ. Stud.* **2019**, *65*, 349–372. [[CrossRef](#)]
81. Soliño, A.S. Sustainability of Public Services: Is Outsourcing the Answer? *Sustainability* **2019**, *11*, 7231. [[CrossRef](#)]

82. Lobao, L.; Gray, M.; Cox, K.; Kitson, M. The shrinking state? Understanding the assault on the public sector. *Camb. J. Reg. Econ. Soc.* **2018**, *11*, 389–408. [\[CrossRef\]](#)
83. Aswini, K. Advantages and Disadvantages of Outsourcing. *Shanlax Int. J. Commer.* **2018**, *6*, 7–9.
84. Pupion, P.-C. Research on Public Strategic Management requiring a new theoretical framework. *Gest. Manag. Public* **2018**, *6*, 6–13.
85. Kekez, A.; Howlett, M.; Ramesh, M. Varieties of collaboration in public service delivery. *Policy Des. Pract.* **2018**, *1*, 243–252. [\[CrossRef\]](#)
86. Johansson, T.; Siverbo, S. The relationship between supplier control and competition in public sector outsourcing. *Financ. Account. Manag. Gov. Public Serv. Charities* **2018**, *34*, 268–287. [\[CrossRef\]](#)
87. Burnes, B.; Anastasiadis, A. Outsourcing: A public-private sector comparison. *Supply Chain Manag. Int. J.* **2016**, *8*, 355–366. [\[CrossRef\]](#)
88. Tayauova, G. Advantages and disadvantages of outsourcing: Analysis of outsourcing practices of Kazakhstan banks. *Procedia-Soc. Behav. Sci.* **2012**, *41*, 188–195. [\[CrossRef\]](#)
89. Schmid, A.U.; Knudsen, S.; Niehoff, T.; Schwietz, K. Planning Distributed Security Operations Centers in Multi-Cloud Landscapes A Systematic Approach, Generalized from A Case Study. *Res. Sq.* **2023**, 1–18. [\[CrossRef\]](#)
90. Saraiva, M.; Mateus-Coelho, N. CyberSoc Framework a Systematic Review of the State-of-Art. *Procedia Comput. Sci.* **2022**, *204*, 961–972. [\[CrossRef\]](#)
91. Shutock, M.; Dietrich, G. Security Operations Centers: A Holistic View on Problems and Solutions. In Proceedings of the 55th Hawaii International Conference on System Sciences, Virtual, 4–7 January 2022.
92. Georgiadou, A.; Mouzakitis, S.; Bounas, K.; Askounis, D. A Cyber-Security Culture Framework for Assessing Organization Readiness. *J. Comput. Inf. Syst.* **2022**, *62*, 452–462. [\[CrossRef\]](#)
93. Dun, Y.T.; Razak, M.F.A.; Zolkiplib, M.F.; Bee, T.F.; Firdaus, A. Grasp on next generation security operation centre (NGSOC): Comparative study. *Int. J. Nonlinear Anal. Appl.* **2022**, *12*, 869–895.
94. Nugraha, I. A Review on the Role of Modern SOC in Cybersecurity Operations. *Int. J. Curr. Sci. Res. Rev.* **2021**, *4*, 408–414. [\[CrossRef\]](#)
95. Kokulu, F.B.; Soneji, A.; Bao, T.; Shoshitaishvili, Y.; Zhao, Z.; Doupe, A.; Ahn, G. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In Proceedings of the CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; ACM: New York, NY, USA, 2019; pp. 1955–1970.
96. Benzaghta, M.A.; Elwalda, A.; Mousa, M.M.; Erkan, I.; Rahman, M. SWOT analysis applications: An integrative literature review. *J. Glob. Bus. Insights* **2021**, *6*, 55–73. [\[CrossRef\]](#)
97. Pasaribu, R.D.; Shalsabila, D.; Djatmiko, T. Revamping business strategy using Business Model Canvas (BMC), SWOT analysis, and TOWS matrix. *Herit. Sustain. Dev.* **2023**, *5*, 1–18. [\[CrossRef\]](#)
98. Hattangadi, V. SWOT & TOWS are Effective Tools for Strategic Formulation. *Eur. Econ. Lett.* **2023**, *13*, 977–981.
99. Wilson, K.S.; Kiy, M.A. Some Fundamental Cybersecurity Concepts. *IEEE Access* **2014**, *2*, 116–124. [\[CrossRef\]](#)
100. CIS. *CIS Critical Controls (R)*; Center for Internet Security: New York, NY, USA, 2021.
101. NIST. *Framework for Improving Critical Infrastructure Cybersecurity v1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
102. NIST. *Security and Privacy Controls for Information Systems and Organizations*; SP 800-53 Rev. 5; NIST: Gaithersburg, MD, USA, 2020.
103. Center for Internet Security. *CIS Community Defense Model v2.0*; Center for Internet Security: New York, NY, USA, 2021.
104. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *MITRE ATT and CK(C): Design and Philosophy*; Defense Technical Information Center: Fort Belvoir, VA, USA, 2018.
105. Kwon, R.; Ashley, T.; Castleberry, J.; McKenzie, P.; Gourisetti, S.N.G. Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. In Proceedings of the 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 19–23 October 2020; IEEE: New York, NY, USA, 2020; pp. 106–112.
106. Deng, S.; Guan, X.; Xu, J. The cooperation effect of learning-by-doing in outsourcing. *Int. J. Prod. Res.* **2021**, *59*, 516–541. [\[CrossRef\]](#)
107. Hamburg, I. Interdisciplinary Training and Mentoring for Cyber Security in Companies. In *Handbook of Research on Cyber Crime and Information Privacy*; IGI Global: Hershey, PA, USA, 2021; pp. 356–371.
108. Burrell, D.N. Assessing the value of executive leadership coaches for cybersecurity project managers. *Int. J. Hum. Cap. Inf. Technol. Prof.* **2019**, *10*, 20–32. [\[CrossRef\]](#)
109. John, S.N.; Noma-Osaghae, E.; Oajide, F.; Okokpujie, K. *Cybersecurity Education: The Skills Gap, Hurdle!* In *Innovations in Cybersecurity Education*; Springer: Cham, Switzerland, 2020; pp. 361–376.
110. Corradini, I. Training Methods. In *Building a Cybersecurity Culture in Organizations*; Studies in Systems, Decision and Control; Springer: Cham, Switzerland, 2020; Volume 284, pp. 115–133.
111. Monzelo, P.; Nunes, S. The Role of the Chief Information Security Officer (CISO) in Organizations. In *CAPSI 2019 Proceedings*; CAPSI: Toronto, ON, Canada, 2019; pp. 1–14.
112. Badhwar, R. *See Something, Do Something!* In *The CISO's Transformation*; Springer: Cham, Switzerland, 2021; pp. 45–53.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

6

DETECCIÓN Y MITIGACIÓN DE CIBERAMENAZAS USANDO VNFs EN SDNs

En esta sección se presenta un artículo derivado de la participación del autor en el proyecto "SmartNet5G: Desarrollo de nuevos mecanismos de gestión en redes programables de próxima generación" (IB18003). Dentro de las líneas de trabajo del proyecto, se exploraron las posibilidades y técnicas aplicables mediante la Virtualización de Funciones de Red (NFV) sobre Redes Definidas por Software (SDN) en la gestión de redes de comunicaciones. El artículo describe el desarrollo de un algoritmo para detectar y mitigar ataques de denegación de servicio a nivel de red. El algoritmo se basa en la caracterización del tráfico mediante el análisis estadístico de la entropía de los datagramas, identificando patrones anómalos que puedan representar una amenaza. Ante un ataque detectado, el elemento de red redirige el tráfico malicioso a una función de red virtualizada encargada de su filtrado. Para la investigación, se creó un entorno experimental con proyectos de software libre para simular una red SDN/NFV, emular un ataque y detectarlo. Los resultados demostraron la capacidad del sistema para discriminar y mitigar el tráfico de ataques de denegación de servicio, evidenciando la viabilidad de aplicar lógica de ciberseguridad en arquitecturas SDN/NFV.

Este resultado de investigación contribuye al objetivo de la tesis O3, definido en el apartado 1, Objetivos y metodología de investigación.

Referencia: M. Domínguez-Dorado, J. Calle-Cancho, J. Galeano-Brajones, F. J. Rodríguez-Pérez, and D. Cortés-Polo, “*Detection and mitigation of security threats using virtualized network functions in software-defined networks*”. *Applied Sciences*, vol. 14, no. 1, p. 374, 2023. <https://doi.org/10.3390/app14010374>.

Factor de impacto de la publicación (JIF) en JCR 2023: 2.5

Categoría: CHEMISTRY, MULTIDISCIPLINARY. Ranking JIF: 114/230 (Q2).

Categoría: ENGINEERING, MULTIDISCIPLINARY. Ranking JIF: 44/79 (Q1).

Categoría: MATERIALS SCIENCE, MULTIDISCIPLINARY. Ranking JIF: 257/438 (Q3).

Categoría: PHYSICS, APPLIED. Ranking JIF: 87/179 (Q2).

Licencia: <https://creativecommons.org/licenses/by/4.0/>

© 2024 Los autores.

Article

Detection and Mitigation of Security Threats Using Virtualized Network Functions in Software-Defined Networks

Manuel Domínguez-Dorado ¹, Jesús Calle-Cancho ^{2,*}, Jesús Galeano-Brajones ²,
Francisco-Javier Rodríguez-Pérez ² and David Cortés-Polo ²

- ¹ Department of Domains, Systems and Digital Toolkit, Public Business Entity Red.es., 28020 Madrid, Spain; manuel.dominguez@red.es
- ² Department of Computing and Telematics Engineering, Universidad de Extremadura, Avd. Universidad S/N, 10003 Cáceres, Spain; jgaleanobra@unex.es (J.G.-B.); fjrodri@unex.es (F.-J.R.-P.); dcorpola@unex.es (D.C.-P.)
- * Correspondence: jesus calle@unex.es

Abstract: The evolution of interconnected systems and the evolving demands in service requirements have led to data centers integrating multiple heterogeneous technologies that must coexist. Consequently, the resource management and the security of the infrastructure are becoming more complex than in traditional scenarios. In this context, technologies such as Software-Defined Networking (SDN) or Network Function Virtualization (NFV) are being embraced as mechanisms that facilitate communication management. The integration of both technologies into a single framework, termed Software-Defined NFV (SDNFV) introduces a multitude of tools for managing the security of the data center's resources. This work delineates the primary characteristics of the evolution of these communication networks and their application to information security and communications within a data center. It presents an illustrative use case demonstrating the application of these next-generation technologies to detect and mitigate a security issue through virtualized network functions deployed in containers.

Keywords: NFV; SDN; security threats; detection; mitigation; dockers



Citation: Domínguez-Dorado, M.; Calle-Cancho, J.; Galeano-Brajones, J.; Rodríguez-Pérez, F.-J.; Cortés-Polo, D. Detection and Mitigation of Security Threats Using Virtualized Network Functions in Software-Defined Networks. *Appl. Sci.* **2024**, *14*, 374. <https://doi.org/10.3390/app14010374>

Academic Editor: Juan-Carlos Cano

Received: 16 December 2023

Revised: 29 December 2023

Accepted: 30 December 2023

Published: 31 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The service provision landscape has undergone a paradigm shift in recent years, driven by technological advancements and evolving user demands. Legacy networks, designed for a simpler era, are ill-equipped to address the emerging networking challenges associated with this transformation. The ubiquitous adoption of cloud computing, server virtualization, BYOD (Bring Your Own Device) environments, and the exponential growth of big data and Artificial Intelligence (AI) exemplify the new paradigms necessitating advanced network capabilities [1].

Implementing any change in conventional networks, such as adding, relocating, or removing a network device, necessitates an overhaul of the entire network configuration. Networks comprise multiple devices (switches, routers, firewalls, load balancers, etc.), often from diverse vendors, resulting in intricate configurations that demand extensive time for implementation. The evolving needs of businesses demand enhanced networking capabilities, such as increased bandwidth, Quality of Service (QoS) control, and the convergence of voice, data, and video traffic. Legacy networks lack the dynamic agility necessary to effectively manage these demands [2].

Furthermore, scalability is a major hurdle for legacy networks. Networks typically expand to accommodate new users and their data demands, but this growth often outpaces the capacity of legacy architectures. This results in a network that is increasingly overloaded and unreliable. The need for a new abstraction layer is evident, one that enables the seamless addition of new devices while minimizing the burden on network administrators.

Another significant challenge is the inability to establish consistent policies across the network. Maintaining security or QoS policies within legacy networks is an arduous task. Every network alteration requires the manual configuration of numerous devices, making it prone to errors and inconsistencies. In BYOD environments, where employees use personal mobile devices, policy enforcement becomes even more challenging, increasing the vulnerability of the corporate network to security breaches. The surge in mobile devices and users, combined with the intricacy of traditional networking, has created a perfect storm that hinders the consistent application of policy compliance mechanisms.

Therefore, a fundamental shift in network architecture is necessary to overcome the limitations of legacy infrastructure. There is a need for a more adaptable, scalable, and secure network architecture that can seamlessly integrate with the evolving landscape of service provision [3].

Thus, Software-Defined Networking (SDN) [4] and Network Functions Virtualization (NFV) [5] architectures bring numerous benefits to this new computing paradigm. Their integration under a single framework, termed Software-Defined NFV (SDNFV) [6], is an active area of research and industry focus. This unified framework capitalizes on the control inherited from SDN and the flexibility gained from NFV's virtualized functions, allowing significant improvements in security issue detection and mitigation through SDNFV. Also, they are essential tools for managing security in this paradigm [7] because they are usually complementary technologies. In general, SDNFV-based networks combine SDN's network management with NFV's virtualization of network node functions, as well as the simplification of resource and service utilization within the network.

Due to the integration of diverse technologies and protocols in network orchestration, security assumes a pivotal role in enhancing communication security through the deployment of innovative mechanisms. Traditional security measures like Intrusion Detection Systems (IDS), firewalls, and others are traditionally stationed at the network periphery to fend off external threats. However, the advent of new network architectures necessitates novel security mechanisms to fortify services and networks, such as those employed in traditional deployments [8].

Network security has become a prominent theme for both industry and academia, with a surge of interest in its implementation within SDN [8] and NFV [9] architectures. Some of these implementations take advantage of the programmability of the network by applying solutions based on machine learning to detect anomaly flows [10] or implement a softwarized IDS in the SDN network [11] or develop NFV functions as firewalls to be deployed at the edge [12].

SDNFV technologies embody a novel and sophisticated paradigm to address security issues linked with new service deployments. Varied applications can be devised to manage security concerns of services or applications within the network using the benefits of SDNFV architecture.

In this work, a threat detection and mitigation algorithm is presented that takes the advantages provided by SNDFV-based networks. The algorithm employed leverages information entropy, a fundamental concept introduced by Shannon [13], to quantify uncertainty within network traffic patterns. Information entropy has demonstrated its efficacy in characterizing information content across a multitude of domains and applications like big data, fuzzy logic, or medicine [14–17]. To measure uncertainty within the network, the algorithm calculates the entropy of four key packet parameters: source IP address, destination IP address, source port, and destination port. These entropy values subsequently serve as the foundation for initiating appropriate mitigation techniques within the network infrastructure.

The remainder of this article is organized as follows: Section 2 introduces Network Function Virtualization, Software-Defined Networks, and their relationship. Section 3 details the SDNFV network architecture used in this work, along with its design and protocol development. Section 4 presents threat detection and mitigation in an SDNFV-based network, describing the algorithm for detecting potential security issues and the

mechanisms to mitigate them using virtualized network functions in a real scenario. Finally, Section 5 provides the concluding remarks of this study.

2. Enabling Technologies in Next-Generation Network Communications: SDN and NFV

SDN technology has emerged as a new network paradigm, characterized by separating the data plane from the control plane, aiming to simplify the management and configuration of traditional networks [18]. This shift in control, previously tightly integrated into individual network devices, allows the underlying infrastructure to be abstracted for applications and network services, treating the network as a logical or virtual entity.

Figure 1 illustrates the basic architecture of SDN from a logical perspective. As depicted, the SDN architecture is divided into three layers: application, control, and infrastructure.

- **Applications Layer:** These software programs execute specific tasks within an SDN environment, supplanting and expanding functions traditionally embedded in hardware devices of a conventional network. Examples of SDN applications include load balancing, security, or traffic engineering.
- **Control Layer:** Serving as the core intelligence of an SDN network, the SDN controller receives instructions and requirements from the application layer. It translates and relays these instructions to network devices in the infrastructure layer. Centralized network management through automated SDN applications facilitates the deployment and modification of network services, making it quicker and more straightforward.
- **Infrastructure Layer:** This layer is composed of the devices, which are network components that implement open standards (e.g., OpenFlow), enabling them to control forwarding and data processing capabilities within the network.

The control plane and data plane are distinct layers resulting from the separation of control and forwarding functions, providing applications with more network state information compared with protocols used in traditional networks. This enhanced information dissemination is facilitated by the presence of the network controller proposed by SDN.

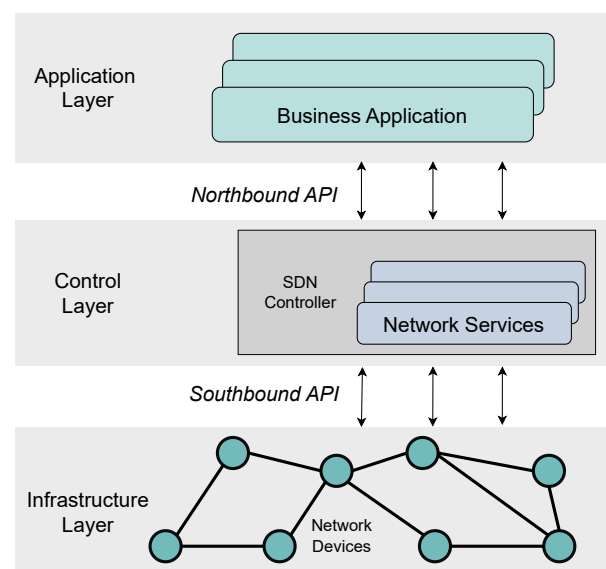


Figure 1. SDN functional architecture.

This technology provides agility, enabling dynamic flow management and optimizing resources for the changing needs of applications run by users in the cluster, which may have varying requirements in terms of features and QoS [19].

Communication and interaction between SDN components occur through APIs (Application Programming Interfaces). The API between defined SDN applications and the SDN controller is commonly referred to as the northbound API. Conversely, the API defined between the SDN controller and SDN network devices is known as the southbound API.

The SDN technology provides a series of important benefits that are outlined below:

- Improved automation and management.
- Deliver new network services quickly and easily.
- Implement a wide range of network policies.
- Reduced costs.
- Increased agility.
- Improved security.

On the other hand, NFV offers significant advantages in provisioning services in next-generation networks. This paradigm's primary goal is to decouple network functions from the physical devices on which they run.

Moreover, NFV has the potential to facilitate and enhance the deployment of new services with greater agility [20], allowing for meeting the low latency and high-reliability requirements needed by applications [21]. Typically, deploying new sophisticated network services like firewalling, load balancing, IPS (Intrusion Prevention System), IDS, routing, or WAN optimization demands the acquisition of specialized and costly hardware-based appliances by enterprises. This process also involves the installation of new equipment, which requires physical space, increases energy costs, demands specialized knowledge, and occasionally presents integration challenges. NFV seeks to revolutionize the architecture of network operators by leveraging standard virtualization technology. This transformation aims to consolidate various types of network equipment onto standard high-volume servers, switches, and storage solutions prevalent in data centers, network nodes, and end-user premises. NFV entails implementing network functions in software capable of operating on diverse industry-standard server hardware. These functions can be flexibly moved or instantiated at different locations within the network as needed, eliminating the necessity for new equipment installations.

The principal attributes of NFV encompass the following:

- **Flexibility:** NFV architecture facilitates the swift and straightforward deployment, installation, and provisioning of novel network services, thereby expediting Time-to-Market to meet the demands of businesses and users.
- **Cost-effectiveness:** NFV eliminates the requirement for costly hardware-based appliances by allowing the emulation of these devices via virtualization on standard high-volume servers, which are notably more economical.
- **Scalability:** NFV enables the deployment of new services or machines across multiple servers, obviating the necessity for additional physical space and simplifying network scalability to align with business requirements.
- **Security:** Network operators can administer and oversee the network while permitting their customers to securely manage their own virtual space and firewall within the network.
- **Ubiquity:** NFV facilitates the deployment of network services worldwide through virtualization, ensuring global availability.

Frequently, IT experts place SDN and NFV together because they share common objectives, as depicted in Figure 2. The primary aim of both SDN and NFV is to logically manage the network using software, reducing manual interaction with network devices. Hence, SDN and NFV paradigms are closely related [5], and with the efficient integration of both, significant cost savings and greater flexibility in service provisioning could be achieved. The integration of these paradigms into a single environment is known as an SDNFV network.

Finally, although both solutions are complementary, they are not mutually dependent and can be implemented separately, allowing for the deployment of SDN, NFV, or a combination of both. According to the NFV white paper [22], the objective of virtualizing network functions is to enable their use without applying SDN mechanisms, relying on the techniques currently prevalent in most data centers. However, approaches based on the separation of the control and forwarding planes, as proposed by SDN, improve

performance, simplify compatibility with existing deployments, and facilitate management and maintenance protocols.

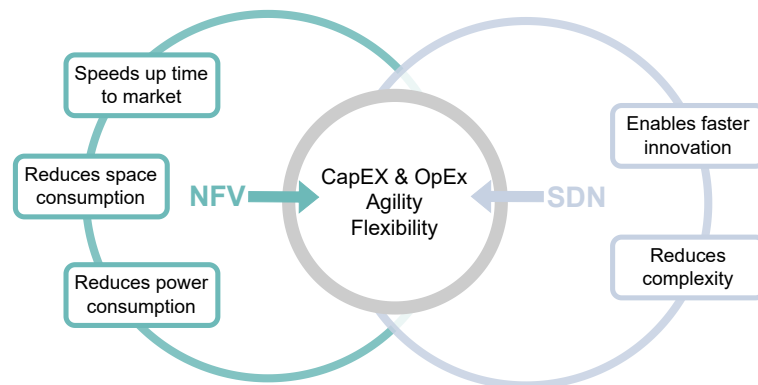


Figure 2. Relationship between SDN and NFV.

3. Security in SDNFV

Information security has perennially been a critical concern in the digital era due to the paramount value of information and the imperative need for its protection. Information security encompasses preventive and responsive measures taken by individuals, organizations, and technological systems to safeguard and preserve the confidentiality, integrity, and availability of information, often referred to as the CIA triad. This triad serves as a foundational model guiding information security policies within organizations, as outlined in ISO/IEC 27000:2018 [23]:

- Confidentiality: Ensures that information is not disclosed to unauthorized individuals, entities, or processes.
- Integrity: Ensures the accuracy and completeness of information.
- Availability: Ensures information is accessible and usable upon demand by authorized entities.

While the CIA triad represents fundamental properties in information security, additional properties like authenticity, accountability, nonrepudiation, and reliability can also be critical.

Networks play a key role in information systems, facilitating the exchange of information among various computers and resource distribution. A secure information system necessitates a secure network. The advent of novel network architectures has accommodated new business requisites; however, it has concurrently introduced fresh threats and vulnerabilities to the CIA triad that necessitate attention. For this reason, it is important to analyze vulnerabilities and threats associated with SDN and NFV architectures.

3.1. SDN Security Issues

As discussed in the previous section, the primary objective of SDN architecture is the separation of data and control planes. Consequently, the SDN architecture (refer to Figure 1) comprises three layers: the application layer, the control layer, and the infrastructure layer, each containing specific subcomponents:

- Network elements (NE) situated in the infrastructure layer.
- SDN controllers located in the control layer.
- SDN-enabled applications situated in the application layer.

While legacy networks possess a single type of component (network devices), the SDN architecture encompasses multiple elements (NE, SDN controllers, SDN applications, and northbound and southbound interfaces). Therefore, there is a need to protect not only network devices but also controllers, applications, and their communications.

Prior works [24] have analyzed each component of the SDN architecture using the Microsoft STRIDE methodology and identified potential threats to which they are vulnerable. Table 1 summarizes the potential threats.

Table 1. SDN Risks Analysis.

Attack Type	Security Property	SDN NE	SDN Controller	SDN App.
Spoofing	Authentication	Vulnerable	Vulnerable	Vulnerable
Tampering	Integrity	Vulnerable	Vulnerable	Vulnerable
Repudiation	Nonrepudiation	-	Vulnerable	-
Information Disclosure	Confidentiality	Vulnerable	Vulnerable	Vulnerable
Denial of Service (DoS)	Availability	Vulnerable	Vulnerable	Vulnerable
Elevation of Privileges	Authorization	Vulnerable	Vulnerable	-

The northbound interface (NBI) presents a significant attack vector due to the multiplicity of APIs employed by SDN controllers. These APIs leverage diverse technologies and languages, such as Python, Java, C, REST, XML, JSON, FTP, LDAP, and others. Exploiting vulnerabilities in any of these technologies or programming languages could grant an attacker control over the SDN network through the compromised controller. For instance, a compromised NBI could enable an attacker to create malicious SDN policies and manipulate the network environment.

Similarly, the southbound interface (SBI) constitutes a potential attack vector. Numerous APIs and protocols facilitate communication between the controller and network elements. These protocols include OpenFlow, Simple Network Management Protocol (SNMP), Secure Shell (SSH), NETCONF, OVSDDB (Open vSwitch Database Management Protocol), OF-Config (OpenFlow Management and Configuration Protocol), etc. While each protocol utilizes its security methods, their relative novelty and potential implementation flaws leave them vulnerable. An attacker could exploit these vulnerabilities to modify or create malicious flows within a device's flow table, enabling the introduction of illegal traffic or the manipulation of routing for malicious purposes, such as Man-in-the-Middle (MITM) attacks.

The relative novelty of SDN and its software-based infrastructure presents a distinct challenge in terms of security. The lack of a historical record of security incidents hinders our ability to anticipate and proactively address potential attack vectors. This necessitates a proactive approach to network hardening, emphasizing robust security measures across all interfaces and protocols within the SDN architecture.

To improve the security of SDN networks, several measures can be implemented. A strategy is to secure the controller, which is considered the network's core. So, if this component is compromised, the overall functioning of the network is affected [25]. Another measure is to address the communication bottleneck between the controller and the switches, which can be exploited by attackers [26].

3.2. NFV Security Issues

In the actual networking landscape, the deployment of Virtual Network Functions (VNFs) must ensure that the robust security features inherent in legacy networks are preserved. While NFV offers numerous benefits, it also introduces new security concerns related to orchestrator and hypervisor protection, ubiquitous virtual appliances, third-party access, shared virtual machines and storage, and more.

VNFs, as network functions running on virtual machines, are susceptible to three categories of security threats:

- Generic virtualization threats: These include memory leakage, interrupt isolation, and other vulnerabilities inherent in virtualized environments.
- Threats specific to legacy network functions: These encompass existing threats previously targeted at physical network functions, such as flooding attacks and routing security vulnerabilities.
- New threats arising from the combination of virtualization and networking technologies: These threats are specific to NFV environments and exploit the unique characteristics of virtualized network functions.

The NFV security problem statement outlines these potential threats, including both novel threats and existing threats that manifest in new ways. To address these concerns, a security expert group designated by the European Telecommunications Standards Institute (ETSI) has provided comprehensive guidelines for securing NFV deployments [27]. These guidelines focus on the following key security areas:

- Topology validation and enforcement: Ensuring the network topology adheres to security policies and preventing unauthorized modifications.
- Availability of management support infrastructure: Guaranteeing the availability and integrity of critical infrastructure supporting NFV management.
- Secured boot: Implementing mechanisms that ensure only verified software is loaded during the boot process.
- Secure crash: Protecting system memory and state information in the event of a system crash.
- Performance isolation: Preventing resource starvation and ensuring fair resource allocation among VNFs.
- User/tenant authentication, authorization, and accounting (AAA): Implementing robust user and tenant authentication, authorization, and accounting mechanisms.
- Authenticated time service: Providing a reliable and tamper-proof time service for VNFs.
- Private keys within cloned images: Protecting private keys used for encryption and authentication within cloned virtual machine images.
- Backdoors via virtualized test and monitoring functions: Preventing the introduction of unauthorized backdoors through virtualized testing and monitoring functions.
- Multiadministrator isolation: Ensuring the isolation of different administrative domains to prevent unauthorized access and privilege escalation.

By implementing these security measures and adhering to best practices outlined by ETSI, network operators can leverage the benefits of NFV while mitigating potential security risks and ensuring a secure and reliable network environment.

4. Implementation of Security Mechanisms into SDNFV-Based Networks

As previously discussed, while SDN and NFV offer significant benefits for modern network architectures, they also present security challenges for the network and its data. Integrating both approaches within a unified framework, known as an SDNFV-based network, offers improved mechanisms for detecting and mitigating security threats.

Due to the combined control and flexibility advantages inherited from SDN and NFV, respectively, SDNFV has become a hot topic in both research and industry. Several technologies have emerged to implement SDNFV frameworks due to the inherent complexity of its architecture and the relationship between the two approaches.

An SDNFV-based network defines complex network services that can operate on general-purpose hardware, replacing traditional dedicated hardware designed for specific functions [28]. This integration between NFV and SDN hardware is partially achieved through the decoupled control plane and data plane in SDN. The controller managing the network's control plane orchestrates the deployment of services, selecting the optimal location for each virtualized function.

While the controller's primary function in a pure SDN architecture remains managing the control plane and directing network flows, an SDNFV-based network requires additional functionality for orchestrating network resources, deploying virtualized functions, and managing their life cycle.

From a security perspective, the controller/orchestrator plays a vital role in handling key services for attack detection and mitigation, allocating network resources for black hole creation, and analyzing traffic flows, sources, and sinks.

Figure 3 illustrates the architecture and how both paradigms interconnect through the controller/orchestrator deployed in the network. As observed in the figure, the architecture is divided into different types of interconnected nodes. There are two types of SDN switches in the proposed SDNFV network architecture.

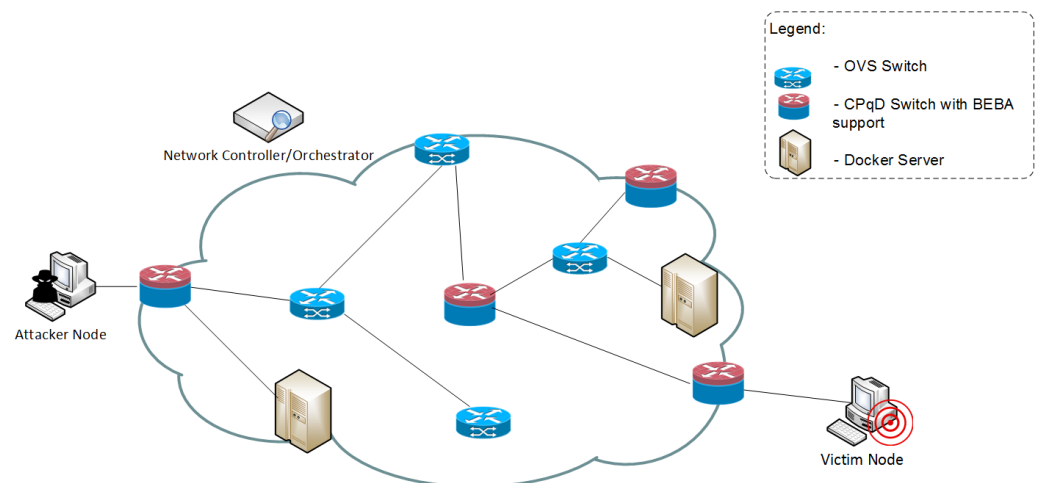


Figure 3. Proposed SDNFV network.

The first is built upon CPqD/ofsoftswitch13, which is an OpenFlow 1.3 Software Switch version executed in user space and implementing all standard functionalities. This switch has been modified by the BEHAVIOURAL-BASED forwarding (BEBA) project workgroup to introduce an extended set of actions and primitives designed to monitor network traffic and enhance communication security[29]. The BEBA approach is an open-source implementation of an OpenState controller and switch, which is available at [30]. The second type of switch utilized within this setup is the Open vSwitch (OVS), functioning as a kernel module supporting OpenFlow, effectively replacing the Linux bridge implementation.

Another integral component is the RYU OpenFlow controller, managing the control plane of both switch types to facilitate intelligent routing within the SDNFV network. For the sake of simplicity, this controller also assumes the role of an orchestrator, overseeing the management of resources within the network function virtualization infrastructure (NFVI). These functions can be split into two entities in the network to separate the controller and orchestrator functionalities.

In this architecture, the infrastructure for deploying network functions virtualized utilizes a Docker infrastructure, operating within a Docker cluster. These Docker servers are integrated into the network as nodes, accessible through various routes. All virtualized functionalities are deployed within these servers, requiring the controller to adapt routes to incorporate NFV functionalities within the network and manage interactions with the network flows.

4.1. SDN Network

As highlighted in the preceding section, the SDN network incorporates two distinct switch types. OVS switches, functioning as nonintelligent switches, primarily operate by following packet switching rules established by the controller. They are also integrated into the Docker cluster to facilitate the deployment of Dockers that implement the NFV architecture.

The CPqD switches, designed with BEBA support, embody the proposal known as OpenState [31,32]. OpenState extends the core functionalities of OpenFlow, enabling the application of diverse match-action rules based on various states detected within the SDN flow tables of the switch.

This enhanced functionality empowers the switch to respond to packet-level events by analyzing the flows being switched. If the analysis aligns with the predefined rules in the flow tables, the switch can act following those rules.

OpenState operates as an extension of OpenFlow, integrating a traditional match/action flow table with an additional state table containing flow states. BEBA-enabled switches initially match packets with states from the state table before executing the flow table to determine the subsequent actions to take. Figure 4 illustrates the architecture of OpenState.

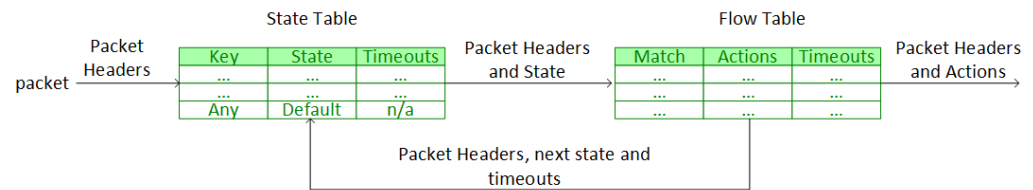


Figure 4. OpenState architecture.

4.2. NFV Architecture

The NFV architecture is implemented through the utilization of Docker containers within a cluster. For effective orchestration and deployment of virtualized functionalities, the network controller necessitates comprehensive information about the cluster, encompassing hardware details and server IPs to establish the NFVI. With these data, the controller can efficiently allocate resources and deploy virtualized functionalities.

Within this ecosystem, network functions are encapsulated within lightweight Docker containers. This containerized approach ensures the independence of function deployment from the underlying platform. Figure 5 illustrates the NFVI architecture and the virtualization of functions within this framework.

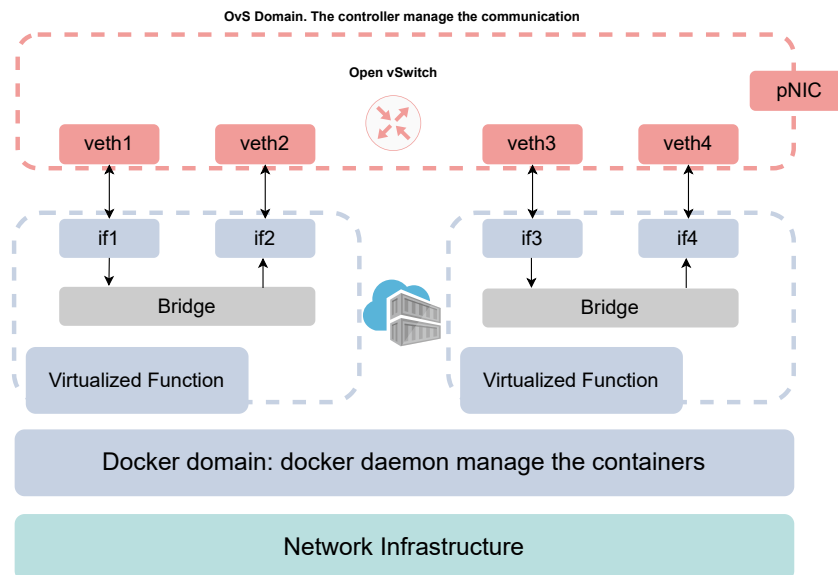


Figure 5. NFVI architecture.

The NFVI establishes connectivity with the SDNFV network via the physical network interfaces (pNIC). These interfaces facilitate packet exchange between the virtualized network functions and the SDN network. Each encapsulated virtual function within a container is equipped with two virtual network interfaces interconnected via a bridge (enabling dynamic virtual network configuration among containers using physical switch functions

for NFV infrastructure). This framework allows a small cluster to deploy numerous instances, configuring network connections and interfaces while facilitating communication between containers. Dockers implement container functionality through a file termed Dockerfile, containing instructions for automatic environment setup within a Docker image. This image, when instantiated within the NFVI, executes functions within the SDNFV network. Secure communication between the controller/orchestrator and the NFVI is ensured by encryption, facilitating the transmission of virtualized function configurations, the creation of Dockerfiles, and the deployment commands essential for NFV infrastructure.

4.3. SDNFV Controller/Orchestration

The architecture incorporates a RYU-based controller, which is a component-based SDN controller, featuring a set of predefined components essential for its functionality. These components are customizable within the controller application to adapt its behavior to specific problem requirements.

To support fundamental BEBA functionalities, various new messages, actions, and match fields must be integrated. The BEBA-supported controller extends the basic controller implementation, enabling the parsing of user-defined applications. It utilizes experimental messages to construct the application's logical model and a user-defined payload to convey essential information for traffic switching, flow decisions, or network rule execution.

The BEBA implementation has been adapted to incorporate the NFV orchestrator. It acquires information from the NFVI (in this scenario, the Docker cluster), deploys virtualized functions, and redirects traffic to the NFV. Figure 6 illustrates the comprehensive architecture of the controller/orchestrator.

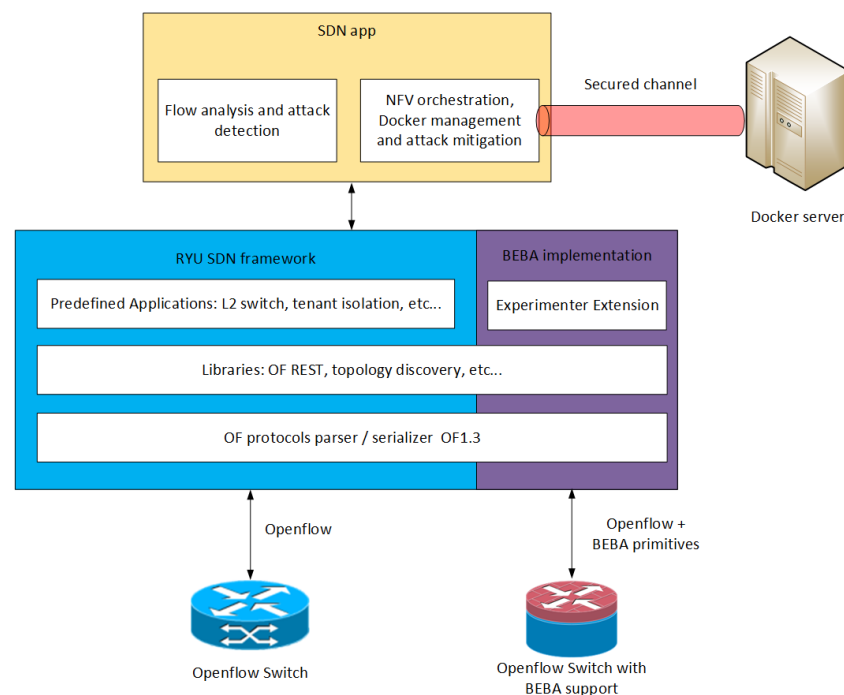


Figure 6. Architecture of the controller/orchestrator.

The RYU SDN framework is expanded through BEBA implementation utilizing the OpenFlow 1.3 protocol [33] and external libraries integrated into the original framework [34]. Notably, the SDNFV network is heterogeneous, demanding the controller to manage switches and implement a switching protocol for flow routing. OpenFlow switches with BEBA support execute normal applications (like predefined L2 switches).

The developed application built upon this framework leverages BEBA implementation to analyze flows and detect suspicious ones. Subsequently, the NFV orchestration module selects the optimal Docker server to deploy the container housing the NFV functionality.

It establishes a secure channel, executes deployment commands for the NFV, and upon successful deployment, reconfigures the flow tables to divert the identified flow to the NFV container, thus mitigating the attack.

5. Results

5.1. Detection and Mitigation

As described in the previous section, the controller/orchestrator integrates two modules designed for attack detection and mitigation. These modules are interlinked as the mitigation process necessitates detailed flow information, including source IP, source port, destination IP, destination port, and the attacking protocol. The detection module operates as a thread, routinely issuing requests to the OpenFlow switch to gather statistical information.

To obtain a response from the switch, an event handler was created to capture the messages containing the statistics' reply. These statistics undergo analysis to extract the packet's source and destination address, as well as the TCP or UDP source and destination port, to tally the different analyzed flows. Upon completing the flow analysis, entropy calculation ensues. Entropy is utilized for detecting Denial of Service (DoS) attacks by assessing statistical attributes within the packet header. Specifically, the analysis relies on comparing entropy across successive packet samples to identify an attack and can be defined as Equation (1):

$$E = - \sum_{i=1}^n p_i \log_2 p_i \quad (1)$$

where E is the entropy, n is the number of elements detected in the flow analysis, and p_i is the probability of finding the i -th element in the conjunction of elements detected in the analysis. The application of entropy allows for the analysis of multiple variables within a flow by calculating the probability that the next packets encountered have similar information that the others processed previously. The attack performed in this experiment is a UDP flood attack by the malicious node, as a result of which the entropy of the flow sent by that node will be significantly reduced once packets of the same type start to be sent to the victim over the network. Once the entropy is calculated, the detection algorithm is executed. The algorithm is based on Equations (2) to (4).

$$lower - lim = \bar{x}_p - precision * \sigma_p \quad (2)$$

$$upper - lim = \bar{x}_p + precision * \sigma_p \quad (3)$$

$$Attack = \begin{cases} false & \text{if } lower - lim \leq x \leq upper - lim \\ true & \text{otherwise} \end{cases} \quad (4)$$

where \bar{x}_p is the mean value of the analyzed elements, and $precision$ is the value used to define the precision in the detection algorithm. In this case, the values used for precision are 68% for low precision, 95% for medium precision, and 99.7% for high precision. Finally, σ_p is the standard deviation.

If an attack is detected, the controller/orchestrator searches a database containing information about the Docker cluster to select the server capable of efficiently implementing the NFV function. Once the server is chosen, the controller opens a secure channel to deploy the NFV in a Docker container. The deployment is carried out using the Dockerfile descriptor. This file describes the NFV function and the Docker's behavior. Algorithm 1 shows an example of a Dockerfile.

The Dockerfile defines the rules with which the Docker will be launched. Once the Docker container is built, the interfaces are created and the bridge between them is established. All of this is deployed on the chosen server from the Docker cluster. The controller, after completing the deployment phase, modifies the forwarding tables of the switches involved in the DoS attack communication to mitigate it. With this mechanism, the switches receiving the attack only need to forward the packets to the output port, and

the attack is mitigated using a server designed to absorb it without causing a DoS on the target node chosen by the attacker. In this case, the destination is the firewall deployed as an NFV function, a software implementation of a firewall with relevant rules to filter malicious traffic.

Algorithm 1 Example Dockerfile

```
# Firewall allowing traffic
# from port 80
FROM base
ENTRYPOINT ifinit && \
brinit && \
iptables -A FORWARD -p tcp && \
-dport 80 -j ACCEPT && \
iptables -A FORWARD -j DROP && \
/bin/bash
```

5.2. Testbed and Results

The scenario used is presented in Figure 7, and it is built on the top of Containernet and Docker servers infrastructure. As depicted in the figure, each infrastructure is deployed in a physical server interconnected by an Ethernet network.

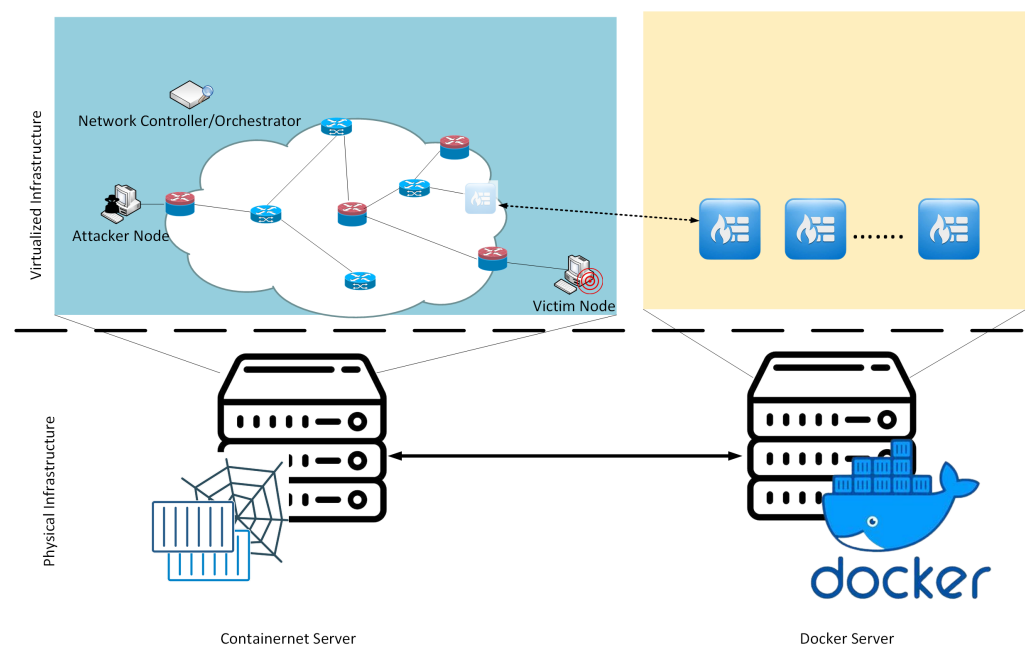


Figure 7. Scenario used to the experimental results.

The network was deployed in Containernet because it offers a fully virtualized environment based on Docker containers. These containers utilize sophisticated isolation features (e.g., Mount, UTS, IPC, PID, Network) to achieve a superior degree of sandboxing. This enhanced isolation capability is crucial to measure the resources used by the analyzed scenario.

Containernet is a fork of the widely recognized network emulator Mininet. While Mininet efficiently emulates specific use cases, its inherent limitations due to it not fully isolating emulated hosts have been a crucial issue for election.

In the scenario, a real trace with legitimate network traffic is inserted to the scenario to generate background traffic and make it difficult for the detection module of the algorithm. At around fifteen seconds, the attack is produced, and the attacker starts to generate illegitimate network traffic and send it to the victim. As can be observed in Figure 8a, the throughput is increased very quickly.

In this scenario, a real network traffic trace, obtained from project BEBA, is introduced to the environment to generate background traffic. This will complicate the algorithm’s detection process and validate the process of attack mitigation. Around fifteen seconds after the beginning of the scenario, the attacker starts to generate illegitimate network traffic and send it to the victim. As depicted in Figure 8a, there is a rapid surge in throughput observed when the attack is started. In this scenario, the network does not implement any mechanism to mitigate the attack; hence, the throughput sent to the network is maintained during the experiment. As can be observed, the experiment was repeated 15 times to avoid random events in the scenario. Compared with the experiment with a mitigation mechanism based on the entropy analysis of the flows, the average throughput reached in the network is reduced by around 8%, and the attack is mitigated in less than 5 s, as can be observed in Figure 8b. At around the eighteenth second, the traffic starts to decrease in the network.

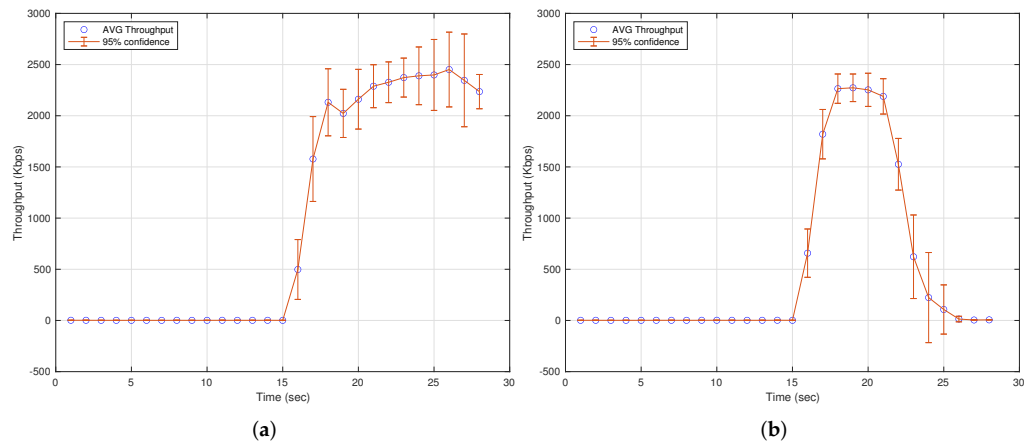


Figure 8. Network throughput: (a) scenario without any mitigation and (b) scenario with the proposed mitigation mechanism.

The entropy analysis, shown in Figure 9, studies the information stored in the controller and demonstrates the evolution of the entropy parameter in the source and destination IP address, which are the source and destination port of the attacking flow. As can be seen, when the attack is launched, the entropy level drops below the minimum, and the controller triggers the mitigation by redirecting the traffic over the network to the deployed Docker with the firewall service, which filters the packets belonging to the attack and leaves the rest of the packets that are sent and are legitimate.

Once the invalid traffic is filtered (around the twentieth second), the entropy returns to normal levels as the amount of packets sent to the victim has decreased.

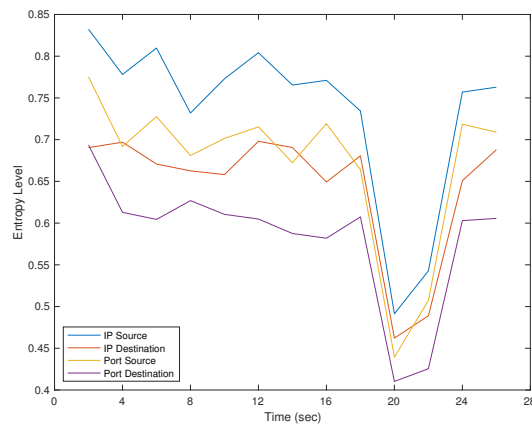


Figure 9. Entropy for each analyzed parameter.

Another of the most important parameters evaluated in this article is the average amount of CPU used in attacks, as shown in Figure 10a,b. The first shows the average CPU usage without mitigation, which is a continuous use throughout the experiment due to the need for the devices to receive the sent packets, process them, and forward them to the next hop, or attend to requests in case of a victim node. On the contrary, when the mitigation mechanism is active, it can be observed that it never reaches 100%, and the maximum CPU usage is achieved within seconds of the attack until it is detected. Additionally, it can be observed that the average CPU usage decreases once the network traffic is redirected to the virtualized NFV function.

As can be seen, the attacks analyzed in the scenario impact the network bandwidth as well as the CPU of the attacked devices. Thanks to the simplicity of the detection algorithm, it can be deployed on a controller with limited resources without impacting its normal operation. Additionally, as shown, this algorithm can detect and mitigate an attack in approximately 5 s, which is a short enough time not to saturate the CPU of the device, as shown in Figure 10.

This simple scenario allows for much greater development, where the implementation of new algorithms in the controller can analyze packets using much more complex and deep techniques, such as deep learning algorithms.

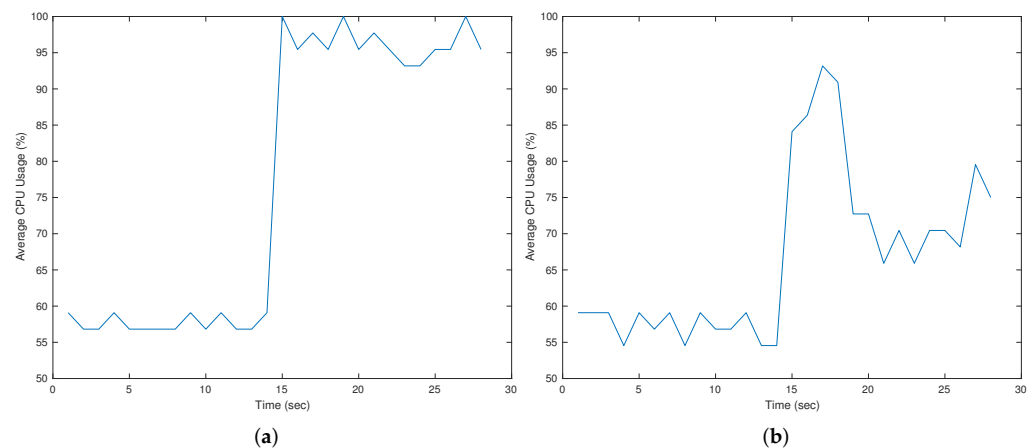


Figure 10. CPU usage: (a) without any mitigation mechanism and (b) with the proposed mitigation mechanism.

6. Conclusions

This paper introduces a novel architecture that takes advantage of the benefits introduced by SDNFV-based architecture, and it allows the detection and mitigation of DoS attacks by utilizing virtualized functions within a Docker cluster. The presented architecture represents a straightforward and cost-efficient SDN-based network that scrutinizes flows and identifies attacks through an entropy mechanism developed within the controller. This mechanism demonstrates heightened capabilities in detection and mitigation by specifically targeting the flow involved in the attack. Moreover, it can discriminate among various attributes such as IP addresses, ports, or protocols.

The framework enables the deployment of diverse virtualized functionalities, which are contingent on the application running atop the RYU controller. While this work focuses on the presentation of the firewall virtualized function, the framework's versatility allows for the deployment of other functions, such as traffic conformation, packet deep inspection, sFlow collectors, and analyzers.

The potential of the framework lies in ensuring a transparent implementation of network functionalities for end-users. Moreover, the control plane is managed by the controller/orchestrator, efficiently handling network resources to enhance overall performance.

In future works, the algorithm used to detect and mitigate the DoS attack can be extended to detect other threats, as explained in Table 1. By leveraging the network's

programmability, the advantages offered by the OpenState framework, and the adaptability of virtualized functions, numerous other scenarios can be examined utilizing this innovative architecture. Additionally, the impact in more complex scenarios will be studied in depth in future work, where a greater number of nodes will be used to deploy the infrastructure to analyze the performance of the scenarios in detail.

Author Contributions: Conceptualization, M.D.-D., J.C.-C., and D.C.-P.; Methodology, J.C.-C., D.C.-P., and F.-J.R.-P.; Software, M.D.-D., J.C.-C., D.C.-P., J.G.-B., and F.-J.R.-P. Funding acquisition, D.C.-P.; Validation, M.D.-D., J.G.-B., and D.C.-P.; Formal analysis, M.D.-D., J.C.-C., and D.C.-P.; Investigation, M.D.-D., J.C.-C., and D.C.-P.; Resources, F.-J.R.-P. and D.C.-P.; Data Curation, J.C.-C.; Writing—original draft preparation, M.D.-D., J.C.-C., and D.C.-P.; Writing—review and editing, M.D.-D., J.C.-C., D.C.-P., J.G.-B., and F.-J.R.-P.; Supervision, D.C.-P. and J.C.-C.; Project Administration, D.C.-P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by TED2021-131699B-I00AEI/10.13039/501100011033/ Unión Europea NextGenerationEU/PRTR and by the Spanish Ministry of Science and Innovation [PID2020-112545RB-C54, PDC2022-133900-I00].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: Author Manuel Domínguez-Dorado was employed by the company Department of Domains, Systems and Digital Toolkit, Public Business Entity Red.es. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Salahdine, F.; Han, T.; Zhang, N. 5G, 6G, and Beyond: Recent advances and future challenges. *Ann. Telecommun.* **2023**, *78*, 525–549. [[CrossRef](#)]
2. Anerousis, N.; Chemouil, P.; Lazar, A.A.; Mihai, N.; Weinstein, S.B. The Origin and Evolution of Open Programmable Networks and SDN. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1956–1971. [[CrossRef](#)]
3. Munther, M.N.; Hashim, F.; Abdul Latiff, N.A.; Alezabi, K.A.; Liew, J.T. Scalable and secure SDN based ethernet architecture by suppressing broadcast traffic. *Egypt. Inform. J.* **2022**, *23*, 113–126. [DOI: 10.1016/j.eij.2021.08.001](#) [[CrossRef](#)]
4. Kreutz, D.; Ramos, F.M.V.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *Proc. IEEE* **2015**, *103*, 14–76. [[CrossRef](#)]
5. Mijumbi, R.; Serrat, J.; Gorricho, J.L.; Bouten, N.; De Turck, F.; Boutaba, R. Network Function Virtualization: State-of-the-Art and Research Challenges. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 236–262. [[CrossRef](#)]
6. Wood, T.; Ramakrishnan, K.K.; Hwang, J.; Liu, G.; Zhang, W. Toward a software-based network: Integrating software defined networking and network function virtualization. *IEEE Netw.* **2015**, *29*, 36–41. [[CrossRef](#)]
7. Martinez, H.F.; Mondragon, O.H.; Rubio, H.A.; Marquez, J. Computational and Communication Infrastructure Challenges for Resilient Cloud Services. *Computers* **2022**, *11*, 118. [[CrossRef](#)]
8. Correa Chica, J.C.; Imbachi, J.C.; Botero Vega, J.F. Security in SDN: A comprehensive survey. *J. Netw. Comput. Appl.* **2020**, *159*, 102595. [DOI: 10.1016/j.jnca.2020.102595](#) [[CrossRef](#)]
9. Madi, T.; Alameddine, H.A.; Pourzandi, M.; Boukhtouta, A. NFV security survey in 5G networks: A three-dimensional threat taxonomy. *Comput. Netw.* **2021**, *197*, 108288. [[CrossRef](#)]
10. Ahmad, A.; Harjula, E.; Ylianttila, M.; Ahmad, I. Evaluation of machine learning techniques for security in SDN. In Proceedings of the 2020 IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
11. Varghese, J.E.; Muniyal, B. An Efficient IDS Framework for DDoS Attacks in SDN Environment. *IEEE Access* **2021**, *9*, 69680–69699. [[CrossRef](#)]
12. Cziva, R.; Pezaros, D.P. Container Network Functions: Bringing NFV to the Network Edge. *IEEE Commun. Mag.* **2017**, *55*, 24–31. [[CrossRef](#)]
13. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [[CrossRef](#)]
14. Jia, X.; Shang, L.; Zhou, B.; Yao, Y. An information entropy-based approach to outlier detection in rough sets. *Expert Syst. Appl.* **2010**, *37*, 6338–6344. [[CrossRef](#)]
15. Feng, G.; Li, Z.; Zhou, W.; Dong, S. Entropy-based outlier detection using Spark. *Clust. Comput.* **2020**, *23*, 409–419. [[CrossRef](#)]
16. Yuan, Z.; Chen, H.; Li, T.; Liu, J.; Wang, S. Fuzzy information entropy-based adaptive approach for hybrid feature outlier detection. *Fuzzy Sets Syst.* **2021**, *421*, 1–28. [[CrossRef](#)]

17. Combalia, M.; Codella, N.C.; Rotemberg, V.; Carrera, C.; Dusza, S.; Gutman, D. Validation of artificial intelligence prediction models for skin cancer diagnosis using dermoscopy images: The 2019 International Skin Imaging Collaboration Grand Challenge. *Lancet Digit. Health* **2022**, *4*, e659–e671. [CrossRef]
18. Nunes, B.A.A.; Mendonca, M.; Nguyen, X.N.; Obraczka, K.; Turletti, T. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1617–1634. [CrossRef]
19. Mahmoud, H.H.H.; Amer, A.A.; Ismail, T. 6G: A comprehensive survey on technologies, applications, challenges, and research problems. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4233. [CrossRef]
20. Adoga, H.U.; Pezaros, D.P. Network Function Virtualization and Service Function Chaining Frameworks: A Comprehensive Review of Requirements, Objectives, Implementations, and Open Research Challenges. *Future Internet* **2022**, *14*, 59. [CrossRef]
21. Banafaa, M.; Shayea, I.; Din, J.; Hadri Azmi, M.; Alashbi, A.; Ibrahim Daradkeh, Y.; Alhammadi, A. 6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities. *Alex. Eng. J.* **2023**, *64*, 245–274. [CrossRef]
22. ETSI. Network Functions Virtualization, White Paper. 2012. Available online: <https://www.etsi.org/technologies/nfv> (accessed on 16 December 2023).
23. ISO/IEC. ISO/IEC 27000:2018. Technical Report ISO/IEC 27000:2018. 2018. Available online: <https://www.iso.org/standard/73906.html> (accessed on 16 December 2023).
24. ONF. Threat Analysis for the SDN Architecture. Technical Report TR-530. 2016. Available online: <https://www.opennetworking.org/technical-communities/areas/services/1918-security> (accessed on 16 December 2023).
25. Siddiqui, S.; Hameed, S.; Shah, S.A.; Ahmad, I.; Aneiba, A.; Draheim, D.; Dustdar, S. Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects. *IEEE Access* **2022**, *10*, 70850–70901. [CrossRef]
26. Shen, Y.; Wu, C.; Kong, D.; Cheng, Q. Flow Table Saturation Attack against Dynamic Timeout Mechanisms in SDN. *Appl. Sci.* **2023**, *13*, 7210. [CrossRef]
27. ETSI. NFV Security Requirements. Technical Report ETSI GR NFV-SEC 001. 2013. Available online: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/001/01.01.01_60/gs_nfv-sec001v010101p.pdf (accessed on 16 December 2023).
28. Zhang, T.; Qiu, H.; Linguaglossa, L.; Cerroni, W.; Giaccone, P. NFV Platforms: Taxonomy, Design Choices and Future Challenges. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 30–48. [CrossRef]
29. Bifulco, R.; Matsiuk, A. Towards Scalable SDN Switches: Enabling Faster Flow Table Entries Installation. In Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication (SIGCOMM'15), New York, NY, USA, 17–21 August 2015; pp. 343–344. [CrossRef]
30. BEBA. BEBA Project. Available online: <https://github.com/beba-eu> (accessed on 16 December 2023).
31. Bianchi, G.; Bonola, M.; Capone, A.; Cascone, C. OpenState: Programming Platform-Independent Stateful Openflow Applications inside the Switch. *SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 44–51. [CrossRef]
32. Wazirali, R.; Ahmad, R.; Alhiyari, S. SDN-OpenFlow Topology Discovery: An Overview of Performance Issues. *Appl. Sci.* **2021**, *11*, 6999. [CrossRef]
33. OpenFlow. OpenFlow 1.3 Switch. Available online: <https://github.com/CPqD/ofsoftswitch13> (accessed on 29 December 2023).
34. Fernandes, E.L.; Rojas, E.; Alvarez-Horcajo, J.; Kis, Z.L.; Sanvito, D.; Bonelli, N.; Cascone, C.; Rothenberg, C.E. The road to BOFUSS: The basic OpenFlow userspace software switch. *J. Netw. Comput. Appl.* **2020**, *165*, 102685. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

7

CONCLUSIONES Y TRABAJO FUTURO

En este último capítulo se resumen los hallazgos y resultados de la investigación realizada en la tesis y se detallan las nuevas áreas de investigación identificadas para futuros estudios. En cuanto a los resultados, se destaca la complejidad y diversas limitaciones para adoptar un enfoque holístico de gestión y evaluación de la ciberseguridad en las entidades públicas. Se muestra cómo la solución propuesta en la tesis, centrada principalmente en aspectos metodológicos y procedimentales, pero también respaldada por soluciones tecnológicas, facilita la implementación de este enfoque en el Sector Público, mejorando su postura de ciberseguridad y aumentando el control y la concienciación sobre la protección de sus activos de negocio. En cuanto a las posibles investigaciones futuras, se identifican dos áreas de mejora significativa: el entrenamiento de la conciencia situacional en ciberseguridad de la organización para gestionar ciber crisis, y la aplicación del concepto de gemelo digital para simular escenarios de riesgo cibernético y detectar y predecir el estado de preparación de la organización ante ellos. Este capítulo no solo concluye la investigación de la tesis, sino que también abre nuevas posibilidades para expandir el modelo y hacerlo más completo.

7.1

Conclusiones

A lo largo de la tesis, se puede inferir que el diseño de un modelo de gestión y evaluación de la ciberseguridad holística, que se enfoque en los niveles tácticos y operativos y que utilice el activo de negocio como punto de referencia para aplicar medidas de ciberseguridad, es una herramienta esencial para que las entidades del Sector Público puedan abordar de manera efectiva la ciberprotección de sus operaciones. Este modelo permite una coordinación y estructuración adecuadas tanto dentro de la organización, en términos horizontales y verticales, como también en relación con las entidades de su cadena de suministro.

Partiendo de los objetivos específicos detallados en la sección “Objetivos y metodología de investigación”, se enumeran los resultados obtenidos en los siguientes párrafos:

- R1. **Referido al objetivo O1 - Diseño de un marco de trabajo para la gestión y evaluación de la ciberseguridad en el Sector Público.** En respuesta a este objetivo de la tesis, se realizó un minucioso análisis de los factores que dificultan la adopción de un enfoque integral de ciberseguridad, junto con una exhaustiva revisión de los estándares, normativas y literatura existente para evaluar cómo abordan estas dificultades los modelos actuales. El propio análisis de este ecosistema constituye por sí mismo un resultado interesante de la tesis por cuanto contribuye a ampliar el cuerpo de conocimiento de la ciberseguridad holística en el contexto de las organizaciones en general y de las entidades públicas en particular. Con sustento en este análisis, se desarrolló una base de conocimiento compartida sobre ciberseguridad holística, unificando los conceptos que deben usarse entre diferentes áreas de la organización y su cadena de suministro. Se definieron los procesos y estructuras necesarias para aplicar la ciberseguridad holística centrada en el activo de negocio, desde los niveles tácticos y operativos, involucrando a la cadena de suministro y manteniendo la coherencia con las necesidades estratégicas de ciberseguridad. Como parte de los trabajos, también se desarrollaron un conjunto de métricas de ciberseguridad holística que permitiesen evaluar los niveles de ciberseguridad y seguir el progreso hacia los objetivos estratégicos, siendo aplicables estas también a las entidades de la cadena de suministro como parte de la ciberseguridad general de la organización. Este modelo se aplicó de forma práctica en una entidad del Sector Público con resultados satisfactorios y a día de hoy continúa siendo el modelo seguido por dicha organización para la gestión holística de la ciberseguridad. Este resultado fue refrendado por la comunidad científica en la publicación asociada, como se detalla en el capítulo 2.
- R2. **Referido al objetivo O2 - Desarrollo de soluciones algorítmicas para la optimización.** Atendiendo a lo requerido por este objetivo de la tesis, durante los trabajos de investigación se exploran las aplicaciones potenciales de los algoritmos evolutivos para la optimización de la ciberseguridad. Se realizó un

análisis exhaustivo de la literatura existente sobre estos algoritmos, así como de sus variantes y aplicaciones específicas en el ámbito de la gestión de la ciberseguridad. A partir de esta esta revisión, se desarrolló un algoritmo genético de optimización multicriterio diseñado para integrarse completamente en el modelo previamente desarrollado. Este algoritmo permite una selección eficaz y rápida de acciones de ciberseguridad que se alinean con los objetivos estratégicos de la ciberseguridad holística, considerando los controles de seguridad ya implementados para permitir una aplicación gradual de medidas de ciberseguridad en la organización. Sin la aplicación de este algoritmo, el modelo desarrollado, dependiendo del conjunto de objetivos a optimizar y de las restricciones impuestas por las personas que deben aplicarlo, puede requerir un tiempo inasumible para encontrar y acordar un conjunto factible de actuaciones de ciberseguridad que permitan la consecución de los objetivos estratégicos, dado que puede haber múltiples combinaciones para ello. Las evidencias empíricas generadas durante la fase de pruebas de dicho algoritmo en la que se realizaron miles de ejecuciones, permiten afirmar que este tiempo se reduce a segundos, demostrando que la aplicación de los algoritmos evolutivos optimiza la aplicación del modelo de gestión propuesto. Este resultado fue validado por la comunidad científica en la publicación asociada, como se detalla en el capítulo 3.

- R3. **Referido al objetivo O3 - Análisis y desarrollo de soluciones tecnológicas para facilitar la implantación práctica del modelo.** Para abordar este objetivo de la tesis se realizaron dos desarrollos en los cuales se encapsuló el algoritmo genético de optimización multicriterio desarrollado. Estas soluciones consistieron en una librería diseñada para su integración en software de terceros y una aplicación gráfica destinada al uso directo por parte de organizaciones que hayan implementado el marco de gestión propuesto en esta tesis. Este software simplifica el proceso de toma de decisiones al evaluar el estado actual de ciberseguridad de los activos de negocio, establecer los objetivos estratégicos deseados y utilizar el algoritmo desarrollado para identificar conjuntos de controles de ciberseguridad necesarios para lograr dichos objetivos. Como parte de estos trabajos ambos desarrollos fueron probados en la práctica en dos organizaciones voluntarias: una perteneciente al Sector Público y otra perteneciente al sector privado del campo de la automoción, con resultados satisfactorios en ambos casos. La aplicación de estas soluciones software permitió no sólo una mayor eficiencia a estas organizaciones en la elección de controles específicos de ciberseguridad, sino que también minimizó la aparición de conflictos durante dicho proceso. La elección de uno u otro conjunto de actuaciones de ciberseguridad puede significar una mayor carga de trabajo o gasto de presupuesto para algunas áreas en relación con otras. En lugar de entrar en conflictos improductivos, el algoritmo permite hallar diversos conjuntos, de forma eficiente, sobre los que poder analizar ventajas e inconvenientes. Este resultado fue validado por la comunidad científica en la publicación asociada, como se detalla en el capítulo 4. El trabajo detallado en el capítulo 6, fruto de la colaboración paralela en un proyecto de investigación, también contribuye a este resultado.
- R4. **Referido al objetivo O4 - Diseño de extensiones metodológicas para abordar la ciberseguridad de la cadena de suministro.** Para afrontar el último de los objetivos de la tesis, se llevó a cabo una revisión detallada de la literatura

relacionada con la gestión de la ciberseguridad en el contexto de las entidades públicas. Se examinaron varios aspectos, como los fundamentos de la ciberseguridad holística, la gestión del personal operativo de ciberseguridad, el desarrollo y retención del talento en ciberseguridad, la subcontratación y externalización de servicios de ciberseguridad en el sector público. De nuevo, este análisis en sí mismo constituye un resultado interesante al aflorar toda la problemática específica de las entidades públicas en relación con la gestión de la ciberseguridad. El objeto de estos trabajos de investigación consistió en realizar un análisis profundo del caso específico de una entidad pública colaboradora relacionada con el impulso de la transformación digital, realizar un análisis del estado del arte, como se ha comentado, y analizar de forma metódica si en dicho estado del arte se reflejaban las mismas casuísticas que en la organización analizada, buscando puntos comunes que permitieran una generalización a todo el Sector Público partiendo del caso de estudio. Esta generalización, de nuevo, constituye un resultado en sí mismo y puede ser utilizada por otros investigadores como base para sus estudios. Finalmente, tras este trabajo, se desarrollaron estrategias para maximizar las capacidades de las entidades públicas en ciberseguridad holística explotando sus fortalezas en subcontratación. Se diseñaron elementos metodológicos para permitir a las entidades públicas la identificación de capacidades y habilidades requeridas para una ciberseguridad efectiva en alineación con el modelo de gestión propuesto en esta tesis y la traslación con garantías a su cadena de suministros, bien en forma de centro de operaciones de ciberseguridad externalizado, bien como requisitos de ciberseguridad para otros contratos externalizados no directamente relacionados con la ciberseguridad. Los resultados de este estudio fueron utilizados por la entidad pública que colaboró en los trabajos, permitiendo de forma satisfactoria, según las valoraciones realizadas, la identificación de requisitos de ciberseguridad y su transferencia, en modalidad de subcontratación, a su cadena de suministro. Este resultado fue refrendado por la comunidad científica en la publicación asociada, como se detalla en el capítulo 5.

7.2

Trabajo futuro

Tras la elaboración de esta tesis, se han detectado nuevas necesidades que aún no han sido abordadas en la literatura actual en el contexto del objetivo de este trabajo. Esto ha llevado a la identificación de diversas áreas de investigación futura, las cuales se describen a continuación:

- TF1. **Entrenamiento de conciencia situacional en ciberseguridad.** Los resultados de la tesis permiten a las entidades públicas identificar claramente las responsabilidades en ciberseguridad para todos los dominios funcionales de la misma, de forma que cada área funcional, formada, por personal interno o

como parte de su cadena de suministro, sepa cuál es su contribución a la ciberseguridad global de la organización. Sin embargo, en la aplicación práctica del modelo, como se describe en la publicación del capítulo 5, se ha identificado la necesidad de que los equipos multidisciplinares, mixtos (público-privados), no sólo sepan qué les corresponde hacer para la ciberseguridad desde su campo de especialización, sino que conozcan el conjunto de factores que pueden hacer más efectiva dicha contribución. Por ejemplo, el concepto proporcionalidad en la ciberseguridad, el conocimiento de la contribución que otras áreas funcionales hacen, a su vez, a la ciberseguridad holística de la organización, las distintas facetas o dimensiones de la ciberseguridad o el hecho de que el nivel de ciberseguridad de un activo de negocio pueda variar simplemente porque cambie el contexto de ciberamenazas, de forma que este estado es siempre dinámico y potencialmente volátil. Esto es especialmente necesario cuando la organización afronta un escenario de ciber crisis en el cual existe mucha presión, poco tiempo, poca información y se deben adoptar decisiones rápidas y acertadas. En este contexto el equipo multidisciplinar encargado de abordar la ciberseguridad tiene que ser capaz de interpretar el entorno, el contexto y anticipar el efecto de sus acciones no sólo respecto a la ciber crisis, sino también respecto al resto de miembros que participan desde otras áreas funcionales en el establecimiento de una ciberseguridad efectiva. Por ello, se ha identificado como una línea relevante de trabajo futuro la profundización, en el contexto del modelo propuesto en esta tesis, en el entrenamiento de las capacidades de conciencia situacional en ciberseguridad para todas las personas de la organización participantes en la misma.

- TF2. **Monitorización continua de postura de ciberseguridad de la organización respecto a riesgos concretos potenciales.** Alcanzado un nivel de madurez determinado en la organización, ésta está capacitada para autoevaluarse en cuanto a ciberseguridad con un grano muy fino, con la implantación del modelo propuesto y seguimiento de las métricas desarrolladas en la tesis. Este estado de ciberseguridad, centrado en el activo de negocio, puede ser alcanzado con la implementación de múltiples combinaciones de controles y actuaciones de ciberseguridad. También es habitual que surjan de forma continuada actores maliciosos y ciberamenazas cuyas tácticas, técnicas y procedimientos sean conocidos. Como parte de una futura mejora del modelo propuesto se ha identificado como relevante la posibilidad de que el modelo permita a la organización, no sólo la monitorización del estado de ciberseguridad de sus activos, sino ir un paso más allá y permitir conocer el grado de preparación frente a potenciales actores maliciosos o ciberamenazas concretas y, además, la identificación de qué controles holísticos sería necesario implementar para que la organización estuviese en condiciones de afrontar la materialización de dicha amenaza concreta sobre alguno de sus activos. Especialmente, es relevante profundizar en las posibilidades de aplicación del concepto de gemelo digital que permitiese mantener una versión virtual sincronizada de la organización, en términos de ciberseguridad, sobre la que poder contrastar diversos escenarios de materialización de ciberamenazas.
- TF3. **Predicciones sobre la aplicación del marco.** La tesis desarrolla un conjunto de exhaustivo de métricas que permiten conocer el efecto de las actuaciones de ciberseguridad implantadas sobre la consecución de los objetivos de

estratégicos de ciberseguridad. No obstante, como parte de la mejora del marco, se ha detectado la necesidad de desarrollar un conjunto ampliado de indicadores y métricas que permitan realizar predicciones y proyecciones sobre si los objetivos estratégicos de ciberseguridad de la organización podrán ser alcanzados en el plazo esperado, atendiendo a diversos factores como la evolución en la implantación de las distintas actuaciones de ciberseguridad, la evolución del contexto de ciberamenazas o los distintos hechos sobrevenidos (pérdida de personal especializado, cambio de prioridades organizacionales, falta de presupuesto, etcétera). Con ello, la organización sería capaz no sólo de saber en todo momento cuan cerca o lejos se encuentra de lograr los objetivos definidos, sino la probabilidad de conseguirlos en el plazo esperado, facilitando la toma de decisiones encaminadas a la corrección proactiva y temprana.

REFERENCIAS

- [1] ENISA, ENISA Threat Landscape 2023, Heraclión: European Union Agency for Cybersecurity, 2023.
- [2] CCN-CERT, "Ciberamenazas y tendencias: edición 2022," Centro Criptológico Nacional, Madrid, 2022.
- [3] H. M. Rodríguez Zambrano and C. H. Moreno Tamayo, "Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática," *Estudios y Perspectivas*, vol. 4, no. 1, pp. 159-178, 2024.
- [4] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186-202, 2024.
- [5] S. Hussein and S. Mohammed, "Analyzing the Legal Framework and Implications of Federal Decree-Law No. 34/2021 in Combatting Cyber Blackmail in the UAE," in *Proceedings of the 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 2024.
- [6] R. Davidson, "The fight against malware as a service," *Network Security*, vol. 2021, no. 8, pp. 7-1, 2021.
- [7] J. L. Worrell, "A survey of the current and emerging ransomware threat landscape," *The EDP Audit, Control, and Security Newsletter*, vol. 69, no. 2, pp. 1-11, 2024.
- [8] Z. Abou el Houda, "Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape," in *Cyber Security for Next-Generation Computing Technologies*, Boca Raton, CRC Press, 2024, pp. 84-101.
- [9] J. J. Paul Latupeirissa, N. L. Yulyana Dewi, I. K. Rian Prayana, M. Budi Srikandi, S. Aflah Ramadiansyah and I. B. Gde Agung Yoga Pramana, "Transforming Public Service Delivery: A Comprehensive Review of Digitization Initiatives," *MDPI Sustainability*, vol. 16, no. 7, pp. 1-23, 2024.
- [10] A. Shaji George, T. Baskar and P. Balaji Srikanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," *International Innovation Journal*, vol. 2, no. 1, pp. 51-75, 2024.
- [11] T. Zaid and S. Garai, "Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers," *Blockchain Health Today*, vol. 7, pp. 1-14, 2024.
- [12] V. Varma Vegesna, "Cybersecurity of Critical Infrastructure," *International machine learning journal and computer engineering*, vol. 7, no. 7, pp. 1-17, 2024.
- [13] G. Bansal and Z. Axelson, "Impact of Cybersecurity Disclosures on Stakeholder Intentions," *Journal of Computer Information Systems*, vol. 64, no. 1, pp. 78-91, 2023.
- [14] T. Komninos and D. Serpanos, "Cyberwarfare in Ukraine: Incidents, Tools and Methods," in *Hybrid Threats, Cyberterrorism and Cyberwarfare*, Boca Raton, CRC Press, 2023, pp. 1-21.

- [15] M. Oladipo Akinsanya, C. Chizoba Ekechi and C. David Okeke, "The evolution of cyber resilience frameworks in network security: A conceptual analysis," *Computer Science & IT Research Journal*, vol. 5, no. 4, pp. 926-949, 2024.
- [16] Y. Weng and J. Wu, "Fortifying the Global Data Fortress: A Multidimensional Examination of Cyber Security Indexes and Data Protection Measures across 193 Nations," *International Journal of Frontiers in Engineering Technology*, vol. 6, no. 2, pp. 13-28, 2024.
- [17] T. Oluwaseun Abrahams, S. Kuzankah Ewuga, S. Onimisi Dawodu, A. Oluwatoyin Adegbite and A. Olanipekun Hassan, "A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 1-25, 2024.
- [18] Z. Oruj, "Cyber security: contemporary cyber threats and national strategies," *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects*, vol. 1, no. 2, pp. 100-116, 2023.
- [19] W. Alec Cram and J. Yuan, "Out with the old, in with the new: examining national cybersecurity strategy changes over time," *Journal of Cyber Policy*, vol. 8, no. 1, pp. 26-47, 2023.
- [20] S. Mohamed Alhidaifi, M. Rizwan Asghar and I. Shafique Ansari, "A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 8, pp. 1-48, 2024.
- [21] P. Contreras, "The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Wales, 2023.
- [22] P. Kulkarni and K. B. Akhilesh, "Role of Cyber Security in Public Services," in *Smart Technologies*, Singapore, Springer, 2019, pp. 67-77.
- [23] W. Aman and J. Al Shukaii, "A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, pp. 1-8, 2021.
- [24] S. K V S N and A. Choudhari, "Legacy mainframe back-ends supporting new age enterprise applications: can the elephant run with deers?," in *ISEC'13: Proceedings of the 6th India Software Engineering Conference*, New Delhi, 2013.
- [25] Y. Sattarova Feruza and K. Tao-hoon, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 2, no. 2, pp. 17-32, 2007.
- [26] X. Zhang, Y. Tu Xu and L. Ma, "Information technology investment and digital transformation: the roles of digital transformation strategy and top management," *Business Process Management Journal*, vol. 29, no. 2, pp. 528-549, 2023.
- [27] R. Anderson and T. Moore, "The Economics of Information Security," *SCIENCE*, vol. 314, no. 5799, pp. 610-613, 2006.
- [28] K. Rakhima Jamshedovna and Q. Jahongir Rahim o'g'li, "Cybersecurity in the Digital Age: Safeguarding Business Assets," *Open Herald: Periodical of Methodical Research*, vol. 2, no. 3, pp. 42-45, 2024.

- [29] B. Abazi, "Establishing the National Cybersecurity (Resilience) Ecosystem," *IFAC-PapersOnLine*, vol. 55, no. 39, pp. 42-47, 2022.
- [30] N. Abbateamarco, "Cyber Capabilities as Dynamic Capabilities: Meeting the Demands of the Ever-Evolving Cybersecurity Environment," in *Proceedings of the 57th Hawaii International Conference on System Sciences*, Waikiki, 2024.
- [31] E. A. Perafán Del Campo, S. Polo Alvis, M. E. Sánchez Acevedo and A. León Quiroga , "Cyberspace: A New Frontier," in *Frontiers – Law, Theory and Cases*, Springer, 2023, pp. 89-126.
- [32] C. Catal, A. Ozcan, E. Donmez and A. Kasif, "Analysis of cyber security knowledge gaps based on cyber security body of knowledge," *Education and Information technologies*, vol. 28, no. 2023, pp. 1809-1831, 2023.
- [33] S. Furnell, "The cybersecurity workforce and skills," *Computers & Security*, vol. 100, no. 102080, pp. 1-10, 2021.
- [34] J. DeCrosta, *Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage*, (Doctoral dissertation, Utica College)., 2021.
- [35] M. S. Jalali, M. Siegel and S. Madnick, "Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment," *The Journal of Strategic Information Systems*, vol. 28, no. 1, pp. 66-82, 2019.
- [36] M. Smeets and J. D. Work, "Operational Decision-Making for Cyber Operations: In Search of a Model," *The Cyber Defense Review*, vol. 5, no. 1, pp. 95-114, 2020.
- [37] R. Dillon, P. Lothian, S. Grewal and D. Pereira, "Cyber Security: Evolving Threats in an Ever-Changing World," in *Digital Transformation in a Post-Covid World*, Boca Ratón, CRC Press, 2021, pp. 1-26.
- [38] Y. Zhiwei and J. Zhongyuan, "A Survey on the Evolution of Risk Evaluation for Information Systems Security," *Energy Procedia*, Vols. 17, Part B, pp. 1288-1294, 2012.
- [39] A. Sinha, T. H. Nguyen, D. Kar, M. Brown, M. Tambe and A. X. Jiang, "From physical security to cybersecurity," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 19-35, 2015.
- [40] A. D. Khaleefah and H. M. Al-Mashhadi, "Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review," *Iraqi Journal of Science*, vol. 65, no. 1, pp. 468-486, 2024.
- [41] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," in *International Conference On Cyber Management And Engineering (CyMaEn)*, Bangkok, Thailand, 2023.
- [42] A. Copestake, J. Estefania-Flores and D. Furceri, "Digitalization and resilience," *Research Policy*, vol. 53, no. 3, p. 104948, 2024.
- [43] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97-102, 2013.
- [44] J. van der Ham, "Toward a Better Understanding of “Cybersecurity”," *Digital Threats*, vol. 2, no. 3, article 18, 2021.

- [45] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.
- [46] ISO/IEC, "27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 2022. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en>. [Accessed 01 02 2023].
- [47] R. von Solms, "Information security management: why standards are important," *Information Management & Computer Security*, vol. 7, no. 1, pp. 50-58, 1999.
- [48] A. Henschke and S. Brandt Ford, "Cybersecurity, trustworthiness and resilient systems: guiding values for policy," *Journal of Cyber Policy*, vol. 2, no. 1, pp. 82-95, 2017.
- [49] K. Hausken, «Cyber resilience in firms, organizations and societies,» *Internet of Things*, vol. 11, n° September, 2020, p. 100204, 2020.
- [50] O. Khan and D. A. Sepúlveda Estay, "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research," *Technology Innovation Management Review*, vol. 5, no. April, pp. 6-12, 2015.
- [51] I. Linkov and A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks. Risk, Systems and Decisions*, Springer, Cham, 2019, pp. 1-25.
- [52] A. Deljoo, T. van Engers, R. Koning, L. Gommans and C. de Laat, "Towards Trustworthy Information Sharing by Creating Cyber Security Alliances," in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 2018.
- [53] H. Hakan Kilinc and U. Cagal, "A reputation based trust center model for cyber security," in *Proceedings of the 4th International Symposium on Digital Forensic and Security (ISDFS)*, Little Rock, AR, USA, 2016.
- [54] F. Olan, U. Jayawickrama, E. Ogiemwonyi Arakpogun, J. Suklan and S. Liu, "Fake news on Social Media: the Impact on Society," *Information Systems Frontiers*, vol. 26, p. 443–458, 2024.
- [55] C. Carvalho and E. Marques, "Adapting ISO 27001 to a Public Institution," in *Proceedings of the 14th Iberian Conference on Information Systems and Technologies (CISTI)*, Coimbra, Portugal, 2019.
- [56] R. Reardon and N. Choucri, "The role of cyberspace in international relations: A view of the literature," in *Proceedings of the 2012 ISA Annual Convention*, San Diego, CA, 2012.
- [57] U. M. Mbanaso and E. S. Dandaura, "The Cyberspace: Redefining A New World," *Journal of Computer Engineering*, vol. 17, no. 3, pp. 17-24, 2015.
- [58] L. Xu, Y. Li and J. Fu, "Cybersecurity Investment Allocation for a Multi-Branch Firm: Modeling and Optimization," *Mathematics*, vol. 7, no. 7, p. 567, 2019.
- [59] B. Hammi, S. Zeadally and J. Nebhen, "Security Threats, Countermeasures, and Challenges of Digital Supply Chains," *ACM Computer Surveys*, vol. 55, no. 14s, pp. 1-40, 2023.

- [60] J. K. Nwankpa and P. M. Datta, "Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers," *Computers & Security*, vol. 130, no. July 2023, p. 103266, 2023.
- [61] M. Ala, I. Obeidat, L. Abualigah, S. Alzubi and M. S. Daoud, "Intelligent cybersecurity approach for data protection in cloud computing based Internet of Things," *International Journal of Information Security*, vol. 23, p. 2123–2137, 2024.
- [62] L. Gjesvik, A. L. Khanyari, H. Bryhni, A. Arouna and N. N. Schia, "Digital Supply Chain Dependency and Resilience," in *Proceedings of the 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia, 2023.
- [63] D. A. S. Estay, R. Sahay, M. B. Barfod and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Computers & Security*, vol. 97, no. 2020, p. 101996, 2020.
- [64] Z. A. Soomro, M. H. Shah and J. Ahmed, "Information security management needs more holistic approach: A literature review," *International Journal of Information Management*, vol. 36, no. 2, pp. 215-225, 2016.
- [65] I. Atoum, A. Otoom and A. Abu Ali, "A holistic cyber security implementation framework," *Information Management & Computer Security*, vol. 2, no. 3, pp. 251-264, 2014.
- [66] R. van Kranenburg and G. Le Gars, "The Cybersecurity Aspects of New Entities Need a Cybernetic, Holistic Perspective," *International Journal of Cyber Forensic and Advanced Threat Investigations*, vol. 1, no. 63-68, p. 2, 2021.
- [67] C. Del-Real and A. M. Díaz-Fernández, "Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange," *International Cybersecurity Law Review*, vol. 3, pp. 313-343, 2022.
- [68] J. Jacob, M. Peters and T. A. Yang, "Interdisciplinary Cybersecurity: Rethinking the Approach and the Process," in *Proceedings of the National Cyber Summit (NCS) Research Track*, Huntsville, Alabama, USA, 2019.
- [69] D. Hulatt and E. Stavrou, "The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation," in *Human Aspects of Information Security and Assurance. 15th IFIP WG 11.12 International Symposium, HAISA 2021*, Virtual event, Springer, 2021, pp. 138-147.
- [70] T. Rashid and K. Chauhan, "Cyber Security in the Public Sector: Awareness of Potential Risks among Public Policy Executives," in *Security Analytics for the Internet of Everything*, Boca Ratón, CRC Press, 2020, pp. 67-91.
- [71] A. V. Bogoviz, A. V. Berezhnoi, I. S. S. Mezhov, O. V. Titova and O. G. Kryukova, "Decision Making in Modern Business Systems by the Principles of Outsourcing," in *Specifics of Decision Making in Modern Business Systems*, Emerald Publishing Limited, 2019, pp. 141-148.
- [72] L. Axon, A. Erola, A. J. van Rensburg, J. R. C. Nurse, M. Goldsmith and S. Creese, "Practitioners' Views on Cybersecurity Control Adoption and Effectiveness," in *ARES 21: Proceedings of the 16th International Conference on Availability, Reliability and Security*, Vienna, ACM ICPS, 2021, pp. 1-10.

- [73] M. Antunes, M. Maximiano and R. Gomes, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 219-238, 2021.
- [74] S. AlDaajeh and S. Alrabaei, "Strategic cybersecurity," *Computers & Security*, vol. 141, no. June 2024, p. 103845, 2024.
- [75] A. Kekez, M. Howlett and M. Ramesh, "Varieties of collaboration in public service delivery," *Policy Design and Practice*, vol. 1, no. 4, p. 243–252, 2018.
- [76] L. L. Sussman, "Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers," *Journal of Higher Education Theory and Practice*, vol. 21, no. 6, pp. 99-117, 2021.
- [77] B. Arora, "Teaching cyber security to non-tech students," *Politics*, vol. 39, no. 2, pp. 252-265, 2019.
- [78] F. Bannister, "Dismantling the silos: extracting new value from IT investments in public administration," *Information Systems Journal*, vol. 11, no. 1, pp. 65-84, 2001.
- [79] S. Bundred, "Solutions to Silos: Joining Up Knowledge," *Public Money & Management*, vol. 26, no. 2, pp. 125-130, 2006.
- [80] M. Dotterud Leiren and J. K. Steen Jacobsen, "Silos as barriers to public sector climate adaptation and preparedness: insights from road closures in Norway," *Local Government Studies*, vol. 44, no. 4, pp. 492-511, 2018.
- [81] N. Ahmad, P. A. Laplante, J. F. DeFranco and M. Kassab, "A Cybersecurity Educated Community," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 3, pp. 1456-1463, 2022.
- [82] T. De Zan, *Mitigating the cyber security skills shortage: The influence of national skills competitions on cyber security interest*, Linacre College. Department of Education and Centre for Doctoral Training in Cyber Security. University of Oxford, 2021.
- [83] F. Reeder y P. Alan, «What Works in Finding Elite Cybersecurity Talent: Promising Practices for Chief Information Officers,» CIO.org, Newport, UK, 2021.
- [84] M. Shutock and G. Dietrich, "Security Operations Centers: A Holistic View on Problems and Solutions," in *Proceedings of the 55th Hawaii International Conference on System Sciences*, Virtual event, 2022.
- [85] A. Georgiadou, S. Mouzakis, K. Bounas and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," *Journal of Computer Information Systems*, vol. 62, no. 3, pp. 452-462, 2022.
- [86] M. Saraiva and N. Mateus-Coelho, "CyberSoc Framework a Systematic Review of the State-of-Art," *Procedia Computer Science*, vol. 204, no. 1, p. 961–972, 2022.
- [87] D. Helen and Y. Sophie, "From external provision to technological outsourcing: lessons for public sector automation from the outsourcing literature," *Public Management Review*, vol. 25, no. 2, pp. 243-261, 2023.
- [88] O. Pavelko, I. Lazaryshyna, L. Dukhnovska, S. Sharova, T. Oliinyk and I. Donenko, "Construction Development and Its Impact on the Construction Enterprises Financial Results," *Studies of Applied Economics*, vol. 39, no. 3, pp. 1-11, 2021.

