



**UNIVERSIDAD DE CASTILLA-LA MANCHA
ESCUELA SUPERIOR DE INFORMÁTICA**

**MÁSTER UNIVERSITARIO
EN INGENIERÍA INFORMÁTICA**

**MM-CoUCS: Modelo de Madurez para la Concienciación de
los Usuarios finales de las organizaciones en CiberSeguridad**

Miguel de la Cal Bravo

Febrero, 2025



**UNIVERSIDAD DE CASTILLA-LA MANCHA
ESCUELA SUPERIOR DE INFORMÁTICA**

Departamento de Tecnologías y Sistemas de Información

TRABAJO FIN DE MÁSTER

**MM-CoUCS: Modelo de Madurez para la Concienciación de
los Usuarios finales de las organizaciones en CiberSeguridad**

Autor: Miguel de la Cal Bravo

Tutor: Luis Enrique Sánchez Crespo

Febrero, 2025

TRIBUNAL:

Presidente/a:

Vocal:

Secretario/a:

FECHA DE DEFENSA:

CALIFICACIÓN:

PRESIDENTE/A

VOCAL

SECRETARIO/A

RESUMEN

En el contexto actual de las organizaciones una de las principales problemáticas consiste en la concienciación y formación del personal en materia de ciberseguridad y seguridad de la información. Ante el incesante crecimiento de ciberataques, brechas de datos y fugas de información, las empresas del sector privado y las administraciones públicas deben velar por la capacitación y sensibilización de sus empleados, independientemente del sector de actividad, del cargo desempeñado o del nivel de conocimientos en tecnologías de la información y las comunicaciones, garantizando la accesibilidad e inclusión de todas las personas, bajo la premisa de que nadie quede atrás.

Tal es la importancia que ha alcanzado hoy en día la ciberseguridad que se han elaborado algunas normativas como el Esquema Nacional de Seguridad, el cual indica entre sus requisitos las necesidades de concienciación y formación en esta materia. Además, se han definido numerosas estrategias de ciberseguridad y planes a nivel europeo, nacional y regional que en los objetivos incluyen aumentar las capacidades de los usuarios finales de las organizaciones en este ámbito. No obstante, en ninguno de estos casos se llega a detallar ni profundizar en una metodología estandarizada para llevarlo a cabo con una evaluación posterior.

Debido a la tipología de los incidentes de seguridad que se producen dentro de las organizaciones, las personas son uno de los elementos más débiles y, al mismo tiempo, más importantes de la cadena de seguridad. Por ello, resulta imprescindible colaborar en el desarrollo de un ecosistema de ciberseguridad destinando los esfuerzos y recursos necesarios para poder adquirir y validar, al menos, aquellos conocimientos básicos y buenas prácticas para contrarrestar eficazmente las amenazas y riesgos existentes en el ciberespacio.

En este sentido, y mediante la realización de este trabajo, se pretende efectuar un estudio holístico de la situación de partida y desarrollar un proyecto integral que permita establecer los elementos fundamentales que debe tener un marco de trabajo o modelo de madurez de referencia para la concienciación en ciberseguridad de las personas de una organización.

ABSTRACT

In the current context of organizations, one of the main issues is staff awareness and training in cybersecurity and information security. Faced with the incessant growth of cyber-attacks, data breaches and information leaks, private sector companies and public administrations must ensure the education and consciousness of workers, regardless of the sector of activity, position or level of ICT knowledge, guaranteeing the accessibility and inclusion of everyone, preventing them from being left behind.

Such is the importance that cybersecurity has reached today that some regulations have been developed, such as the National Security Framework, which indicates among its requirements the need for awareness and training in this area. In addition, numerous cybersecurity strategies and plans have been defined at European, national and regional level, whose objectives include increasing the capabilities of the organizations' end users in this area. However, in none of these cases do they go into detail or delve into a standardized methodology to carry it out with a subsequent evaluation.

Due to the type of security incidents that occur within organizations, people are one of the weakest and, at the same time, most important elements in the security chain. Therefore, it is essential to collaborate in the development of a cybersecurity ecosystem by allocating the necessary efforts and resources to acquire and validate, at least, the basic knowledge and good practices to effectively counteract the threats and risks that exist in cyberspace.

In this sense, and through this work, the aim is to conduct a holistic study of the initial situation and develop a comprehensive project to establish the fundamental elements that a framework or reference maturity model should have for the cybersecurity awareness of an organization's personnel.

AGRADECIMIENTOS

A mi familia, por su cariño y apoyo incondicional a lo largo de las diferentes etapas de mi vida, por sus enseñanzas y valores que me han inspirado en el camino. Aunque en ocasiones les suene extraño una buena parte de la terminología aplicada en ciberseguridad y seguridad de la información, agradezco infinitamente su escucha activa y sé que, con el paso del tiempo, los esfuerzos de concienciación y sensibilización en esta materia van teniendo sus frutos.

A mis amistades y quienes me acompañan en el día a día, tanto en el ámbito personal como en el profesional, por animarme, brindarme su confianza, preocuparse por mí y compartir conmigo la alegría de celebrar cada pequeño y gran logro, haciendo que cada momento sea más especial.

Al equipo directivo y al profesorado del máster, por los conocimientos y experiencias compartidas en diversas áreas del fascinante mundo de la ingeniería informática, así como las grandes vivencias durante este periodo maravilloso en la Escuela Superior de Informática de Ciudad Real.

A mi tutor, Luis Enrique, por su amabilidad, colaboración, espíritu y naturalidad para guiarme por el buen camino durante el desarrollo del proyecto. Más allá de llevarme un valioso aprendizaje, especialmente, en el campo de la ciberseguridad gracias a su dilatada trayectoria profesional, también me quedo con la bonita oportunidad, suerte y tiempo compartido con una persona ejemplar.

Y finalmente, a todas las personas que contribuyen a hacer del ciberespacio un lugar más seguro.

Muchísimas gracias.

Miguel de la Cal Bravo

ÍNDICE GENERAL

RESUMEN	I
ABSTRACT	III
AGRADECIMIENTOS	V
ÍNDICE GENERAL	VII
ÍNDICE DE FIGURAS	IX
ÍNDICE DE TABLAS	XI
LISTADO DE ACRÓNIMOS	XIII
CAPÍTULO 1. INTRODUCCIÓN	1
1.1 Motivación.....	1
1.2 Competencias específicas	2
1.3 Estructura del documento	2
CAPÍTULO 2. OBJETIVOS	5
2.1 Objetivo General.....	5
2.2 Objetivos Parciales	5
CAPÍTULO 3. ANTECEDENTES, ESTADO DE LA CUESTIÓN.....	7
3.1 Ciberseguridad y cibercriminalidad.....	7
3.2 Factor humano e ingeniería social	10
3.3 Estrategias y planes de ciberseguridad	13
3.4 Normativas de ciberseguridad	15
3.5 Estándares y marcos de referencia en ciberseguridad.....	18
3.6 Actividades de concienciación y formación	19
3.7 Conclusiones.....	24
CAPÍTULO 4. MÉTODO DE TRABAJO	27
4.1 Metodología.....	27
4.2 Enterprise Design Thinking.....	28
4.3 Planificación temporal	34
4.4 Estimación de costes.....	36
4.5 Marco tecnológico	37
CAPÍTULO 5. RESULTADOS.....	39
5.1 Análisis PESTEL.....	39
5.2 Análisis DAFO	40
5.3 Modelo de madurez resultante.....	42
5.4 Principios rectores	44

5.5 Niveles de madurez.....	45
5.6 Ejes estratégicos	46
5.7 Líneas de acción.....	47
5.8 Criterios de éxito	51
5.9 Métricas o KPI's	53
5.10 Aplicación y evaluación del modelo	54
CAPÍTULO 6. CONCLUSIONES Y PROPUESTAS	63
6.1 Análisis de resultados obtenidos	63
6.2 Análisis de competencias adquiridas	64
6.3 Propuestas de futuro.....	65
6.4 Conclusiones y lecciones aprendidas	66
BIBLIOGRAFÍA.....	67
ANEXO A. RELACIÓN DE COMPONENTES DEL MODELO	73
ANEXO B. CRITERIOS DE ÉXITO	79
ANEXO C. RESULTADOS DEL CASO DE USO.....	99
ANEXO D. ACCESIBILIDAD DEL PROYECTO.....	105

ÍNDICE DE FIGURAS

Figura 3.1: Evolución de búsquedas del término ciberseguridad a nivel mundial.....	8
Figura 3.2: Evolución del número de vulnerabilidades con CVE	9
Figura 3.3: Evolución de búsquedas sobre el término ingeniería social a nivel mundial	10
Figura 3.4: Extracto de la matriz MITRE ATT&CK	11
Figura 3.5: Modelo de diamante extendido.....	12
Figura 4.1: Fases de Design Thinking (Stanford d.school).....	28
Figura 4.2: Viñetas de las grandes ideas	29
Figura 4.3: Mapa de empatía.....	30
Figura 4.4: Colinas.....	31
Figura 4.5: Cuadrante de prioridades	32
Figura 4.6: Expectativas y miedos	33
Figura 4.7: Cuadrante de retroalimentación.....	34
Figura 4.8: Diagrama de Gantt del proyecto	35
Figura 5.1: Análisis DAFO	41
Figura 5.2: Contexto del modelo de madurez alrededor de las personas	42
Figura 5.3: Componentes del modelo de madurez.....	43
Figura 5.4: Regla de las 5 C's con los principios rectores del modelo	44
Figura 5.5: Líneas de acción del eje 1. Ingeniería social (isoc)	49
Figura 5.6: Líneas de acción del eje 2. Programas software (sw).....	50
Figura 5.7: Líneas de acción del eje 3. Identidades digitales (id)	50
Figura 5.8: Líneas de acción del eje 4. Comportamientos en la red (red).....	51
Figura 5.9: Incidentes de seguridad por sectores	55
Figura 5.10: Diagrama de Kiviat de resultados del eje 1	59
Figura 5.11: Diagrama de Kiviat de resultados del eje 2	59
Figura 5.12: Diagrama de Kiviat de resultados del eje 3	60
Figura 5.13: Diagrama de Kiviat de resultados del eje 4	60
Figura 5.14: Resultados agregados por niveles en el eje 1.....	62
Figura 5.15: Resultados agregados por niveles en el eje 2.....	62
Figura 5.16: Resultados agregados por niveles en el eje 3.....	62
Figura 5.17: Resultados agregados por niveles en el eje 4.....	62
Figura B.1: Eje estratégico 1, líneas de acción y criterios de éxito.....	84
Figura B.2: Eje estratégico 2, líneas de acción y criterios de éxito.....	88
Figura B.3: Eje estratégico 3, líneas de acción y criterios de éxito.....	92
Figura B.4: Eje estratégico 4, líneas de acción y criterios de éxito.....	97

Figura D.1: Configuraciones de accesibilidad en documentos Microsoft	105
Figura D.2: Advertencia de problemas de accesibilidad en documentos Microsoft	105
Figura D.3: Problemas de accesibilidad a investigar en un documento	106
Figura D.4: Solución de accesibilidad para textos alternativos en figuras	107
Figura D.5: Cumplimiento de accesibilidad en el documento.....	107
Figura D.6: Cumplimiento en todos los apartados de accesibilidad.....	107
Figura D.7: Resultados de la evaluación de accesibilidad en PAC 2024	108

ÍNDICE DE TABLAS

Tabla 3.1: Número de ciberincidentes registrados en 2023	8
Tabla 3.2: Infracciones penales cometidas en o por el ciberespacio.....	9
Tabla 4.1: Planificación de sprints	35
Tabla 4.2: Remuneración de perfiles equivalentes para el proyecto	36
Tabla 4.3: Cómputo de costes directos y gastos generales	37
Tabla 4.4: Cómputo de costes totales de personal	37
Tabla 5.1: Relación de ejes y acrónimos.....	46
Tabla 5.2: Correspondencia de ejes, líneas de acción y niveles de madurez exigidos.....	47
Tabla 5.3: Criterios de éxito por ejes y niveles de madurez	52
Tabla 5.4: Evaluación de criterios de éxito en el eje 1	56
Tabla 5.5: Evaluación de criterios de éxito en el eje 2.....	57
Tabla 5.6: Evaluación de criterios de éxito en el eje 3.....	57
Tabla 5.7: Evaluación de criterios de éxito en el eje 4.....	58
Tabla 5.8: Informe final de resultados en el caso de uso	61
Tabla 6.1: Resultados obtenidos	63
Tabla A.1: Relación de componentes en el eje 1. Ingeniería social (isoc).....	74
Tabla A.2: Relación de componentes en el eje 2. Programas software (sw)	75
Tabla A.3: Relación de componentes en el eje 3. Identidades digitales (id).....	76
Tabla A.4: Relación de componentes en el eje 4. Comportamientos en la red (red)	77
Tabla B.1: Relación de métricas del criterio de éxito isoc.1.a).....	79
Tabla B.2: Relación de métricas del criterio de éxito isoc.1.b)	79
Tabla B.3: Relación de métricas del criterio de éxito isoc.1.c).....	80
Tabla B.4: Relación de métricas del criterio de éxito isoc.2.a).....	80
Tabla B.5: Relación de métricas del criterio de éxito isoc.2.b)	81
Tabla B.6: Relación de métricas del criterio de éxito isoc.2.c).....	81
Tabla B.7: Relación de métricas del criterio de éxito isoc.3.a).....	82
Tabla B.8: Relación de métricas del criterio de éxito isoc.3.b)	82
Tabla B.9: Relación de métricas del criterio de éxito isoc.4.a).....	83
Tabla B.10: Relación de métricas del criterio de éxito isoc.4.b).....	83
Tabla B.11: Relación de métricas del criterio de éxito sw.1.a).....	85
Tabla B.12: Relación de métricas del criterio de éxito sw.1.b).....	85
Tabla B.13: Relación de métricas del criterio de éxito sw.1.c).....	86
Tabla B.14: Relación de métricas del criterio de éxito sw.2.a).....	86
Tabla B.15: Relación de métricas del criterio de éxito sw.2.b).....	87

Tabla B.16: Relación de métricas del criterio de éxito sw.2.c)	87
Tabla B.17: Relación de métricas del criterio de éxito sw.2.d).....	88
Tabla B.18: Relación de métricas del criterio de éxito id.1.a).....	89
Tabla B.19: Relación de métricas del criterio de éxito id.1.b)	89
Tabla B.20: Relación de métricas del criterio de éxito id.2.a).....	90
Tabla B.21: Relación de métricas del criterio de éxito id.2.b)	90
Tabla B.22: Relación de métricas del criterio de éxito id.3.a).....	91
Tabla B.23: Relación de métricas del criterio de éxito id.3.b)	91
Tabla B.24: Relación de métricas del criterio de éxito id.3.c).....	92
Tabla B.25: Relación de métricas del criterio de éxito red.1.a).....	93
Tabla B.26: Relación de métricas del criterio de éxito red.1.b)	93
Tabla B.27: Relación de métricas del criterio de éxito red.1.c).....	94
Tabla B.28: Relación de métricas del criterio de éxito red.2.a).....	94
Tabla B.29: Relación de métricas del criterio de éxito red.2.b)	95
Tabla B.30: Relación de métricas del criterio de éxito red.3.a).....	95
Tabla B.31: Relación de métricas del criterio de éxito red.3.b)	96
Tabla B.32: Relación de métricas del criterio de éxito red.3.c).....	96
Tabla B.33: Relación de métricas del criterio de éxito red.3.d)	97
Tabla C.1: Resultados del eje 1. Ingeniería social (isoc).....	100
Tabla C.2: Resultados del eje 2. Programas software (sw)	101
Tabla C.3: Resultados del eje 3. Identidades digitales (id).....	102
Tabla C.4: Resultados del eje 4. Comportamientos en la red (red)	103

LISTADO DE ACRÓNIMOS

2FA	<i>Two-Factor authentication</i>
ACM	<i>Association for Computing Machinery</i>
APT	<i>Advanced Persistent Threat</i>
ATT&CK	<i>Adversarial Tactics, Techniques, and Common Knowledge</i>
BEC	<i>Business Email Compromise</i>
C2M2	<i>Cybersecurity Capability Maturity Model</i>
CCN	Centro Criptológico Nacional
CE	Competencia Específica
CEO	<i>Chief Executive Officer</i>
CERT	<i>Computer Emergency Response Team</i>
CISA	<i>Cybersecurity and Infrastructure Security Agency</i>
CISO	<i>Chief Information Security Officer</i>
CMMC	<i>Cybersecurity Maturity Model Certification</i>
CSF	<i>Cyber Security Framework</i>
CVE	<i>Common Vulnerabilities and Exposures</i>
DAFO	Debilidades, Amenazas, Fortalezas y Oportunidades
DGBL	<i>Digital Game-Based Learning</i>
DORA	<i>Digital Operational Resilience Act</i>
ECTS	<i>European Credit Transfer System</i>
EDR	<i>Endpoint Detection and Response</i>
EEMM	Estados Miembros
ENISA	<i>European Union Network and Information Security Agency</i>
ENS	Esquema Nacional de Ciberseguridad
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
IA	Inteligencia Artificial
IBM	<i>International Business Machines</i>
IEC	<i>International Electrotechnical Commission</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
INCIBE	Instituto Nacional de Ciberseguridad
IoT	<i>Internet of Things</i>
ISACA	<i>Information Systems Audit and Control Association</i>
ISO	<i>Internacional Organization for Standardization</i>
IVA	Impuesto sobre el Valor Añadido
JCCM	Junta de Comunidades de Castilla-La Mancha

KPI	<i>Key Performance Indicator</i>
KRI	<i>Key Risk Indicator</i>
MFA	<i>Multi-Factor Authentication</i>
MM-CoUCS	Modelo de Madurez para la Concienciación a Usuarios en CiberSeguridad
n.a.	No Aplica
NIS	<i>Network and Information Systems</i>
NIST	<i>National Institute of Standards and Technology</i>
OG	Objetivo General
OP	Objetivo Parcial
PAC	<i>PDF Accessibility Checker</i>
PDF	<i>Portable Document Format</i>
PDF/UA	<i>Portable Document Format/Universal Accessibility</i>
PESTEL	<i>Political, Economic, Social, Technological, Environmental and Legal</i>
PMV	Producto Mínimo Viable
PYME	Pequeña y mediana empresa
SANS	<i>SysAdmin, Audit, Network and Security</i>
SS	Seguridad Social
STIC	Seguridad de Tecnologías de la Información y las Comunicaciones
TFM	Trabajo Fin de Máster
TIC	Tecnologías de la Información y las Comunicaciones
TTP	Tácticas, Técnicas y Procedimientos
UCLM	Universidad de Castilla-La Mancha
UE	Unión Europea
UNE-EN	<i>Una Norma Española – European Norm</i>
VPN	<i>Virtual Private Network</i>
W3C	<i>World Wide Web Consortium</i>
WCAG	<i>Web Content Accessibility Guidelines</i>

CAPÍTULO 1. INTRODUCCIÓN

1.1 MOTIVACIÓN

En la actualidad, las organizaciones proveen una infinidad de productos y servicios a través de la red gracias a la tecnología. Como parte de un enorme proceso de transformación digital, las personas se convierten en un aspecto fundamental a la hora de adaptar sus tareas y procesos a los recursos tecnológicos existentes, los cuales permiten obtener grandes beneficios en el día a día.

No obstante, como consecuencia, los usuarios de estos organismos también se exponen a sufrir ciberataques o estafas que afloran continuamente a través de Internet y pueden afectar a la operativa del negocio. Se observa que las cifras de incidentes de ciberseguridad por fallos humanos no paran de aumentar año tras año, generando un impacto que, en determinados casos, lleva a interrumpir o poner fin a la actividad del negocio, cobrando más importancia en este sentido el factor humano.

Inicialmente, al hablar de ciberseguridad en las corporaciones se ponía el foco en el perímetro de seguridad a través de tecnologías y herramientas de protección para las comunicaciones y las redes internas corporativas, los sistemas de defensa en puestos finales de trabajo y el análisis de los eventos o registros de actividad (*logs*) de los servidores.

Ahora, ese perímetro de seguridad se ha diluido y ya no se puede concebir como antiguamente, por lo que se debe adoptar un enfoque centrado en concienciar a las personas como un elemento más de la cadena de seguridad en el uso de las tecnologías y servicios accesibles en el ciberespacio.

Al mismo tiempo, en los últimos años se han publicado normativas, estrategias y planes de ciberseguridad que tienen en común el objetivo de reforzar tanto las infraestructuras tecnológicas, como las capacidades técnicas, donde también se destaca la necesidad de concienciar y formar a las personas en este ámbito. Sin embargo, todos estos documentos también comparten el hecho de que tratan de alcanzar estos requisitos de una manera muy laxa y superficial, sin incluir una metodología de referencia para llevar a cabo las acciones de concienciación en ciberseguridad de los usuarios con su correspondiente validación en las organizaciones.

Ante esta necesidad, surgió la idea que se cubrirá en este Trabajo Fin de Máster, en adelante TFM, con el claro objetivo de poner los cimientos y realizar una propuesta detallada de un marco o modelo de madurez centrado en la concienciación en ciberseguridad de las personas en el ámbito laboral.

Mediante este modelo de madurez, se presenta una solución integral que permite cubrir los elementos y necesidades fundamentales para ayudar a fortalecer y evaluar ese *firewall* humano, en pro de mejorar la cultura y postura de seguridad de los organismos a través de la concienciación y capacitación efectiva de sus integrantes, creando también un tejido socioeconómico más resiliente.

1.2 COMPETENCIAS ESPECÍFICAS

En el marco de este TFM se trabaja en un total de cuatro competencias específicas (CE), correspondientes a la titulación de “Máster Universitario en Ingeniería Informática” de la Universidad de Castilla-La Mancha (UCLM), a lo largo del estudio y desarrollo del proyecto.

Vinculadas al módulo de dirección y gestión, se abordan las siguientes competencias:

- **[CE1]** Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.
- **[CE2]** Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.

Respecto al módulo de tecnologías informáticas, se exploran las siguientes:

- **[CE6]** Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.
- **[CE7]** Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

En el apartado 6.2 *Análisis de competencias adquiridas*, se elabora un análisis sobre la consecución de las competencias específicas indicadas anteriormente.

1.3 ESTRUCTURA DEL DOCUMENTO

El presente TFM se encuentra dividido en seis capítulos y cuatro anexos, siguiendo la estructura y el formato definido por la UCLM de la siguiente manera:

- **Capítulo 1. Introducción:** Breve introducción en la que se explica el problema a resolver, exposición de motivos y las competencias trabajadas en relación con este TFM.
- **Capítulo 2. Objetivos:** Conjunto de objetivos generales y parciales que se aspiran lograr en el desarrollo de este proyecto.

- **Capítulo 3. Antecedentes, estado de la cuestión:** Estudio holístico de la problemática actual, los conceptos principales y examen de la situación de partida.
- **Capítulo 4. Método de trabajo:** Análisis de la metodología de trabajo, planificación temporal del proyecto, estimación de costes y marco de recursos tecnológicos utilizados.
- **Capítulo 5. Resultados:** Exposición en detalle de los resultados obtenidos en el proyecto para cada uno de los elementos definidos en el modelo de madurez desarrollado.
- **Capítulo 6. Conclusiones y propuestas:** Engloba las conclusiones, análisis de resultados alcanzados incluyendo los objetivos, competencias adquiridas y propuestas de futuro.
- **Bibliografía:** Listado de referencias bibliográficas consultadas a lo largo del TFM.
- **Anexo A. Relación de componentes del modelo:** Introduce la relación de elementos que conforman el modelo, como los ejes estratégicos, líneas de acción y criterios de éxito.
- **Anexo B. Criterios de éxito:** Incluye la selección de los criterios de éxito del modelo y las métricas que aplican para el cumplimiento por cada uno de los niveles de madurez.
- **Anexo C. Resultados del caso de uso:** Comprende las tablas de resultados y valoraciones obtenidas en la aplicación y evaluación de los criterios de éxito en un caso de uso.
- **Anexo D. Accesibilidad del proyecto:** Se comprueba y valida la accesibilidad en la documentación entregada.

CAPÍTULO 2. OBJETIVOS

En este capítulo se concreta el objetivo general del proyecto y se detallan los objetivos parciales correspondientes, los cuales han sido definidos para evaluar el alcance y logro exitoso de este TFM teniendo presentes las competencias específicas a cumplir durante el desarrollo.

2.1 OBJETIVO GENERAL

El objetivo general (OG) del TFM consiste en diseñar y establecer las bases y elementos esenciales de un marco de trabajo o modelo de madurez enfocado en la concienciación de las personas de una organización en ciberseguridad, aumentando las capacidades de los empleados para hacer frente y evitar potenciales incidentes que pudieran comprometer los datos de los sistemas de información de las organizaciones.

2.2 OBJETIVOS PARCIALES

Con el propósito de abordar el objetivo general, se desglosan y establecen un conjunto de cinco objetivos parciales (OP) para la consecución del proyecto:

- [OP1] Analizar y estudiar los escenarios, tácticas, técnicas y procedimientos más frecuentes en ciberataques e incidentes de ciberseguridad sufridos por los empleados de las organizaciones en la actualidad.
- [OP2] Analizar y estudiar las principales normativas, planes y estrategias en ciberseguridad desde una perspectiva enfocada en la concienciación, sensibilización y capacitación de los usuarios finales en esta materia.
- [OP3] Diseñar y establecer las bases y fundamentos por los que se debería regir un marco de trabajo o modelo de madurez que permita fomentar la concienciación y formación en ciberseguridad del personal dentro de una organización.
- [OP4] Diseñar y establecer los elementos esenciales correspondientes como niveles, ejes, líneas de acción, medidas necesarias, métricas e indicadores.
- [OP5] Evaluar y validar el método en base a su aplicación en un caso de uso dentro del contexto de una organización.

CAPÍTULO 3. ANTECEDENTES, ESTADO DE LA CUESTIÓN

Una vez comprendidas las motivaciones y los objetivos, a continuación, se profundiza en el marco conceptual, así como en los espacios de conocimiento destacados en la actualidad, estado de la cuestión, problemática existente y situación de partida en el ámbito de la ciberseguridad.

3.1 CIBERSEGURIDAD Y CIBERCRIMINALIDAD

Para conocer la situación actual, en primer lugar, se define el concepto de ciberseguridad y se presentan algunas tendencias con datos relevantes, noticias de alto impacto en el presente y otros resultados exhibidos en informes destacados, junto con un posterior análisis en el contexto dado.

Por el término ciberseguridad, también conocido habitualmente como seguridad informática o seguridad de tecnologías de la información, el glosario de términos de ISACA [28] explica que trata sobre la protección de los activos de información haciendo frente a las amenazas a la información procesada, almacenada y transportada por sistemas de información conectados en red.

Asimismo, en otra definición, se incluye la protección y restauración de los productos, servicios, soluciones y cadena de suministro, incluida la tecnología, los ordenadores, los sistemas y servicios de telecomunicaciones y la información, para garantizar su disponibilidad, integridad, autenticación, transporte, confidencialidad y resistencia.

Más allá de las definiciones enseñadas, es preciso añadir y completar que la ciberseguridad igualmente involucra, como parte fundamental del funcionamiento de estos productos y servicios, a las personas que las utilizan en el día a día, independientemente de su nivel de conocimientos TIC y de si sus funciones se encuentran estrechamente vinculadas al campo tecnológico.

La ciberseguridad en las organizaciones hoy en día se trata de una obligación y no de una opción, ya que, no puede haber transformación digital sin incorporar la ciberseguridad desde el comienzo. Además, la seguridad de las tecnologías de la información no sólo está presente en el ámbito laboral, sino que, también, juega un papel transcendental en la vida de la ciudadanía en general.

Esto se magnifica con la llegada de la pandemia de COVID-19 y, especialmente, tras los sucesivos conflictos desatados en el este de Europa y Oriente Medio, cuando la ciberseguridad ha ido ganando protagonismo tanto dentro de la cultura de las organizaciones, como en la población a nivel mundial.

En este sentido, en la *Figura 3.1* se observa el interés año a año por el término de búsqueda de ciberseguridad obtenido desde el portal de *Google Trends*¹. En esta gráfica, se muestra una tendencia creciente, substancialmente acentuada en el año 2024 donde alcanza su máxima popularidad [20].



Figura 3.1: Evolución de búsquedas del término ciberseguridad a nivel mundial

Este interés por la ciberseguridad se ve reflejado en el Informe Anual de Seguridad Nacional 2023 [14], elaborado por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, el cual destaca la preocupación de la sociedad por las campañas de desinformación y la vulnerabilidad del ciberespacio como los dos principales riesgos para la Seguridad Nacional, estimando que esta tendencia negativa empeorará mucho durante los próximos cinco años.

Dicho informe también manifiesta un aumento en el número y severidad de los ciberataques, cuyas cifras se resumen a continuación en la *Tabla 3.1* por los principales organismos nacionales:

Organismo	Incidentes
CCN-CERT	107.777
INCIBE-CERT	83.517
ESPDEF-CERT	1.480

Tabla 3.1: Número de ciberincidentes registrados en 2023

En línea con lo anterior, y, según una campaña lanzada por el Ministerio del Interior del Gobierno de España, el número total de ciberdelitos ha ido creciendo notablemente a lo largo de los últimos años. De hecho, las cifras indican que actualmente uno de cada cinco delitos se comete en la red², identificando entre los más frecuentes aquellos que tienen que ver con sextorsiones, *phishing/smishing*, fraude del CEO, *ransomware*, comercio electrónico y estafas o fraudes del amor (*love/romance scam*).

¹ <https://trends.google.com/trends/>

² Uno de cada cinco delitos. <https://unodecadacincodelitos.com/>

De acuerdo con el informe sobre la criminalidad en España del año 2023 [31], en la *Tabla 3.2* se muestran los datos estadísticos anuales de cibercriminalidad conocidos por categorías delictivas:

Categoría delictiva	2019	2020	2021	2022	2023
Acceso e interceptación ilícita	4.004	4.653	5.342	5.578	7.367
Amenazas y coacciones	12.782	14.066	17.319	15.982	17.472
Contra el honor	1.422	1.550	1.426	1.191	1.174
Contra propiedad indust./intelec.	197	125	137	114	64
Delitos sexuales	1.774	1.783	1.628	1.646	1.804
Falsificación informática	4.275	6.289	10.476	12.569	15.137
Fraude informático	192.375	257.907	267.011	335.995	427.448
Interferencia datos y en sistema	1.473	1.590	2.138	1.662	1.659
Total de hechos conocidos	218.302	287.963	305.477	374.737	472.125

Tabla 3.2: Infracciones penales cometidas en o por el ciberespacio

De las cifras anteriores, resulta alarmante el continuo aumento de infracciones cometidas mediante fraudes informáticos, cuyo total supera los 427.000 delitos cibernéticos de este tipo en el año 2023.

Por otro lado, respecto al grave riesgo de vulneración del ciberespacio, la tecnología cada vez se encuentra más presente en las organizaciones y en nuestras vidas generando un gran impacto social. Como consecuencia, el número de vulnerabilidades registradas cada año con código CVE (*Common Vulnerabilities and Exposures*) también sigue al alza año tras año, consiguiendo rebasar la barrera de las 40.000 vulnerabilidades y batiendo de nuevo el récord en el año 2024 [10].

Más abajo, en la *Figura 3.2*, se muestra la evolución del total de vulnerabilidades notificadas con CVE por cada año [10]. En ella, se observa una tendencia acrecentada especialmente a partir del año 2020 y, por causa de este notable aumento, las organizaciones y las personas se encuentran cada vez más expuestas a ser víctimas de ciberataques a causa un uso indebido del ciberespacio.



Figura 3.2: Evolución del número de vulnerabilidades con CVE

3.2 FACTOR HUMANO E INGENIERÍA SOCIAL

Continuando con el punto anterior, uno de los aspectos destacados que más intervienen en los incidentes de ciberseguridad es el factor humano, en especial, a través de la ingeniería social.

Primeramente, debemos entender que el concepto de ingeniería social [26] se corresponde con un conjunto de técnicas que utilizan los ciberdelincuentes con el fin de ganarse la confianza de la otra persona, para que esta realice alguna acción bajo un engaño y manipulación. Algunos ejemplos pueden llevar desde la ejecución de programas dañinos, compartir credenciales y datos personales de la víctima, hasta realizar transferencias bancarias o efectuar compras en portales web ilegítimos.

Los ciberdelincuentes conocen la importancia del factor humano combinado con la ciberseguridad y las técnicas de ingeniería social, permaneciendo alerta para adaptar estas técnicas en sus estafas y, con ello, buscar continuamente hacer el mal en las entidades y la sociedad en general.

En la *Figura 3.3*, al igual que se expuso anteriormente con el término de ciberseguridad, se revela una tendencia ascendente en el interés de búsquedas acerca de la ingeniería social [21]. De nuevo, coincidiendo principalmente con la emergencia sanitaria derivada de la pandemia de COVID-19 y, como consecuencia del confinamiento mundial, cada vez más delincuentes buscaron aprovecharse de la situación para acometer fraudes a través del ciberspacio. A su vez, este aumento prosigue hasta la fecha acompañado de los acontecimientos sociales y políticos ocurridos en los últimos años.

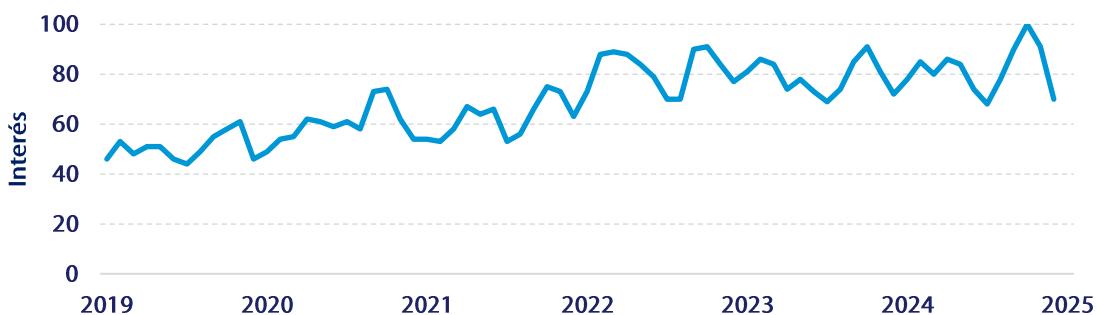


Figura 3.3: Evolución de búsquedas sobre el término ingeniería social a nivel mundial

En esta línea, una de las grandes citas que se le atribuye al famoso *hacker* Kevin Mitnick en su libro, *The Art of Deception* [32], publicado en el año 2003, nos decía ya que la ingeniería social es la mayor amenaza para la seguridad de los activos de negocio: “*What's the greatest threat to the security of your business assets? That's easy: the social engineer*”.

Esta frase, traducida en datos representativos, que han sido obtenidos de informes y noticias de actualidad, según el proveedor de ciberseguridad Kaspersky [29] se nos expone que el 64% del total de los ciberincidentes fueron causados por error humano. La multinacional Verizon [46], por su parte, indica en un informe que el componente humano causó hasta el 68% de las brechas de seguridad.

Como parte de la ingeniería social, se destaca la matriz de MITRE ATT&CK [33] por ser una base de conocimientos ampliamente utilizada que recoge las tácticas, técnicas y procedimientos (conocidos habitualmente bajo las siglas TTP's) empleados por los adversarios en observaciones del mundo real. La matriz empresarial sirve en los escenarios de ciberinteligencia para detectar y analizar las técnicas utilizadas por los grupos de amenazas y cibercriminales, estando formada actualmente por un total de 14 tácticas, más de 200 técnicas y 400 subtécnicas.

La Figura 3.4 muestra algunos ejemplos de tácticas y técnicas registradas en MITRE ATT&CK:

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Facing Application	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Brower Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication
Phishing for Information (4)	Establish Accounts (3)	Obtain Capabilities (7)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)
Search Closed Sources (2)	Phishing (4)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)
Search Open Technical Databases (5)	Supply Chain Compromise (3)	Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (5)	Direct Volume Access	Execution Guardrails (1)	Modify Authentication Process (9)
Search Open Websites/Domains (3)	Valid Accounts (4)		Serverless Execution	Event Triggered Execution (16)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception
Search Victim-Owned Websites			Shared Modules	Event Triggered Execution (16)	Event Triggered Execution (16)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation
			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Hide Artifacts (12)	Network Sniffing
			System Services (2)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	OS Credential Dumping (8)
			User Execution (3)	Implant Internal Image	Impair Defenses (11)	Impersonation	Steal Application Access Token
			Windows Management Instrumentation	Modify Authentication Process (9)	Indicator Removal (9)	Indirect Command Execution	
				Scheduled Task/Job (5)			

Figura 3.4: Extracto de la matriz MITRE ATT&CK

Según el último informe del panorama de amenazas elaborado por ENISA [15], encontramos entre las técnicas más comunes de ingeniería social en primer lugar el *phishing* (identificada bajo la técnica T1566 de MITRE ATT&CK, correspondiente a la táctica de acceso inicial), así como también el *smishing*, *spear-phishing*, *vishing*, *pretexting*, *Business Email Compromise (BEC)* y otras variantes derivadas que surgen continuamente de las anteriores. Todas ellas tienen en común el objetivo de engañar a las víctimas ganándose su confianza, para obtener sus datos personales, credenciales válidas de cuentas corporativas o, incluso, datos bancarios para robarles su dinero.

Dentro del contexto empresarial, el uso de estas técnicas en la ciberdelincuencia presenta un sinfín de oportunidades para suplantar a empresas y altos cargos que pueden suponer un vector de entrada que ocasione, en algunos casos, la revelación de información sensible o la disruptión del negocio con pérdidas multimillonarias y, en el peor caso, llevar al cierre definitivo del mismo.

Con el objetivo de analizar y modelar las amenazas e intrusiones en los sistemas de información, complementando a las TTP's establecidas en la matriz de MITRE citada anteriormente, tenemos el modelo de diamante que recoge los aspectos clave de las actividades maliciosas.

Debido a su forma de diamante, se identifica un total de cuatro elementos (uno por cada vértice) que componen los eventos de intrusiones [5]:

- Adversario: Se refiere al actor u organización que busca comprometer los sistemas de información utilizando sus capacidades contra la víctima. Existen diferentes tipos de adversarios, como un individuo interno o externo a la corporación, grupo u organización.
- Capacidades: Describe las herramientas y técnicas empleadas por el adversario en el evento, pudiendo ser métodos manuales o automatizados de una manera más sofisticada, aprovechando un arsenal o conjunto de capacidades compuestas por vulnerabilidades.
- Infraestructura: Son las estructuras de comunicación físicas y lógicas utilizadas por el adversario para proporcionar una capacidad, mantener el control de las capacidades y obtener resultados de las víctimas. Esto puede incluir, entre otros, direcciones IP, nombres de dominio, direcciones de correo electrónico y dispositivos físicos.
- Víctima: Es el objetivo del adversario, contra el que se explotan las vulnerabilidades y exposiciones de datos e información. Una víctima puede ser, entre otras, una organización, una persona, una dirección de correo electrónico o una dirección IP. El modelo distingue entre una persona víctima (persona u organización) y un activo víctima (redes y sistemas).

Estos cuatro componentes principales están unidos en forma de diamante y, de manera extendida, se resaltan las relaciones naturales a nivel sociopolítico y tecnológico en la *Figura 3.5* [5]:

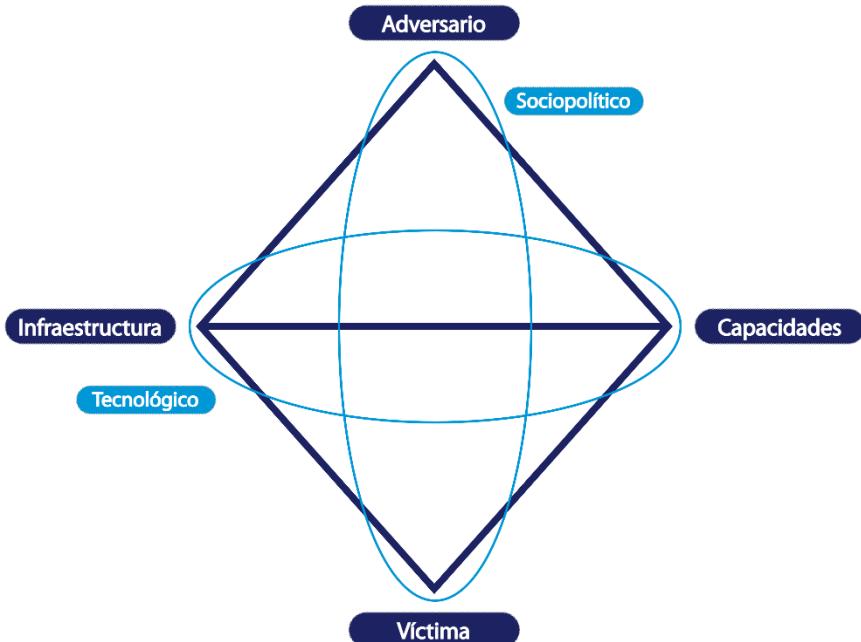


Figura 3.5: Modelo de diamante extendido

3.3 ESTRATEGIAS Y PLANES DE CIBERSEGURIDAD

Dentro del contexto estratégico se identifican y analizan los principales documentos publicados a nivel europeo, nacional y autonómico con las metas y objetivos establecidos para los próximos años.

Estrategia de Ciberseguridad de la Unión Europea

A finales del año 2020 la Comisión Europea y el Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad presentaron una nueva estrategia de ciberseguridad de la Unión Europea [16], como parte de las metas digitales para 2030 en la Década Digital de Europa.

En el documento se estima que existen 291.000 puestos vacantes de profesionales en ciberseguridad en Europa, con el objetivo añadido de reducir la brecha de género, pese a que actualmente existen procesos lentos de contratación y entrenamiento de expertos en esta materia que llevan a aumentar los riesgos de ciberseguridad para las organizaciones.

La estrategia, a través del revisado Plan de Acción de Educación Digital (2021-2027), pretende aumentar la concienciación en ciberseguridad entre las personas, especialmente menores de edad, así como las organizaciones, especialmente las pymes.

Como consecuencia del panorama cada vez más hostil con la expansión de las ciberamenazas y el impacto de ciberataques más sofisticados contra las instituciones, organismos y agencias de la Unión Europea, se plantea la necesidad de incrementar las inversiones con el objetivo de alcanzar un mayor nivel de madurez en ciberseguridad.

En este punto, se menciona que se está creando un programa de concienciación cibernetica (*Cyber Awareness Programme*) con el fin de aumentar la concienciación del personal, la higiene en el ciberespacio y apoyar una cultura común de ciberseguridad. De esta manera, queda patente la obligación de concienciar en ciberseguridad en el marco de las organizaciones.

Estrategia de Seguridad Nacional 2021

Elaborada por el Consejo de Seguridad Nacional, cuenta con la participación de los departamentos ministeriales, Centro Nacional de Inteligencia, expertos y especialistas del campo de la seguridad, así como las comunidades y ciudades autónomas.

En esta estrategia [12], se establece como el segundo objetivo favorecer la dimensión de seguridad de las capacidades tecnológicas y de los sectores estratégicos, teniendo presente los aspectos de seguridad en el desarrollo tecnológico desde el inicio. Además, considera que debe haber constantes adaptaciones y actualizaciones que afectan al ámbito regulatorio, controles de calidad y formación.

Dentro del segundo eje: “*Una España que promueve la prosperidad y el bienestar de los ciudadanos*”, se destaca la importancia de garantizar un uso del ciberespacio seguro y fiable. Para ello, es necesario aumentar las capacidades no sólo tecnológicas y económicas, sino, también, aquellas capacidades humanas para robustecer la ciberseguridad nacional.

Estrategia Nacional de Ciberseguridad 2019

Se trata de la principal estrategia de ciberseguridad dentro del panorama nacional [13], donde se profundiza más en esta materia respecto a la estrategia comentada anteriormente si bien, es cierto que no ha sido actualizada desde el año 2019. Aprobada por el Consejo de Seguridad Nacional, en su elaboración han participado los distintos ministerios, el Departamento de Seguridad Nacional y un comité de expertos de diversas asociaciones, empresas y mundo académico.

La estrategia está formada por una serie de principios rectores, objetivo general y objetivos específicos. En concreto, en el objetivo IV: “*Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas*”, se indica que es necesario contar con recursos técnicos y humanos con la capacitación adecuada para un uso más seguro del ciberespacio.

Para ello, se debe mejorar la ciberseguridad colectiva divulgando una cultura de la ciberseguridad a la ciudadanía, administraciones y empresas. Respecto a las capacidades humanas, se quiere promover la capacitación en ciberseguridad de un gran espectro de profesionales en cumplimiento con las demandas del mercado laboral, impulsando la formación y cualificación especializada.

Seguidamente, establece un conjunto de líneas de acción y medidas para abordar la consecución de los objetivos definidos en la estrategia. Concretamente, en la línea de acción 7: “*Desarrollar una cultura de ciberseguridad*”, se incluyen las medidas que responden al objetivo IV citado más arriba.

De las ocho medidas determinadas en esta línea de acción, se subrayan las siguientes:

1. *Incrementar las campañas de concienciación a ciudadanos y empresas (...)*
3. *Impulsar iniciativas y planes de alfabetización digital en ciberseguridad*
4. *Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa*
6. *Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar*
7. *Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades*

8. *Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad*

Así, la última Estrategia Nacional de Ciberseguridad contempla entre sus necesidades aquellas en materia de concienciación, capacitación y formación en ciberseguridad tanto a la ciudadanía en general, como a los distintos roles profesionales en el mundo laboral.

Planes y estrategias de ciberseguridad en Castilla-La Mancha

Desde el año 2021 el Gobierno de Castilla-La Mancha ha puesto en marcha un Plan Director de Seguridad [47] que está basado en tres líneas:

- i) *Desarrollar y establecer una cultura de ciberseguridad*
- ii) *Reforzar y ampliar el actual sistema integral de gestión de la seguridad*
- iii) *Impulsar nuevos servicios de ciberseguridad*

De las líneas anteriores cabe subrayar la primera, donde se persigue el objetivo de capacitar y concienciar a la plantilla de la organización, creando un cambio en la cultura corporativa girando en torno a la ciberseguridad y teniendo presentes los riesgos que se derivan del ciberespacio.

Como continuación del Plan Director de Seguridad, el Gobierno de Castilla-La Mancha está desarrollando su propia estrategia de ciberseguridad a nivel regional [19], que formará parte de la estrategia digital autonómica, para formar a especialistas y capacitar y sensibilizar a la ciudadanía.

De esta manera, se pretende contribuir hacia un entorno tecnológico más seguro, cubriendo ampliamente la formación y capacitación de las personas en ciberseguridad, tanto para quienes cuentan con conocimientos tecnológicos muy específicos, como para el resto de la ciudadanía.

3.4 NORMATIVAS DE CIBERSEGURIDAD

En el aspecto legal se establecen una serie de reglamentos y directivas europeas que aplican a los Estados miembros de la Unión, así como otras normas en forma de reales decretos en España.

En este apartado se analiza el contexto regulatorio actual encuadrado dentro de las necesidades presentes de concienciación principalmente de las personas en ciberseguridad en las organizaciones y, por extensión derivado de lo anterior, también es aplicable a los ciudadanos en general.

Desde esta perspectiva, se observan las obligaciones que se imponen juntamente con las carencias que se detectan en cuanto a los marcos, modelos o metodologías que debieran seguir para estudiar en qué punto de madurez se encuentran las organizaciones en este ámbito de aplicación.

Reglamento DORA

El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo [4], conocido como DORA (*Digital Operational Resilience Act*), trata el objetivo de fortalecer la resiliencia operativa digital y la ciberseguridad en el sector financiero. Desde comienzos del año 2025, tanto las entidades financieras como los proveedores de servicios TIC de terceros deben cumplir obligatoriamente los requisitos descritos en el reglamento.

Entre los requisitos definidos en DORA, se incluyen las siguientes obligaciones:

- Artículo 5.2. g), señala que dentro del marco de gobernanza de la organización el órgano de dirección deberá asignar y revisar periódicamente los presupuestos destinados a los programas de sensibilización en materia de seguridad de las TIC para todo el personal.
- Artículo 13.6., ligado al aprendizaje y evolución, establece que las entidades desarrollarán programas de sensibilización en materia de seguridad de las TIC como módulos obligatorios en sus acciones formativas. Estos programas aplican con un nivel de complejidad acorde a la atribución de las funciones de todos los empleados, incluyendo al personal de la alta dirección y, cuando proceda, también a aquellos proveedores terceros de servicios TIC.
- El artículo 16.1. h), vinculado al marco simplificado de gestión del riesgo relacionado con las TIC, y el artículo 30.2. i), de cláusulas contractuales, incluyen entre sus condiciones la participación en programas de sensibilización de los actores anteriores.

En este reglamento se pone de manifiesto la necesidad de llevar a cabo actividades de formación a todas las personas adaptadas a su perfil, lo cual en este sentido es muy positivo para lograr una concienciación efectiva. Pese a ello, estas obligaciones carecen de una manera estandarizada de validar los resultados obtenidos a partir de este proceso de capacitación y actividades relacionadas.

Directiva NIS2

La directiva 2022/2555 (UE) del Parlamento Europeo y del Consejo [1], conocida como NIS2 (*Network and Information Systems*), impulsa las medidas necesarias con el objetivo de garantizar un elevado nivel general de ciberseguridad en toda la Unión Europea. Desde octubre de 2024, todos los Estados miembros deben cumplir las normas de ciberseguridad de la última directiva NIS.

Para ello, se destacan necesidades enfocadas en las personas en diferentes artículos de la directiva:

- Artículo 7.1. h), que hace referencia a que un plan de ciberseguridad nacional incluya las medidas necesarias para elevar el nivel general de concienciación de la ciudadanía en materia de ciberseguridad.

- Artículo 7.2. f), en el cual se indica que los Estados miembros deben promocionar y desarrollar la educación y formación en materia de ciberseguridad, sensibilización y buenas prácticas sobre ciber higiene destinadas a la ciudadanía.
- Artículo 20.2., donde rubrica que se debe garantizar la asistencia de los miembros de los órganos de dirección a formaciones sobre detección y gestión de riesgos de ciberseguridad, alentando a sus empleados a adquirir estos conocimientos periódicamente.
- Artículo 21.2. g), que destaca las prácticas básicas de ciber higiene y formación en ciberseguridad dentro de las medidas para gestionar los riesgos de ciberseguridad.
- Artículo 29.1. b), incluye como mecanismo de intercambio de información el requisito de concienciar sobre ciberamenazas para reforzar el nivel de ciberseguridad.

Como se deduce de los artículos enumerados anteriormente de la directiva NIS2, las medidas de educación y formación son fundamentales y deben estar contenidas en los planes de ciberseguridad de los EEMM. A pesar de estas indicaciones de la Unión Europea, tampoco se incluyen modelos o guías de referencia para llevar a cabo la concienciación de las personas en ciberseguridad, ni se puntualiza una forma común de evaluar si se está realizando eficazmente.

Esquema Nacional de Seguridad

A nivel nacional, una de las normativas más destacadas es el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad [3] (también conocido como ENS).

Este real decreto se aplica a todo el sector público, así como a los sistemas de información de las entidades del sector privado cuando presten servicios a entidades del sector público, determinando un total de siete principios básicos y quince requisitos mínimos.

Dentro del Anexo II del ENS, se especifican las medidas de seguridad, de las cuales se pondrá el foco en las siguientes, pertenecientes al grupo de medidas de gestión del personal:

- [mp.per.3] Concienciación
- [mp.per.4] Formación

En sus requisitos, los cuales son aplicables a todas las categorías y las dimensiones de seguridad de los sistemas de información, se indica lo siguiente:

- [mp.per.3] Concienciación: “*Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos (...)*”.
- [mp.per.4.1] Formación: “*Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones (...)*”.

Como bien se enuncia en el ENS, resulta obligatorio poner el foco en la concienciación y formación del personal en materia de seguridad de la información. Sin embargo, estas medidas de seguridad están muy ligadas a la gestión de procesos y tecnologías, siendo muy superficiales desde la perspectiva humana y sin encontrarse sustentadas en un marco o modelo de madurez que permita desempeñar las bases para la capacitación de las personas en esta materia.

Con este punto de partida, desde el plano normativo nacional resulta imprescindible llevar a cabo un estudio sobre la forma en que estos contenidos puedan ser incluidos en las acciones formativas correspondientes a este ámbito con su correspondiente validación efectiva.

Ley de Seguridad Nacional

Publicada como norma con rango de Ley 36/2015, de 28 de septiembre, de Seguridad Nacional [2], en su artículo 10 considera la ciberseguridad como uno de los ámbitos de especial interés de la Seguridad Nacional para preservar los derechos, libertades y bienestar de la ciudadanía.

Esta ley no hace alusiones directas a la concienciación y capacitación en ciberseguridad, aunque en su artículo 8 incluye la participación ciudadana para contribuir a la Seguridad Nacional estableciendo mecanismos que permitan la formulación y ejecución de políticas en su favor.

Adicionalmente, en el artículo 27 se enfatiza la importancia del sector público y privado mediante la contribución de sus recursos humanos y materiales a la Seguridad Nacional en el Sistema de Seguridad Nacional, mientras que en su artículo 28 se alude discretamente a la capacitación de las personas una vez aprobada la creación de un catálogo de recursos.

3.5 ESTÁNDARES Y MARCOS DE REFERENCIA EN CIBERSEGURIDAD

De manera complementaria a la normativa presente, existen otros estándares, marcos y programas de referencia a nivel internacional que versan sobre la ciberseguridad. En esta unidad, se abordan algunos ejemplos desde la perspectiva de concienciar a los usuarios dentro de las organizaciones.

Como estándares de referencia para la gestión de riesgos de seguridad de la información de manera efectiva tenemos la familia o serie de la ISO/IEC 27000 y el marco de ciberseguridad CSF 2.0 de NIST. No obstante, la relación de controles y medidas incluidas en estos conocidos estándares no ahondan en la concienciación y sensibilización de las personas para enfrentarse a dichos riesgos.

Aproximándose un poco al enfoque perseguido por este trabajo, existe el modelo de madurez C2M2 (*Cybersecurity Maturity Model*) [9] propuesto por la agencia de ciberseguridad y seguridad de las infraestructuras de los Estados Unidos, más conocida como CISA, para ayudar a las organizaciones a evaluar sus capacidades en ciberseguridad y optimizar sus inversiones en seguridad.

En este caso, en dicho modelo se propone una serie de dominios en los que se tratan objetivos y prácticas genéricas sobre la gobernanza y gestión de la ciberseguridad en las empresas, sin ofrecer una perspectiva clara desde el lado de los humanos y la capacitación requerida en la materia.

Por último, están presentes otros documentos que tratan de nivelar la madurez de las organizaciones en ciberseguridad. Algunos ejemplos son el modelo de madurez propuesto por el SANS Institute [41] y el modelo CMMC (*Cybersecurity Maturity Model Certification*) [43] del departamento de defensa de los Estados Unidos.

En el caso del primero, se definen un conjunto de cinco etapas o fases a alcanzar con indicadores de programas de formación muy genéricos, algunas métricas potenciales de interés y próximos pasos para continuar a la siguiente fase. En el segundo, se concretan tres niveles de madurez haciendo referencias al cumplimiento de requisitos incluidos en la normativa NIST SP 800-171, la cual se limita al tratamiento y protección de la información no clasificada, por lo que este modelo se encuentra de nuevo al margen de la concienciación de los usuarios en ciberseguridad.

En conclusión, en el ámbito internacional existen estándares que profundizan en la gobernanza y gestión de riesgos de ciberseguridad desde el plano de la organización. En ellos, se observan otra vez las carencias a la hora de precisar los elementos necesarios para sostener la clasificación de los niveles de madurez desde una perspectiva enfocada en la concienciación efectiva de las personas.

3.6 ACTIVIDADES DE CONCIENCIACIÓN Y FORMACIÓN

A nivel nacional se desarrollan diferentes acciones para concienciar y formar al personal en ciberseguridad. En este apartado se describen algunas de las actividades principales en el plano nacional impartidas desde diferentes instituciones y organizaciones especializadas en la materia.

Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia, oferta varios cursos STIC semestralmente y de manera gratuita para el personal de las Administraciones Públicas, con un número de participantes limitado a través de la plataforma ÁNGELES³ [6]. Además, esta plataforma incluye otros itinerarios formativos, superando los 30.000 usuarios registrados [7].

³ <https://angeles.ccn-cert.cni.es/es/cursos-stic>

Por otro lado, el CCN también lleva a cabo seminarios web en directo abiertos al resto de profesionales del sector privado que posteriormente son compartidos públicamente en el portal de contenidos VANESA⁴.

Las anteriores actividades formativas proporcionan conocimientos muy técnicos en su mayoría, por lo que pueden resultar de gran interés para un amplio número de profesionales del sector TIC.

Instituto Nacional de Ciberseguridad

Otros programas formativos para destacar son los que se imparten a través del Instituto Nacional de Ciberseguridad (INCIBE⁵), desde el que se coordinan actividades de formación⁶ sobre fundamentos básicos en ciberseguridad y gestión de incidentes para el personal de las empresas y autónomos [25] e itinerarios interactivos para actualizar los conocimientos de sus empleados en esta materia de manera gratuita.

Asimismo, existen acciones de formación y concienciación enfocadas en la ciudadanía, desde los más mayores hasta menores de edad mediante una serie de cursos en línea, guías, talleres, recursos descargables en *Academia Hacker*⁷, así como juegos y otras actividades interactivas. Estas acciones formativas permiten alcanzar nociones básicas de ciberseguridad, seguridad de la información y protección de datos, así como realizar un uso seguro de la red y la tecnología.

Dentro de la iniciativa *CyberCamp*⁸, el INCIBE coorganiza eventos con universidades de las diferentes comunidades autónomas españolas, entre las que participan algunos de los campus de la Universidad de Castilla-La Mancha [44] para promover el desarrollo del conocimiento y capacidades digitales en el ámbito de la ciberseguridad, junto con una cátedra institucional de ciberseguridad [44].

De manera complementaria, es preciso señalar el programa *cibercooperantes*⁹ de INCIBE, mediante el cual se imparten charlas formativas en ciberseguridad en centros, asociaciones y otras entidades gracias a la participación de personas voluntarias con interés en la divulgación de ciberseguridad. Estas charlas se encuentran destinadas a toda la sociedad, incluyendo tanto a jóvenes como a personas adultas.

⁴ <https://vimeo.com/ccnvanesa>

⁵ INCIBE. <https://www.incibe.es/>

⁶ INCIBE formación. <https://www.incibe.es/empresas/formacion>

⁷ Academia Hacker. <https://www.incibe.es/ed2026/talento-hacker/academia-hacker>

⁸ INCIBE. CyberCamp. <https://www.incibe.es/eventos/cybercamp>

⁹ Programa cibercooperantes. <https://www.incibe.es/incibe/cibercooperantes>

RETECH Ciberseguridad

Las Redes Territoriales de Especialización Tecnológica (RETECH) [27], aplicadas al ámbito de ciberseguridad, se tratan de una iniciativa nacional coordinada por el INCIBE para el desarrollo de capacidades y talento en ciberseguridad en sectores productivos estratégicos que cuenta con la participación de las Comunidades Autónomas.

En concreto, y alineado con la estrategia regional de ciberseguridad de Castilla-La Mancha [19] en el ámbito de las empresas TIC, en septiembre de 2024 se publicó la licitación de la actuación denominada “*Ciberreg*” [18]. Esta iniciativa cuenta con diferentes lotes donde se dirigen múltiples acciones formativas y sesiones divulgativas para la capacitación y sensibilización en ciberseguridad.

Plan Nacional de Competencias Digitales¹⁰

Enmarcado dentro de la Agenda España Digital 2026¹¹, en el eje 9, competencias digitales, encontramos el Plan Nacional de Competencias Digitales (*digital skills*), que incorpora actuaciones para el desarrollo de las competencias digitales transversales para la ciudadanía, logrando reducir la brecha digital y la brecha de género, aumentando así el porcentaje de especialistas digitales. Asimismo, en la medida 40, impulso a los especialistas digitales, se menciona que se han de crear nuevas titulaciones y adaptar las existentes en los “*ámbitos específicos más demandados por la industria (ciberseguridad, inteligencia artificial, análisis de datos, diseños web, etc.)*”.

Conjuntamente, se enmarca en el Plan de Recuperación, Transformación y Resiliencia, en el componente 19¹². Además, ubicado dentro de este componente, encontramos la inversión 4, profesionales digitales (C19.I4) donde se especifica que las ofertas formativas deben permitir “*adquirir competencias digitales avanzadas y progresar en áreas clave como la ciberseguridad*”.

En relación con este plan, su foco principal consiste en la capacitación digital de la ciudadanía sin mencionar expresamente la concienciación en ciberseguridad. Sin embargo, sí concluye con la necesidad de formar especialistas técnicos en esta materia y reducir la brecha de género.

¹⁰ https://espanadigital.gob.es/sites/espanadigital/files/2022-06/Plan%20Nacional%20de%20Competencias%20Digitales_0.pdf

¹¹ https://espanadigital.gob.es/sites/espanadigital/files/2022-10/Espa%C3%B1a_Digital_2026.pdf

¹² https://planderecuperacion.gob.es/sites/default/files/2023-10/0310203_adenda_plan_de_recuperacion_componente19.pdf

Plan de Capacitación Digital de Castilla-La Mancha

En el ámbito regional, dentro del Gobierno de Castilla-La Mancha desde el proyecto Ciudadanía Digital¹³ se lleva a cabo un plan de capacitación digital mediante cursos en línea y presenciales, en los cuales ya se han formado a más de 27.000 personas de la región, siendo un 65% mujeres [17].

Dentro de las acciones formativas ofertadas, entre otras, las siguientes se encuentran relacionadas con el área de ciberseguridad y están pensadas para la ciudadanía sin conocimientos técnicos previos:

- *Buenas prácticas de ciberseguridad¹⁴*
- *Protege tus dispositivos digitales contra el malware¹⁵*
- *¡Ojo! Privacidad propia y ajena en la compartición de datos¹⁶*

Universidades y Formación Profesional

En el contexto académico, cada vez es más común encontrar asignaturas relacionadas con la ciberseguridad y seguridad de la información, tanto en un plano técnico, como de gestión.

Tal es la concienciación y demanda de especialistas en los últimos años que, incluso, se están adaptando y creando nuevas titulaciones universitarias (grado, máster y cursos de formación continua), así como cursos de especialización de Formación Profesional en ciberseguridad. Desde el portal web de INCIBE se ofrecen catálogos de formación reglada en ciberseguridad en España [24].

Por ejemplo, en Castilla-La Mancha se ofertan las siguientes titulaciones regladas:

- Máster de Formación Permanente en Ciberseguridad y Seguridad de la Información¹⁷ (impartido por la Universidad de Castilla-La Mancha)
- Curso de Especialización de Formación Profesional en Ciberseguridad en Entornos de las Tecnologías de la Información¹⁸ (impartido por el sistema educativo de la Consejería de Educación, Cultura y Deportes de Castilla-La Mancha)

¹³ <https://ciudadaniadigital.castillalamancha.es/>

¹⁴ <https://ciudadaniadigital.castillalamancha.es/curso/buenas-practicas-de-ciberseguridad>

¹⁵ <https://ciudadaniadigital.castillalamancha.es/curso/protege-tus-dispositivos-digitales-contra-el-malware>

¹⁶ <https://ciudadaniadigital.castillalamancha.es/curso/ojo-privacidad-propia-y-ajena-en-la-comparticion-de-datos>

¹⁷ <https://www.uclm.es/estudios/propios/master-formacion-permanente-ciberseguridad-seguridad-informacion>

¹⁸ <https://www.educa.jccm.es/es/fpclm/cursos-especializacion/curso-especializacion-ciberseguridad-entornos-tecnologias-i>

Las titulaciones anteriores se encuentran enfocadas para la generación de talento en ciberseguridad, alineadas con la medida 40 de la Agenda España Digital 2026 señalada anteriormente, yendo más allá de la formación básica para la concienciación a la ciudadanía.

Publicaciones científicas

Además de lo anterior, resulta de interés analizar algunos artículos científicos buscados en Google Académico (también conocido como *Google Scholar*) publicados por editoriales y otras entidades de prestigio como ACM, Elsevier o IEEE, sobre investigaciones recientes enfocadas en la temática de concienciación de las personas en ciberseguridad en diferentes ámbitos de aplicación.

En el primer trabajo de investigación analizado se proponen dos juegos serios [49] que ponen el foco en aumentar la concienciación sobre la ciberseguridad en ingeniería de software, abordando prácticas de codificación segura y seguridad en la nube en entornos de trabajo híbridos.

Otra investigación realiza una propuesta empleando la gamificación para educar en ciberseguridad de padres a hijos [39], resaltando los importantes riesgos que pueden encontrar en la red, promoviendo la colaboración y el diálogo activo sobre ciberseguridad. En otro artículo académico, se presenta un juego para mejorar la ciberseguridad en diversos contextos mediante el aprendizaje digital basado en juegos (*DGBL*) para educar a través de varios géneros [34].

Dentro del ámbito de las pymes [8], también se ha encontrado una publicación que investiga sobre las lagunas de concienciación en ciberseguridad identificando algunos retos clave, como la escasez de recursos, la inadecuación de los contenidos y métodos de concienciación, la falta de compromiso de la alta dirección y la necesidad de marcos de concienciación específicos para estas empresas.

Eventos y foros sectoriales

A continuación, se subrayan algunos de los congresos, conferencias y eventos referentes tanto a nivel regional como nacional, considerando que estas actividades formativas pueden estar dirigidas para profesionales del sector de la ciberseguridad con amplios conocimientos técnicos en la materia.

Primeramente, a nivel nacional destacan las Jornadas STIC¹⁹ organizadas cada año por el CCN, además del congreso de ciberseguridad *RootedCON*²⁰ celebrado en diferentes ciudades de España, donde se exponen herramientas e investigaciones muy especializadas.

¹⁹ <https://jornadas.ccn-cert.cni.es/es/>

²⁰ <https://www.rootedcon.com/inicio/>

En segundo lugar, en el plano regional una de las más conocidas es *Navaja Negra*, organizada anualmente en la provincia de Albacete. Igualmente, se desarrollan los congresos de ciberseguridad de *MorterueloCON*²¹ y *HoneyCON*²², en las ciudades de Cuenca y Guadalajara, respectivamente.

Por último, desde el Departamento de Seguridad Nacional, se producen sesiones de trabajo del Foro Nacional de Ciberseguridad²³, dependiente del Consejo Nacional de Ciberseguridad, con el objetivo de promover la ciberseguridad entre la ciudadanía y las empresas mediante la colaboración público-privada en esta disciplina.

La creación del foro viene determinada por la Estrategia Nacional de Ciberseguridad 2019 [13] analizada anteriormente, a través de la línea de acción 4: “*Impulsar la ciberseguridad de ciudadanos y empresas*”, en la medida 9: “*Promover la creación del foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, (...)*”.

Gracias a ello, se crean diferentes grupos de trabajo formados por personas especialistas y expertas en ciberseguridad, en los que se comparte conocimiento a través de publicaciones sobre los desafíos, tendencias y amenazas existentes en el ciberspacio.

3.7 CONCLUSIONES

En este capítulo se ha comenzado realizando un análisis de la situación actual e interés de la ciberseguridad en la sociedad, cómo esto se traduce en las cifras de ciberdelitos, la tipología de los incidentes más frecuentes y su relación con el factor humano de la mano de la ingeniería social.

Seguidamente, se ha llevado a cabo un estudio intenso de las estrategias y planes de ciberseguridad propuestos a nivel europeo, nacional y autonómico para encarar las ascendentes exigencias del contexto regulatorio en este ámbito.

De estos documentos, se ha llegado a dos conclusiones muy aparentes: la primera es que en todas las estrategias y normativas de ciberseguridad se pone de manifiesto la obligatoria necesidad de concienciar y formar a las personas de las organizaciones en ciberseguridad; la segunda, que ninguna de las anteriores puntualiza ni profundiza en un marco, modelo o metodología de referencia para llevarlo a cabo por niveles, sin tampoco ahondar en los detalles para el proceso de validación final.

²¹ <https://www.morteruelo.net/>

²² <https://honeycon.eu/>

²³ <https://foronacionalciberseguridad.es/>

Por último, se realiza una investigación de las acciones formativas que se imparten dentro del territorio nacional a través de diferentes entidades, así como se estudian algunos artículos científicos recientes publicados por editoriales de prestigio. En este punto, se analizan las temáticas tratadas, el tipo de público al que van dirigidas y la complejidad de estas actividades, poniendo de manifiesto la urgencia de concienciar en ciberseguridad a todos los niveles dentro y fuera de las organizaciones.

Como consecuencia de lo anterior, en este proyecto se propone el objetivo de implementar un modelo de referencia para evaluar eficazmente la madurez de las organizaciones en la concienciación de sus usuarios en ciberseguridad, desde una perspectiva que pone en el centro a las personas, cubriendo las carencias evidenciadas en las publicaciones analizadas a lo largo de este capítulo.

CAPÍTULO 4. MÉTODO DE TRABAJO

El presente capítulo abarca todo aquello relacionado con las metodologías empleadas que han permitido un alcance exitoso en el desarrollo del proyecto, así como la planificación temporal, estimación de costes y el marco de tecnologías que lo componen.

4.1 METODOLOGÍA

El proyecto ha sido desarrollado especialmente mediante la utilización de metodologías de trabajo ágiles, las cuales, a través de varias iteraciones, permiten cumplir con las competencias y objetivos definidos a lo largo de diferentes intervalos regulares de tiempo delimitados por semanas.

Gracias a las metodologías ágiles, es posible obtener resultados de gran valor en períodos reducidos de tiempo. Esto permite refinar el producto a través de entregas parciales en las sucesivas iteraciones hasta su puesta final, logrando un producto mínimo viable (PMV) en poco tiempo.

Además, gracias a estas metodologías dicho producto puede ser actualizado fácil y rápidamente gracias a su modularidad, en beneficio de cumplir lo antes posible con las necesidades de mercado, reduciendo considerablemente de esta manera el “*time to market*”.

Para aprovechar estas bondades ofrecidas por las metodologías ágiles, se ha optado por utilizar una metodología basada en el pensamiento de diseño o *Design Thinking*, la cual fue impulsada originalmente en Estados Unidos por la escuela d.school de la Universidad de Stanford [11]. Se trata de un método que sirve para la resolución de problemas de manera creativa y como marco de trabajo en proyectos de valor del mundo real.

El modelo propuesto en Stanford [42] se caracteriza por estar enfocado en las personas gracias a una serie de herramientas de diseño y está compuesto por un total de cinco fases descritas en la *Figura 4.1* [40], desde las cuales se puede volver hacia las anteriores debido a su naturaleza iterativa. A continuación, se explican las etapas propuestas en *Design Thinking*:

1. Empatizar: Primera fase en la que se lleva a cabo un proceso de diseño centrado en las personas, comprendiendo sus experiencias, necesidades y motivaciones.
2. Definir: En ella se busca plantear, enfocar y esclarecer el desafío a resolver.
3. Idear: Consiste en captar el máximo número de ideas posible, para transitar de los problemas identificados hacia la búsqueda de soluciones para los usuarios.
4. Prototipar: Se centra en construir una serie de artefactos o prototipos experimentales para dar solución a las ideas y retos definidos en fases previas.
5. Evaluar: Última etapa en la que se tiene el objetivo de afianzar y depurar aquellas ideas y prototipos trabajados, aprendiendo de manera conjunta con los usuarios finales.

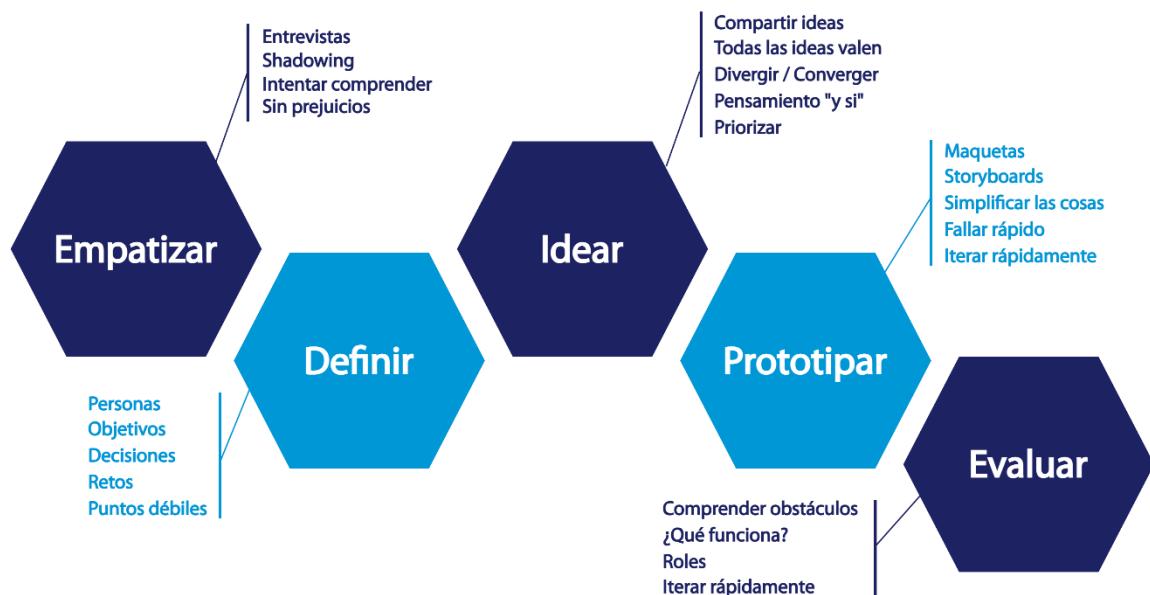


Figura 4.1: Fases de Design Thinking (Stanford d.school)

4.2 ENTERPRISE DESIGN THINKING

Derivado de la metodología de *Design Thinking*, la empresa tecnológica multinacional estadounidense International Business Machines Corporation, más conocida como IBM, ofrece una serie de guías y cajas de herramientas para ponerla en práctica. En concreto, a través de la propuesta que IBM ha bautizado como *Enterprise Design Thinking* [20], se proponen un total de catorce actividades para ejercitarse las habilidades en la citada metodología, pudiendo crear los artefactos o prototipos manteniendo las ventajas originales.

Para ello, la metodología se basa en un total de tres principios guía:

- Centrarse en los resultados para el usuario: Trata sobre aprender de los usuarios siguiendo de cerca sus experiencias e identificando sus necesidades reales.
- Reinención inquieta: Consiste en la búsqueda de la mejora continua, sabiendo que se puede llegar a mejores soluciones, pero sin lograr nunca la perfección.
- Equipos diversos y empoderados: Consiguen alcanzar mejores resultados colaborando mediante ideas innovadoras.

Además de los principios anteriores, este marco subraya otros dos conceptos fundamentales:

- El bucle o *loop*: Nos impulsa a comprender el presente y vislumbrar el futuro en un ciclo continuo de observación, reflexión y creación.
- Las claves o *keys*: Nos ayudan a mantener a los equipos enfocados y alineados en los resultados que verdaderamente importan a los usuarios. Están formados por las colinas o

hills que alinean a los equipos para obtener resultados significativos, las reproducciones o *playbacks* enhilan en el tiempo mediante la retroalimentación continua y los usuarios patrocinadores para mantenerse fiel con las necesidades reales de los usuarios finales.

Finalmente, los artefactos disponibles en *Enterprise Design Thinking* [23] se obtienen a partir de algunas de las actividades siguientes: mapa de empatía, viñetas de las grandes ideas, colinas, cuadrante de prioridades (*priorization grid*), cuadrante de retroalimentación (*feedback grid*) y las expectativas y miedos (*hopes and fears*).

Mapa de empatía

En primer lugar, como se explicó anteriormente, la empatía supone la primera fase del proceso de *Design Thinking*, por lo que tiene su artefacto correspondiente donde se crea una cuadrícula conformada por un total de cuatro cuadrantes centrados en las personas.

En este mapa se refleja la importancia de acercarse y ponerse en el lado del usuario con observaciones reales sobre lo que dice (*says*), hace (*does*), piensa (*thinks*) y, por último, siente (*feels*), como parte del bucle que se propone en los conceptos principales de la metodología escogida. En la *Figura 4.3* (ver siguiente página) se esboza el resultado obtenido gracias a esta actividad.

Viñetas de las grandes ideas

El motivo para llevar a cabo esta actividad consiste en la búsqueda de posibles soluciones para satisfacer rápidamente las necesidades de los usuarios, considerando que cualquier persona puede contribuir con ideas válidas sobre la experiencia del usuario una vez se ha empatizado con este.

A continuación, en la *Figura 4.2* se muestra el artefacto resultante correspondiente:



Figura 4.2: Viñetas de las grandes ideas

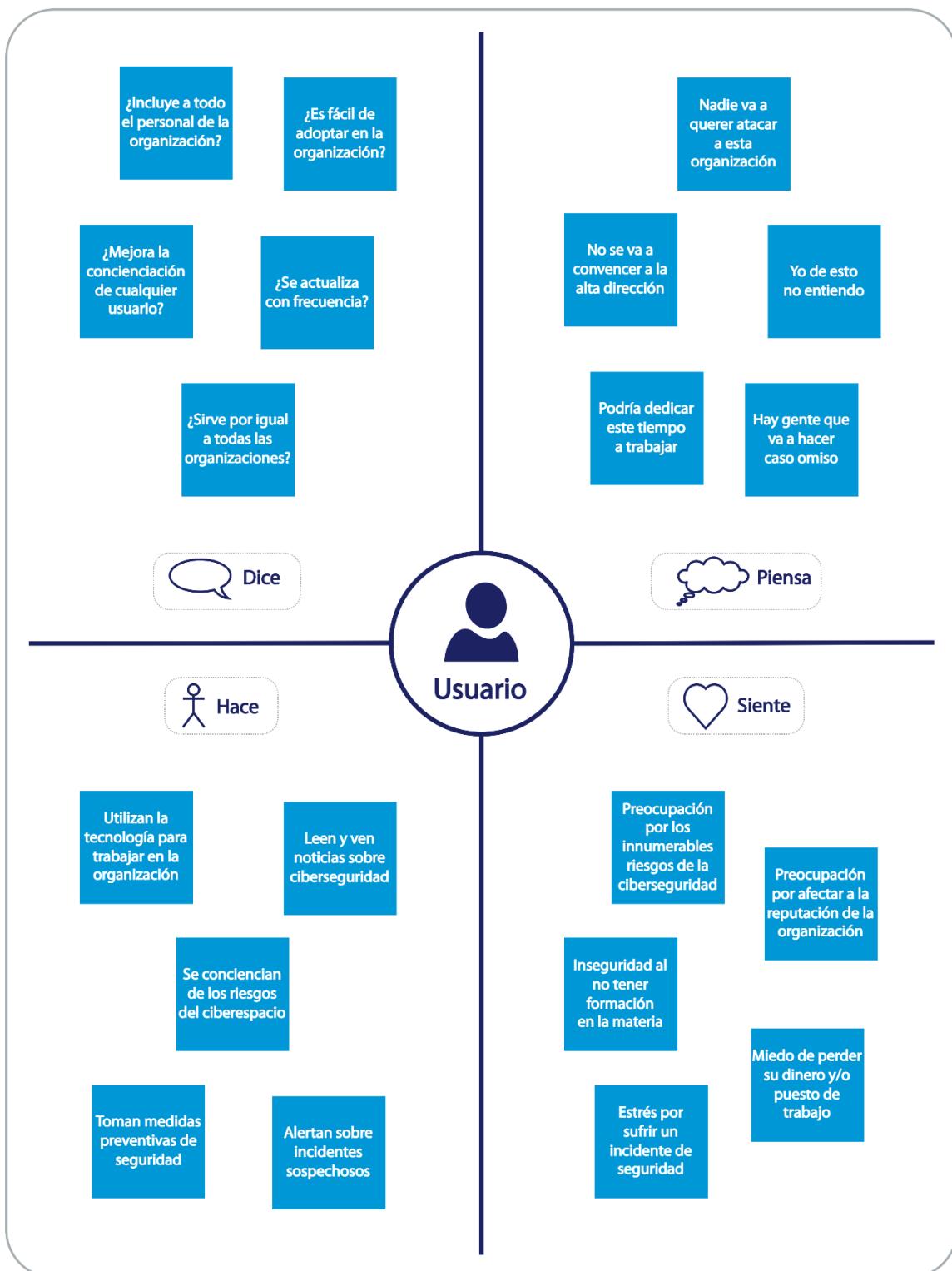


Figura 4.3: Mapa de empatía

Colinas

Se trata de una de las claves que forman parte de la presente metodología, ya que permiten exponer de manera clara a los usuarios (*who*) las utilidades reales del proyecto (*what*) y los resultados (*wow*) de valor que se esperan obtener. En la *Figura 4.4* se exhibe la propuesta obtenida:

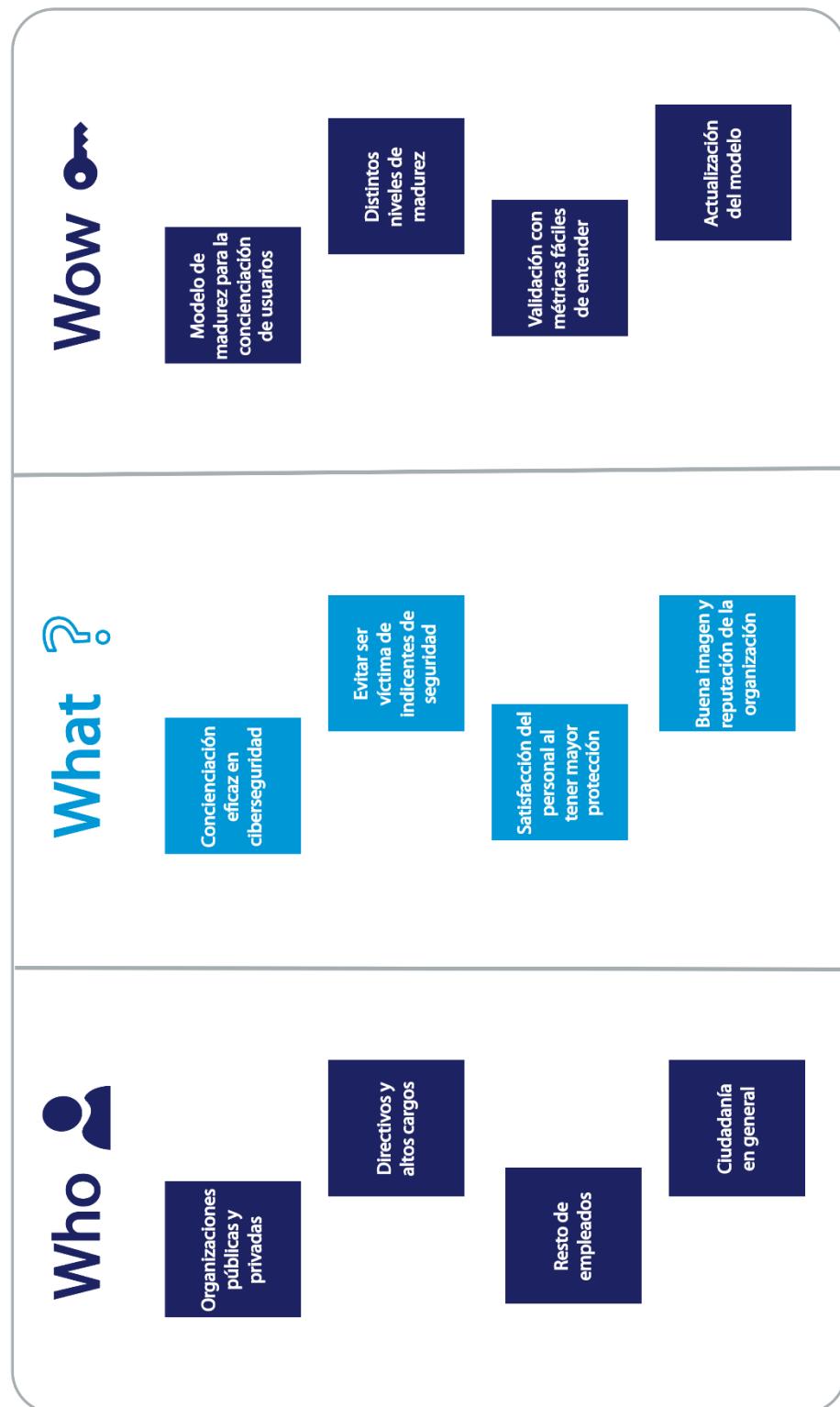


Figura 4.4: Colinas

Cuadrante de prioridades

Este artefacto tiene por objetivo evaluar y reflexionar sobre las ideas identificadas para priorizarlas en base a la importancia de las necesidades, su nivel de viabilidad real y el valor que aportan al usuario en el proyecto a desarrollar.

Se trata de un cuadrante que está formado por dos ejes, donde se clasifican de menor a mayor la importancia de las ideas descritas (en el eje de ordenadas), así como la viabilidad de su ejecución (en el eje de abscisas).

A continuación, en la *Figura 4.5* se exponen los resultados conseguidos en la presente actividad:

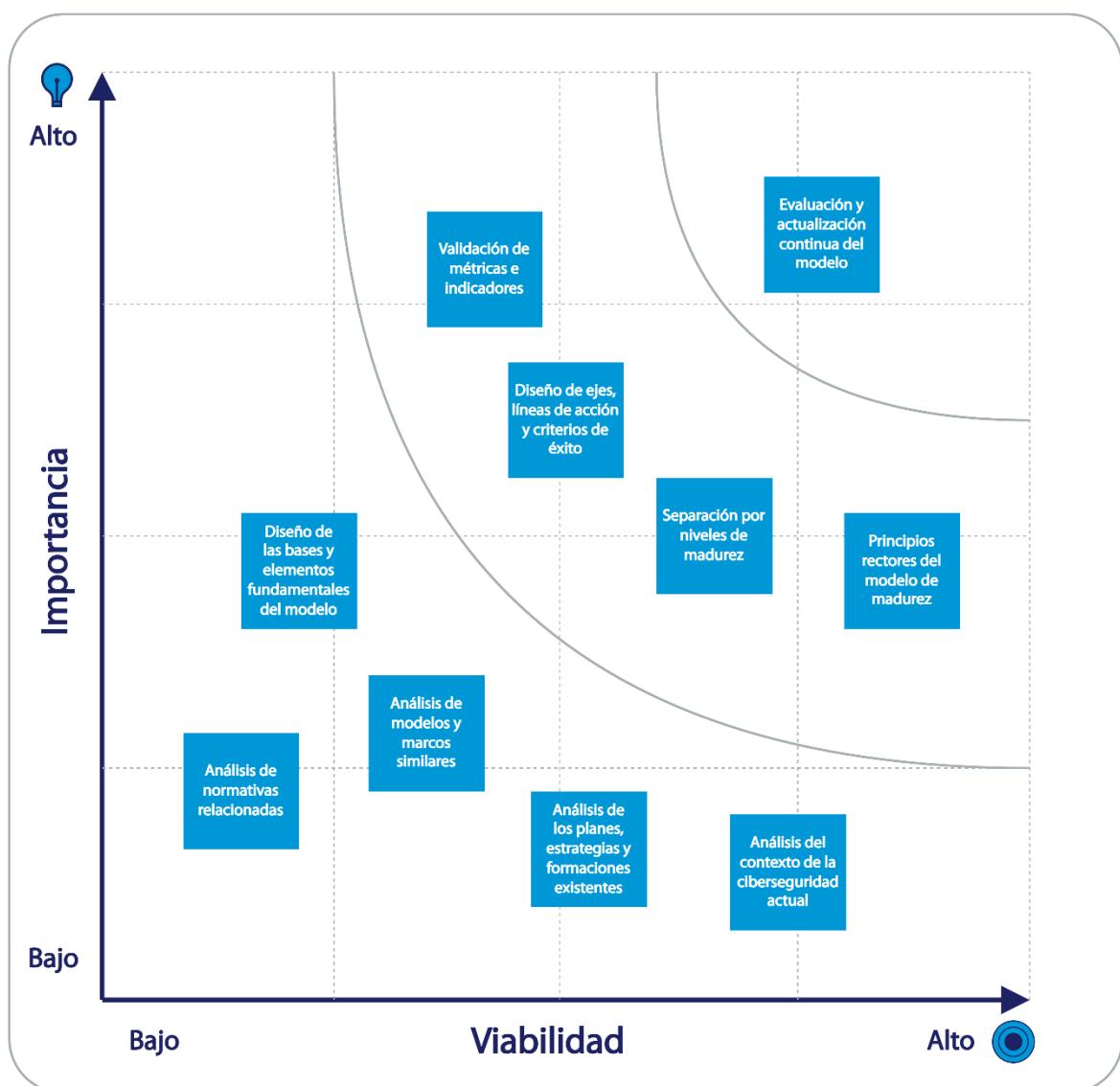


Figura 4.5: Cuadrante de prioridades

Cuadrante de retroalimentación

En este prototipo se busca reunir y organizar el *feedback* recibido por parte de los usuarios, miembros del equipo y demás interesados en el proyecto, partiendo de la experiencia y trayectoria profesional tanto del tutor, como del alumno, en el campo de la ciberseguridad.

Para ello, se dibuja una rejilla formada por cuatro cuadrantes:

1. Aquello que ha funcionado bien (*works*)
2. Necesidades de cambio para mejorar (*change*)
3. Preguntas formuladas (*questions*)
4. Nuevas ideas para probar (*ideas*)

En la *Figura 4.7* (ver siguiente página) se presenta el producto logrado en esta tarea.

Expectativas y miedos

En la actividad correspondiente a este último artefacto se discuten las expectativas de los usuarios, sobre aquello que se pretende conseguir y los posibles miedos antes dar comienzo el proyecto, analizando y debatiendo abiertamente sobre los asuntos o temas que generen mayor interés.

En la *Figura 4.6* se muestra el artefacto cosechado en este trabajo final:



Figura 4.6: Expectativas y miedos

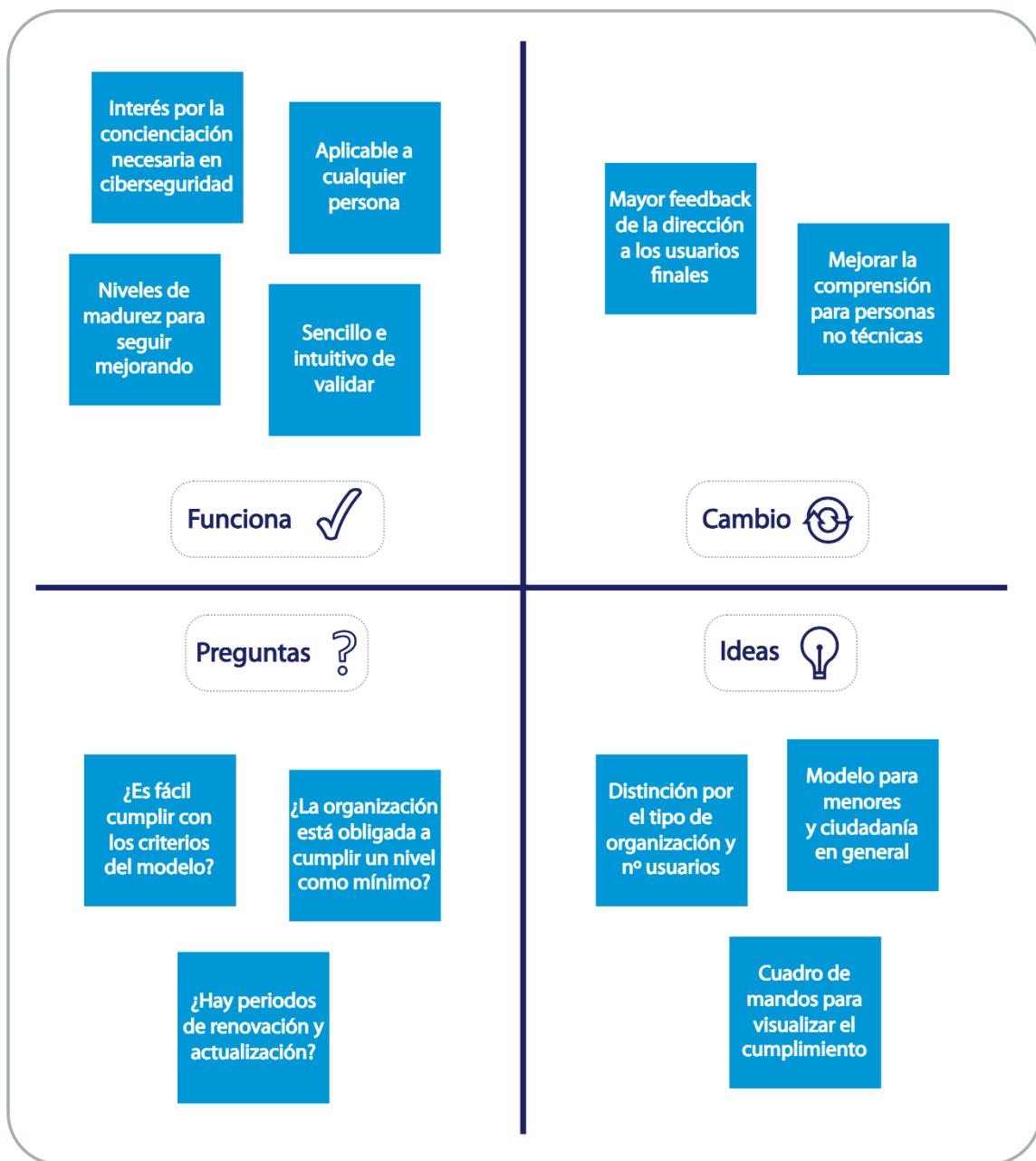


Figura 4.7: Cuadrante de retroalimentación

4.3 PLANIFICACIÓN TEMPORAL

En esta sección se aborda someramente la planificación temporal estimada por fases del proyecto, teniendo en cuenta que para su realización se ha compaginado con las actividades laborales y la participación en otros compromisos profesionales tanto del tutor, como del alumno.

Para comenzar, se llevó a cabo una iteración o *sprint* inicial (S0) para determinar el alcance y los objetivos del TFM con el envío de la propuesta final a la comisión académica y su correspondiente aprobación. Posteriormente, tras siete *sprints* (del S1 al S7) con una duración comprendida entre dos y tres semanas, se realizaron entregas parciales a lo largo del desarrollo del proyecto.

Para cumplir con las 225 horas de trabajo correspondientes a los 9 créditos ECTS estipulados en la asignatura correspondiente al TFM, se estima que cada *sprint* tendrá un esfuerzo promedio aproximado de 5 horas del tutor y 35 horas por parte del alumno, a excepción del *sprint* inicial.

Las fechas de realización del proyecto coinciden con el primer cuatrimestre académico del curso en que se presenta, dando comienzo en el mes de septiembre de 2024 y finalizando en enero de 2025.

En la *Tabla 4.1*, se muestra la relación de *sprints* del proyecto junto con las fechas de comienzo y finalización respectivas, así como el desglose de los objetivos trabajados en los mismos:

Sprint	Fecha inicio	Fecha fin	Objetivos
S0	19/09/2024	02/10/2024	Propuesta
S1	03/10/2024	16/10/2024	[OP1]
S2	17/10/2024	06/11/2024	[OP1], [OP2]
S3	07/11/2024	20/11/2024	[OP2], [OP3]
S4	21/11/2024	04/12/2024	[OP3], [OP4]
S5	05/12/2024	18/12/2024	[OP3], [OP4], [OP5]
S6	19/12/2024	08/01/2025	[OP4], [OP5]
S7	09/01/2025	22/01/2025	[OP4], [OP5]

Tabla 4.1: Planificación de sprints

A modo de nota aclarativa, cabe señalar que los *sprints* número dos y seis tienen una duración superior al coincidir con periodos de ausencia por vacaciones del tutor y/o del autor del TFM. Además, en cada *sprint* se redactan simultáneamente los apartados correspondientes de la presente memoria escrita para cumplir con los objetivos indicados, logrando un PMV en el quinto *sprint*.

En la *Figura 4.8*, se muestra un diagrama de Gantt con la planificación e hitos del proyecto:

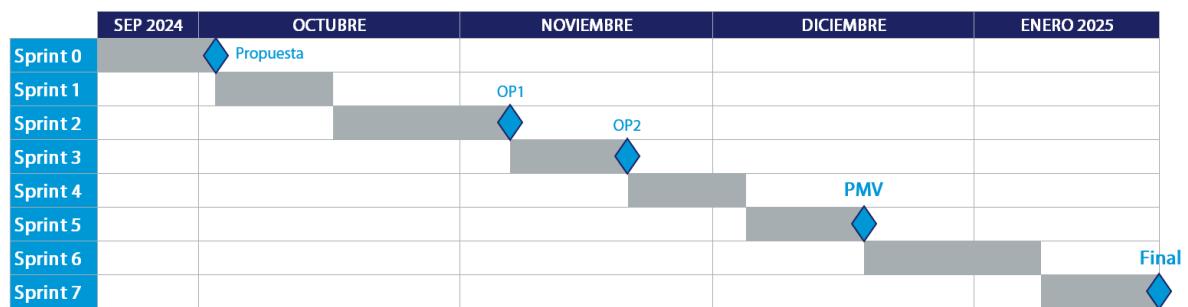


Figura 4.8: Diagrama de Gantt del proyecto

Una vez terminado el último *sprint* y habiendo hecho entrega de la memoria escrita, aunque no se incluye en la planificación de iteraciones ni en el diagrama de Gantt, se dedicará un último esfuerzo junto al tutor en la elaboración de las diapositivas y preparación para la defensa final del TFM ante el Tribunal de la Escuela Superior de Informática de Ciudad Real.

4.4 ESTIMACIÓN DE COSTES

En la planificación de costes del proyecto se realiza un cálculo de los costes asociados de personal de manera aproximada. Al tratarse de un trabajo académico por parte del tutor y alumno, se estiman los costes del esfuerzo realizado para los perfiles correspondientes, siguiendo las tablas del estudio de remuneración de la consultora de recursos humanos Michael Page para el año 2024 [30].

Es preciso remarcar que este esfuerzo ha sido ejecutado de manera autónoma, sin haber contado con alguna financiación comunitaria, apoyo o asesoramiento externo, por lo que ha sido ineludible materializar un empeño adicional y espíritu de emprendimiento e innovación asociado al proyecto.

No obstante, podría haber sido estudiado para su inclusión en el marco del programa RETECH de ciberseguridad promovido por INCIBE, vinculado al Plan de Recuperación, Transformación y Resiliencia como parte del componente 15 correspondiente a conectividad digital, impulso de la ciberseguridad y despliegue del 5G, en la inversión 7, ciberseguridad (C15.I7), para lograr el “*fortalecimiento de las capacidades de ciberseguridad de ciudadanos, pymes y profesionales*” [35].

Se toman como referencia las retribuciones económicas de los perfiles para la ciudad de Madrid, debido a su proximidad con la región de Castilla-La Mancha y, como sueldo base, el valor medio de la horquilla que se muestra en el citado estudio. En la *Tabla 4.2*, se indican los perfiles equivalentes que aparecen como referencia, junto con la experiencia y el salario bruto anual correspondiente:

Perfil	Perfil equivalente	Experiencia	Bruto año (1800h/año)
Alumno	<i>Security Engineer</i>	Entre 4 y 7 años	52.500,00€
Tutor	<i>CISO</i>	Mayor o igual a 8 años	125.000,00€

Tabla 4.2: Remuneración de perfiles equivalentes para el proyecto

Estos costes deben completarse a su vez con otros costes directos, gastos generales derivados y beneficio industrial para la empresa:

- Seguridad Social (SS) de la empresa: Promedio del 35% del salario bruto correspondiente.
- Gastos generales: Se estima en un 15%, vinculados a otros gastos asignados al empleado como alquileres, material de oficina, comunicaciones, equipos informáticos y licencias.
- Beneficio industrial: Se estima en un 10%, que obtendría una empresa como ganancias.

Los porcentajes anteriores, así como el método de selección de los salarios de referencia para los perfiles equivalentes, han sido extraídos de algunos de los estudios económicos [36] [37] publicados en las licitaciones en materia TIC del Gobierno de Castilla-La Mancha, en concreto, en el perfil del contratante correspondiente a la Secretaría General de Hacienda, Administraciones Públicas y Transformación Digital, disponibles en el portal web de contratación del Estado [38].

Por lo tanto, a continuación, separados en la *Tabla 4.3* y *Tabla 4.4* por cuestiones de espacio, se muestran los gastos de personal desglosados por perfil para este proyecto:

Perfil	Bruto año (1800h/año)	Coste/h año	SS empresa	c/H+ss (Coste Directo)	Gastos generales
	(1)	(2) = (1) /1800	(3) = (2)*0,35	(4) = (2)+(3)	(5) = (4)*0,15
Alumno	52.500,00€	29,17€	10,21€	39,38€	5,91€
Tutor	125.000,00€	69,45€	24,31€	93,76€	14,07€

Tabla 4.3: Cómputo de costes directos y gastos generales

Perfil	Subtotal	Beneficio industrial	Total euros/hora	Horas totales	Total euros
	(6) = (4)+(5)	(7) = (6)*0,10	(8) = (6)+(7)	(9)	(10) = (8)*(9)
Alumno	45,29€	4,53€	49,82€	245	12.205,90€
Tutor	107,83€	10,79€	118,62€	35	4.151,70€
Total	153,12€	15,32€	168,44€	280	16.357,60€

Tabla 4.4: Cómputo de costes totales de personal

En consecuencia, se calcula que para una empresa el presupuesto total ascendería a 16.357,60€, sin tener en cuenta la inclusión del IVA que supondría un incremento del 21% del mismo, en el supuesto caso de acometer el proyecto a través de una contratación pública formalizada, por ejemplo, por el propio Gobierno de Castilla-La Mancha.

Respecto a los costes asociados a la infraestructura y tecnología, se emplea un portátil propio y herramientas de software libre o, en su defecto, aquellas que cuenten con licencia de la UCLM para el alumnado como, por ejemplo, el sistema operativo Windows y el ecosistema de Microsoft 365.

4.5 MARCO TECNOLÓGICO

En este apartado se listan y describen aquellas tecnologías empleadas para la realización de este proyecto, distinguiendo entre herramientas software y hardware.

En la siguiente lista se indican las herramientas, programas y recursos tecnológicos utilizados:

- Sistema operativo: Microsoft Windows 11, licencia Education, de 64 bits.
- Documentación y modelado:
 - Microsoft Word: Programa dedicado para la creación y redacción de la memoria del presente TFM. Esta herramienta se encuentra incluida dentro de la cartera de productos de Microsoft 365, estando disponible para el estudiantado de la UCLM

- a través de un licenciamiento del área TIC [46]. Permite la edición en línea de manera simultánea de documentos compartidos entre el tutor y el alumno.
- Microsoft Excel: Programa incluido en Microsoft 365 que permite editar hojas de cálculo y que ha sido empleado para la elaboración de la plantilla de evaluación del modelo de madurez en las organizaciones.
 - Diagrams.net ([draw.io²⁴](https://www.draw.io/)): Herramienta utilizada para el diseño de los diagramas, figuras e infografías incluidas en la memoria escrita. Para ello se utilizan los colores corporativos de los logotipos y tipografías siguiendo el manual de imagen corporativa²⁵ de la Escuela Superior de Informática de Ciudad Real.
 - Obsidian²⁶: Software para la toma de notas y apuntes con sintaxis *Markdown*, utilizado por el alumno para captar ideas y planificar tareas.
 - Gestión del proyecto:
 - Microsoft Outlook: Incluida en Microsoft 365, sirve como herramienta de comunicación vía correo electrónico y ha sido utilizada para mantener conversaciones entre el tutor y el alumno, además de compartir documentos del proyecto y programar las reuniones de seguimiento en el calendario.
 - Microsoft Teams: Incluida en Microsoft 365, se trata de una herramienta colaborativa para el trabajo en equipo y comunicación entre personas vía mensajes o mediante videoconferencias, siendo empleada para las reuniones de seguimiento del proyecto con el tutor.
 - Accesibilidad (más información disponible en el *Anexo D. Accesibilidad del proyecto*):
 - Microsoft Excel y Word: Se han habilitado las herramientas de accesibilidad, gracias a que incluyen un asistente que funciona de manera nativa.
 - PAC 2024 (*PDF Accessibility Checker*)²⁷: Herramienta gratuita para evaluar el cumplimiento de controles de accesibilidad universal en documentos PDF.

Para finalizar, a continuación, se listan los medios y recursos físicos aprovechados:

- Ordenador portátil personal.
- Conexión a Internet de fibra óptica.

²⁴ <https://www.draw.io/>

²⁵ <https://esi.uclm.es/assets/uploads/2022/02/Manual-Logomarca-ESI-2021.pdf>

²⁶ <https://obsidian.md/>

²⁷ <https://pac.pdf-accessibility.org/en>

CAPÍTULO 5. RESULTADOS

Habiendo estudiado los antecedentes y estado de la cuestión, así como el método de trabajo manejado en el proyecto, en este capítulo se exploran en profundidad los resultados obtenidos finalmente a partir de la realización del TFM.

5.1 ANÁLISIS PESTEL

Comprendida la documentación analizada, se realiza un análisis inicial del contexto y los factores políticos, económicos, sociales, tecnológicos, ambientales y legales del proyecto desarrollado:

- Políticos: La creciente sofisticación de los actores malintencionados en el ciberespacio, como los grupos de amenazas persistentes avanzadas (APT's), pone en jaque la estabilidad y seguridad de los gobiernos y las instituciones públicas. Un ejemplo de ello es el caso del *spyware* Pegasus, detectado en actividades ilícitas con fines de espionaje. También, los conflictos internacionales pueden dar lugar a guerras híbridas que, en ocasiones, desembocan en campañas de sabotaje a las infraestructuras críticas de un país.
- Económicos: Los ciberataques pueden tener un impacto económico devastador en las organizaciones, causando pérdidas multimillonarias cada año. Según algunos informes recientes, la mayoría de estas amenazas encuentran su origen en errores humanos, por lo que son necesarias las inversiones en formación y sensibilización de los empleados.
- Sociales: La implantación de programas de concienciación en ciberseguridad supone un cambio cultural profundo en la organización a todos los niveles. La resistencia al cambio puede ser una barrera que dificulte una adaptación e implantación exitosa.
- Tecnológicos: En un entorno en constante evolución, las tecnologías emergentes como la inteligencia artificial, el Internet de las cosas (IoT) y las infraestructuras en la nube juegan un papel esencial. Al mismo tiempo que aportan un sinfín de ventajas, por el contrario, generan importantes riesgos amplificando los vectores de ataque en el ciberespacio.
- Ambientales: Los ciberataques a infraestructuras críticas pueden desencadenar una serie de consecuencias catastróficas para el medio ambiente. Entre los ejemplos encontramos ataques a los sistemas de control industrial o plantas energéticas que aumentan el riesgo de provocar fugas tóxicas, interrupciones en el suministro eléctrico o desastres naturales inducidos por un fallo intencionado de las infraestructuras.
- Legales: El marco normativo está en una continua adaptación frente a las amenazas que cada vez son más cuantiosas e innovadoras. Las estrategias y normativas estudiadas establecen requisitos obligatorios para las organizaciones, que ponen de manifiesto las necesidades de concienciar y sensibilizar al personal en el área de la ciberseguridad.

5.2 ANÁLISIS DAFO

De manera complementaria al análisis anterior, se elabora un análisis DAFO de las características del entorno en el que se enmarca el proyecto y el impacto que crean en el contexto actual:

- Debilidades: Permanecen dentro de la organización y generan un impacto negativo.
 - Resistencia al cambio cultural en la organización, dificultando la integración de nuevos hábitos relacionados con la ciberseguridad.
 - La potencial falta de apoyo y compromiso de una parte de la dirección para su aplicación, lo que podría limitar la inversión de recursos en el organismo.
 - Dificultades que pueden encontrar algunas personas con la tecnología, especialmente aquellas menos familiarizadas con herramientas digitales o procedimientos técnicos.
- Amenazas: Se encuentran fuera de la organización y producen un impacto negativo.
 - La naturaleza dinámica de los ataques en el ciberespacio, que requiere de actualización y concienciación en todo momento para responder adecuadamente.
 - El avance de las tecnologías en manos de los cibercriminales y su derivación en nuevas tácticas, técnicas y procedimientos de ataque cada vez más avanzados.
 - La competencia con entidades y organismos internacionales con mayor dotación de recursos, que pueden desarrollar soluciones alternativas de mayor alcance.
- Fortalezas: Pertencen al perímetro de la organización provocando un impacto positivo.
 - Amplios conocimientos y experiencia en el mundo laboral tanto del tutor como del alumno en el sector de la ciberseguridad y gestión de riesgos de seguridad, lo que garantiza una base sólida en aspectos técnicos, estratégicos y cumplimiento.
 - Aplicabilidad a todos los empleados de cualquier organización desde el comienzo, independientemente de sus conocimientos en ciberseguridad y tecnología, promoviendo una inclusión universal para que nadie se quede atrás.
 - Diseño abierto y modularidad del modelo resultante, que permite ser ajustado y ampliado de manera fácil y rápida en futuras versiones.
 - Enfoque centrado en las personas, lo que fomenta una mayor aceptación del modelo y facilita su integración en la cultura de las corporaciones.
- Oportunidades: Son externas a la organización y causan un impacto positivo.
 - Desarrollo de un proyecto de carácter innovador, revolucionario y pionero, que pretende dotar de una mejora sustancial de la concienciación de los usuarios de las organizaciones a todos los niveles.
 - Ayuda a mantener una buena imagen y reputación de los organismos en materia de ciberseguridad, generando confianza, eficiencia y resiliencia.
 - Posible conversión final en un estándar internacional para consolidar el modelo.

A continuación, en la *Figura 5.1* se resume esquemáticamente el análisis DAFO anterior:



Figura 5.1: Análisis DAFO

5.3 MODELO DE MADUREZ RESULTANTE

El modelo de madurez MM-CoUCS: Modelo de Madurez para la Concienciación a Usuarios en CiberSeguridad, en adelante, el modelo, gira en torno a las personas en base a tres conceptos enmarcados dentro de algunas asignaturas de este máster y muy relevantes dado el contexto actual:

- i) Innovación
- ii) Transformación digital
- iii) Ciberseguridad

El proyecto demuestra un carácter innovador que considera las últimas tendencias del sector y está alineado con las pretensiones del tejido regulatorio existente. Asimismo, el modelo está inmerso en un proceso universal de transformación digital con una gran cantidad de cambios culturales dentro de las entidades, sumando además el enorme reto que supone lidiar contra los innumerables riesgos de ciberseguridad generados del proceso de digitalización y modernización tecnológica.

Más allá de los puntos anteriores, algunas de las competencias específicas trabajadas guardan una cierta relación con otras asignaturas del máster correspondientes a gestión de procesos y servicios, así como la materia de dirección de tecnologías de la información. En el caso de la primera, se debe a la inclusión de contenidos en el temario ligados al estudio de modelos y estándares para la evaluación de la calidad, certificación y mejora continua de los procesos, productos y servicios. Respecto a la segunda, el trabajo realizado queda encuadrado en el bloque de dirección y gobierno de tecnologías de la información, complementando los conceptos de arquitectura de negocio empresarial, gestión del cambio y estrategias corporativas mediante la dirección de ciberseguridad.

Todo ello en conjunto, y situándolo desde una perspectiva que pone en el centro a las personas y sus necesidades específicas (ver *Figura 5.2*), presenta como resultado el modelo de madurez final.

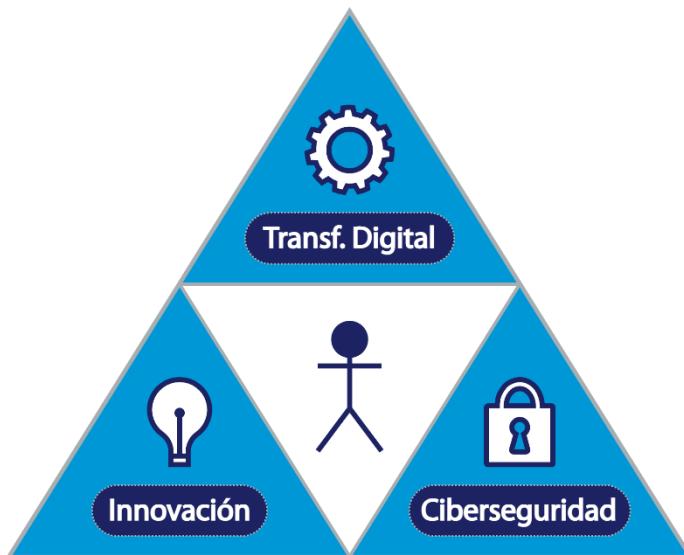


Figura 5.2: Contexto del modelo de madurez alrededor de las personas

La visión del proyecto consiste en convertirse en un modelo abierto, pionero y de referencia global en el sector para evaluar la madurez de las organizaciones en la concienciación de sus usuarios en ciberseguridad, que nace como un TFM realizado dentro de la UCLM y despegando desde la región castellanomanchega hacia el resto del espacio europeo y mundial.

El modelo tiene la misión de facilitar a las organizaciones los instrumentos clave para validar los esfuerzos dedicados en la concienciación de las personas de manera efectiva en ciberseguridad, sirviendo de ayuda para aumentar su confianza, seguridad y resiliencia dentro de la entidad, así como es de utilidad para el cumplimiento regulatorio y reducir los incidentes por fallos humanos.

En la *Figura 5.3*, se representan en una pirámide los elementos que conforman el modelo:



Figura 5.3: Componentes del modelo de madurez

En los siguientes apartados, se describen detalladamente cada uno de los elementos del modelo, proporcionando una relación integral de su estructura, funcionalidad y objetivos principales. Este análisis comprende desde los principios rectores que fundamentan su diseño, hasta los ejes, líneas de acción, criterios de éxito y métricas clave que permiten evaluar su efectiva implementación.

Cada componente del modelo está diseñado para facilitar su aplicación práctica en las corporaciones, promoviendo un enfoque progresivo y sistemático para mejorar la concienciación en ciberseguridad. A través de esta estructura organizada y flexible, el modelo busca ser una herramienta clara, adaptable y eficiente, aportando los instrumentos mínimos necesarios para guiar a los organismos en su camino hacia una cultura de ciberseguridad más robusta, sostenible y alineada con las imperantes demandas estratégicas y las exigencias regulatorias actuales.

5.4 PRINCIPIOS RECTORES

El modelo se rige por una serie de valores en forma de principios rectores fundamentales, diseñados para guiar tanto su definición inicial, como su implantación práctica y prueba en las organizaciones. Estos principios representan los pilares sobre los que se asienta el modelo, creando un ecosistema enfocado en promover una concienciación inclusiva y sostenible en ciberseguridad.

Para facilitar la identificación y memorización de estos principios, se ha elaborado una propuesta innovadora para este TFM creando una regla mnemotécnica bautizada como la “regla de las 5 C’s”, ya que, comenzando por dicha letra del abecedario, se establecen los siguientes cinco principios:

- Concienciación: Se trata del concepto central del modelo de madurez, cuyo objetivo principal es sensibilizar a las personas sobre los riesgos de ciberseguridad y la importancia de adoptar buenas prácticas en su entorno personal y profesional.
- Capacitación: Consiste en proveer a las personas de los conocimientos y habilidades necesarias para que puedan detectar y responder eficazmente ante amenazas e incidentes de ciberseguridad donde se vean involucradas.
- Coordinación: Garantiza que las acciones de concienciación estén alineadas y dirigidas desde los niveles más altos de la organización, propagando las mejores prácticas entre todas las áreas y departamentos.
- Colaboración: Busca fomentar una cultura y espíritu de apoyo mutuo dentro de la organización, donde cualquiera puede contribuir en la mejora de los procesos y prácticas.
- Compartición: Extiende la cultura de ciberseguridad más allá de los límites corporativos, promoviendo el intercambio de información, lecciones aprendidas y mejores prácticas con otras entidades de confianza, aportando la ventaja de mantenerse al día en cuanto al número y magnitud de amenazas emergentes en el espacio cibernético.



Figura 5.4: Regla de las 5 C's con los principios rectores del modelo

Los principios rectores de la *Figura 5.4* son aplicables de manera transversal a todos los elementos del modelo, desde los ejes y líneas de acción hasta los criterios de éxito, asegurando una base sólida y coherente para su desarrollo e implementación posterior cumpliendo con las estrategias estudiadas.

5.5 NIVELES DE MADUREZ

Para determinar el grado de madurez de las organizaciones, se establece una escala de tres niveles diferentes de madurez en concienciación en ciberseguridad a los usuarios finales.

Esta clasificación permite evaluar y categorizar a las corporaciones en función de su capacidad para formar y sensibilizar a su personal sobre las amenazas recientes de ciberseguridad, así como su preparación para prevenir y gestionar incidentes de seguridad relacionados con factores humanos.

Los niveles definidos, inspirados en el Esquema Nacional de Seguridad [3], reflejan un enfoque evolutivo que fomenta la mejora continua y la adopción de buenas prácticas. Cada nivel representa un escalón en la madurez organizativa en este ámbito, englobando desde los aspectos básicos hasta aquellas medidas más avanzadas y proactivas:

1. BAJO: En este nivel inicial la organización realiza esfuerzos mínimos de concienciación, limitándose a los aspectos básicos y conceptos fundamentales. Las acciones suelen ser esporádicas y de alcance limitado, pero, al menos, permiten sentar las bases iniciales.
2. MEDIO: En el segundo nivel la organización lleva a cabo programas de sensibilización más estructurados y regulares, buscando establecer una cultura básica de ciberseguridad. Las actividades de concienciación son más frecuentes y están orientadas a cubrir riesgos más actuales y específicos del entorno.
3. ALTO: En el nivel más avanzado la organización adopta un enfoque proactivo, integrando la ciberseguridad en su cultura organizativa de manera holística. Las acciones y ejercicios de sensibilización son continuos, avanzados y adaptados a las amenazas y riesgos emergentes.

El progreso entre niveles implica el cumplimiento acumulativo de una serie de criterios de éxito establecidos en el modelo. Esto significa que una organización debe satisfacer todos los requisitos del nivel inferior antes de aspirar al siguiente, garantizando así una evolución organizada, razonable y positiva hacia una mayor madurez en la concienciación en ciberseguridad en sus equipos de trabajo.

De este modo, los organismos logran avanzar de manera ordenada, consolidando una cultura de ciberseguridad que abarca desde los contenidos más básicos hasta los ejercicios más complejos. Esta orientación asegura que las entidades estén mejor preparadas para enfrentar los desafíos y nuevos peligros que asoman en el ecosistema digital.

5.6 EJES ESTRATÉGICOS

El modelo se encuentra articulado por una serie de ejes estructurales, concebidos como pilares temáticos que agrupan los distintos aspectos y factores clave relacionados para la concienciación y capacitación eficaz en ciberseguridad en los organismos participantes.

Estos ejes permiten estructurar y organizar el conocimiento de forma lógica y comprensible, facilitando su difusión y posterior asimilación en todos los niveles de la corporación. Gracias a esta segmentación, se promueve una comprensión clara y jerarquizada de las acciones y competencias necesarias para prevenir, identificar y responder con mayor éxito a los peligros de ciberseguridad en un entorno que se encuentra en constante evolución.

Para ello se han definido un total de 4 ejes estratégicos, los cuales se enumeran en la *Tabla 5.1* junto con los acrónimos empleados para facilitar su identificación (ID) en el modelo posteriormente:

Eje	Nombre	ID
1	Ingeniería social	isoc
2	Programas software	sw
3	Identidades digitales	id
4	Comportamientos en la red	red

Tabla 5.1: Relación de ejes y acrónimos

Finalmente, se destaca la importancia cada uno de los ejes estratégicos que componen el modelo:

- Eje 1. Ingeniería social: En el primer eje se tiene en cuenta el elevado riesgo proveniente desde el exterior a raíz de las principales técnicas de ingeniería social, las cuales son frecuentadas por los ciberdelincuentes para acometer fraudes en la red.
- Eje 2. Programas software: Este eje pone el foco en los peligros que pueden originar los programas dañinos o *malware* (*malicious software*), así como la aplicación de buenas prácticas y herramientas para garantizar un uso más seguro de los dispositivos.
- Eje 3. Identidades digitales: El cometido principal del tercer eje consiste en proteger y gestionar las credenciales en línea, conociendo las mejores prácticas de seguridad de las contraseñas y otros mecanismos adicionales de protección en la autenticación.
- Eje 4. Comportamientos en la red: En el último eje se pone de manifiesto el requisito de la formación en diversos aspectos de la ciberseguridad a través de la red en el ámbito laboral, como consecuencia de los nuevos entornos de tecnologías de la información, el auge del teletrabajo o del trabajo híbrido a distancia y los procesos de digitalización y transformación digital en las organizaciones.

5.7 LÍNEAS DE ACCIÓN

A su vez, cada eje está compuesto por un conjunto de líneas de acción que actúan como dominios de conocimiento más específicos, los cuales detallan y desglosan las áreas clave dentro de cada eje. La identificación de las líneas de acción del modelo se compone por el *ID* del eje al que pertenecen, seguido de un punto y un número de manera ordenada (por ejemplo: *isoc.1*, *isoc.2*, etc).

Este componente representa las actuaciones del modelo de manera estructurada, de forma que permiten establecer objetivos concretos y diseñar actividades de formación y concienciación a quienes van dirigidas. Mediante este enfoque modular se facilita la extensibilidad e implementación práctica del modelo en diferentes contextos profesionales, asegurando que cada dimensión de la concienciación en ciberseguridad sea cubierta de una manera más precisa.

El diseño de estas líneas de acción se inspira de manera análoga en las pautas de accesibilidad para el contenido web del estándar WCAG (*Web Content Accessibility Guidelines*), desarrolladas por el consorcio mundial para la web (W3C). Este paralelismo asegura que las líneas de acción se constituyan de forma clara, verificable y orientada a la mejora continua por niveles de cumplimiento, alineándose con otros estándares reconocidos a nivel internacional.

En el modelo se propone establecer 12 líneas de acción en total, que quedan asociadas a los cuatro ejes estratégicos citados previamente por niveles de la manera que se muestra en la *Tabla 5.2*:

Ejes y líneas de acción		Nivel de madurez		
		BAJO	MEDIO	ALTO
isoc	Ingeniería social			
isoc.1	Ingeniería social a través del correo electrónico	aplica	aplica	aplica
isoc.2	Ingeniería social a través del teléfono	aplica	aplica	aplica
isoc.3	Redes sociales	n.a.	aplica	aplica
isoc.4	Bulos y noticias falsas	n.a.	aplica	aplica
sw	Programas software			
sw.1	Seguridad en el software	aplica	aplica	aplica
sw.2	Programas software dañinos	aplica	aplica	aplica
id	Identidades digitales			
id.1	Credenciales de acceso	aplica	aplica	aplica
id.2	Autenticación más segura	n.a.	aplica	aplica
id.3	Gestión de cuentas corporativas	n.a.	aplica	aplica
red	Comportamientos en la red			
red.1	Redes públicas	aplica	aplica	aplica
red.2	Teletrabajo	n.a.	aplica	aplica
red.3	Seguridad de la información	n.a.	aplica	aplica

Tabla 5.2: Correspondencia de ejes, líneas de acción y niveles de madurez exigidos

Para elaborar la tabla anterior se han tenido en cuenta las siguientes convenciones:

- a) La primera columna indica el acrónimo del eje estratégico e identificador de las líneas de acción correspondientes, siguiendo el formato descrito para cada uno de ellos.
- b) La segunda columna indica el nombre del eje estratégico y los nombres de las sucesivas líneas de acción asociadas.
- c) Las columnas en la posición tercera, cuarta y quinta hacen referencia a la aplicabilidad de cada línea de acción en función de su exigencia por cada nivel de madurez.
- d) Para indicar que una línea de acción se debe aplicar en un nivel de madurez concreto se emplea el término «*aplica*». Respecto a las líneas de acción no exigidas para alcanzar un nivel de madurez se denota con la voz «*n.a.*», cuyo significado es «*no aplica*».
- e) Se han empleado los colores verde, amarillo y rojo para favorecer la comprensión de las líneas de acción que aplican a cada nivel de madurez del modelo. El color verde indica que la línea de acción en cuestión contiene criterios de éxito que aplican para el nivel bajo o superior, mientras que en color amarillo se representan aquellos que aplican para nivel medio o superior y, por último, en color rojo tenemos los que se exigen para nivel alto.
- f) En el caso de aquellas líneas de acción que no aplican a los niveles de madurez inferiores se utiliza de fondo el color blanco en las respectivas columnas.

Como bien se observa en dicha tabla, todos los ejes estratégicos que integran el modelo aplican desde el nivel de madurez más bajo. Si bien, es cierto que no todas las líneas de acción que incorporan son exigibles desde dicho nivel, sino que algunas de ellas se requieren a partir del nivel medio.

A fin de conocer en mayor detalle las líneas de acción y su vinculación con los cuatro ejes que constituyen el modelo, se explica el valor aportado por cada una de ellas en la concienciación a los usuarios de las organizaciones en ciberseguridad, fortaleciendo así una cultura digital más segura.

Para el primer eje, correspondiente a ingeniería social (isoc), se proponen las siguientes cuatro líneas de acción:

1. Ingeniería social a través del correo electrónico: Esta primera línea de acción representa uno de los vectores de entrada a las organizaciones más atractivos y típicos para quienes tratan de realizar un uso maligno a través del ciberespacio, para lo cual se realizan actividades de concienciación y entrenamiento para aplicar un uso más seguro del correo electrónico a todos los niveles de la organización.
2. Ingeniería social a través del teléfono: En este caso, de manera continuista con la línea previa, se llevan a cabo ejercicios de capacitación y sensibilización en los peligros que acechan el ciberespacio por la vía telefónica, al ser un elemento muy utilizado en estafas dirigidas y de diversa índole en el seno de las corporaciones.

3. Redes sociales: Tras el auge que vivieron las redes sociales en la denominada web 2.0, progresivamente han ido surgiendo una serie de fraudes digitales u otros usos ilegales que pueden poner en jaque a las organizaciones. Por lo cual, la educación en las prácticas recomendadas de seguridad en este aspecto se convierte en indispensable en el presente.
4. Bulos y noticias falsas: Derivada de la línea anterior, es habitual encontrar contenidos que se comparten y difunden rápidamente en Internet que no siempre son verdaderos. Aprender a detectarlos o identificarlos es un punto cada vez más significativo, al mismo tiempo que se vuelve una tarea más compleja tras emerger y democratizarse el uso de la Inteligencia Artificial en la actualidad.



Figura 5.5: Líneas de acción del eje 1. Ingeniería social (isoc)

En el segundo de los ejes, programas software (sw), se plantean dos líneas de acción asociadas:

1. Seguridad en el software: Pone el foco en el valor esencial del software en el día a día en las organizaciones, resaltando el interés de implantar medidas preventivas, así como la trascendencia de conocer las directrices óptimas e incentivar un uso más seguro y sensato dentro de los entornos profesionales.
2. Programas software dañinos: Más allá de las bondades y oportunidades ofrecidas por el software, existen una serie de programas que, de manera malintencionada, buscan aprovecharse de necesidades o urgencia de las personas para realizar actividades ilícitas en sus dispositivos. Por esta razón, se debe enseñar e impartir acciones formativas para facilitar la identificación de las amenazas de tipo *malware* en el contexto empresarial.

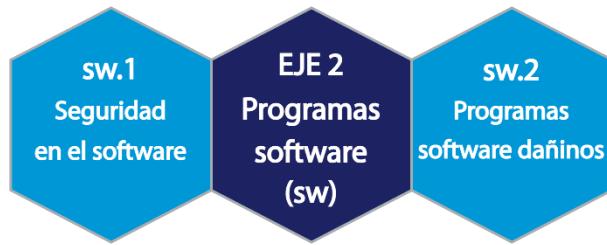


Figura 5.6: Líneas de acción del eje 2. Programas software (sw)

En cuanto al tercer eje, nombrado identidades digitales (id), se presentan tres líneas de acción más:

1. Credenciales de acceso: Las identidades corporativas son un activo muy valioso y atractivo en los foros y mercados ilegales de venta de credenciales, lo que aumenta significativamente los potenciales riesgos para el acceso ilícito a las organizaciones. Por esta razón, se debe cuidar y preservar la seguridad de sus cuentas profesionales, contraseñas y datos asociados en la máxima medida de lo posible.
2. Autenticación más segura: Como barreras de protección adicionales a las credenciales corporativas, es posible configurar segundos o, incluso, terceros mecanismos de autenticación al objeto de resguardar las mismas, resultando indefectible el hecho de instruir los beneficios añadidos a partir de estas valiosas opciones de seguridad.
3. Gestión de cuentas corporativas: Durante el ciclo de vida de las cuentas de las entidades pueden aparecer accesos indebidos a las mismas originados por alguna brecha de seguridad o fuga de datos. En este sentido, se debe formar a las personas en aras de efectuar una óptima gestión de las identidades digitales donde desempeñan su actividad.

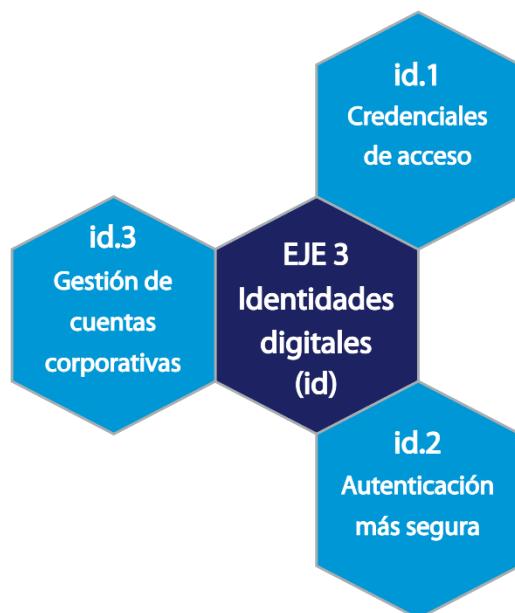


Figura 5.7: Líneas de acción del eje 3. Identidades digitales (id)

En el cuarto y último eje, comportamiento en la red (red), se establecen otras tres líneas de acción:

1. Redes públicas: Se debe hacer hincapié en un uso apropiado y responsable de las redes públicas u otro tipo de comunicaciones inalámbricas de los dispositivos en línea, prestando especial atención a las medidas de protección básicas, así como en la navegación segura y consciente por Internet para evitar posibles conflictos en este entorno.
2. Teletrabajo: A partir de la pandemia de COVID-19 se abrió un panorama que permitió desempeñar las actividades profesionales de manera remota. No obstante, esto introdujo masivamente nuevas formas de abrir y conectarse a las redes internas de las corporaciones, generando un punto de acceso a las mismas muy seductor para la ciberdelincuencia, ocasionando más problemas críticos de seguridad.
3. Seguridad de la información: En último lugar, los archivos, documentos e información compartida y expuesta en la red adquieren una significante valía si no se realiza de manera oportuna. Bajo este marco, se alecciona a los individuos en ejecutar las prácticas idóneas y los mecanismos corporativos existentes para proteger la confidencialidad en las situaciones que lo precisen debido a la criticidad de la información manejada.



Figura 5.8: Líneas de acción del eje 4. Comportamientos en la red (red)

5.8 CRITERIOS DE ÉXITO

Vinculados a cada línea de acción, encontramos los criterios de éxito, definidos como requisitos específicos y medibles que permiten evaluar el grado de cumplimiento de los objetivos asociados a cada eje y línea de acción del modelo. En consonancia con la identificación de los elementos vistos anteriormente, los criterios tendrán un identificador formado por el *ID* del eje y línea de acción

correspondiente, seguido de un punto, una letra de manera ordenada y un paréntesis final de cierre (por ejemplo, algunos de los criterios de éxito serían: *isoc.1.a*, *isoc.1.b*), etc).

Estos criterios de éxito representan una base trascendental sobre la que se determina el nivel de madurez alcanzado por una organización en términos de concienciación en ciberseguridad, funcionando como un instrumento clave para guiar y monitorear el progreso hacia una cultura de seguridad organizativa cada vez más resiliente y robusta.

La creación de estos criterios de éxito, inspirada por analogía en los criterios de conformidad que se plantean en la norma UNE-EN 301549, sigue un enfoque estructurado que cumple con los principios rectores definidos. Dicha norma establece requisitos de accesibilidad para productos y servicios TIC agrupándolos en tres niveles de conformidad, garantizando una progresión lógica y escalable desde niveles básicos hasta avanzados, fomentando la mejora continua en este aspecto.

Para ello, se han establecido 33 criterios de éxito, estando cada uno de ellos asociado con sus correspondientes métricas por nivel. En concreto, se ha determinado sobre el total de los criterios de éxito que 11 de ellos aplican para alcanzar el nivel bajo, 25 para conseguir el nivel medio y los 33 en su totalidad son necesarios para superar el nivel de madurez más alto en las métricas que demanden.

En la *Tabla 5.3*, se muestra un recuento de los criterios de éxito establecidos en el modelo, clasificados por ejes y desglosados por los tres niveles de madurez según su aplicación:

Componente	ID	Nivel de madurez		
		BAJO	MEDIO	ALTO
Eje 1. Ingeniería social	isoc	2	7	10
Eje 2. Programas software	sw	6	6	7
Eje 3. Identidades digitales	id	1	5	7
Eje 4. Comportamientos en la red	red	2	7	9
TOTAL (criterios de éxito)		11	25	33

Tabla 5.3: Criterios de éxito por ejes y niveles de madurez

No obstante, por puntualizar, algunos criterios de éxito podrán compartir la misma métrica entre distintos niveles, al igual que existen otras líneas de acción que no aplican desde el nivel inferior, sino que son exigidas únicamente a partir de niveles de madurez superiores.

En el *Anexo A. Relación de componentes del modelo*, se incluye una tabla diferenciada por cada uno de los ejes estratégicos, incluyendo sus respectivas líneas de acción y criterios de éxito específicos asociados para su cumplimiento en los distintos niveles de madurez.

Para la elaboración de las tablas se sigue la convención de columnas descrita a continuación:

- a) Para comenzar, en la primera columna se determina un identificador del componente descrito en la fila, bien sea una línea de acción o un criterio de éxito.

- b) En la segunda columna, se especifica el nombre de dicho componente del modelo.
- c) La tercera columna muestra el nivel mínimo requerido para cada criterio de éxito.
- d) En las columnas cuarta, quinta y sexta se establecen las métricas exigidas para cada criterio de éxito en los niveles de madurez bajo, medio y alto, respectivamente.
- e) En la séptima y última columna se declara el tipo del rango de valores de las métricas.

A continuación, se describen los convenios utilizados para especificar individualmente cada uno de los criterios de éxito (ver *Anexo B. Criterios de éxito*) vinculados a las líneas de acción pertenecientes en el modelo:

- a) En primer lugar, se introduce y describe someramente cada uno de los criterios de éxito definidos y se destaca su relevancia dentro del modelo.
- b) Posteriormente, se resume en una tabla el criterio de éxito a evaluar con las métricas convenientes para alcanzar cada uno de los niveles de madurez exigidos. De forma análoga a la *Tabla 5.2*, se emplea el mismo código de colores para cada nivel de madurez.
- c) Por último, se detalla la aplicación de las métricas o indicadores para validar la consecución de cada uno de los niveles de madurez establecidos.

Dada la extensión de los criterios definidos en el modelo, en el *Anexo B. Criterios de éxito*, se estudia la su aplicación efectiva de cada uno de ellos en el modelo.

5.9 MÉTRICAS O KPI'S

Finalmente, encontramos el último elemento del modelo que conforma la base de la pirámide, el cual proporciona los mecanismos necesarios para evaluar por niveles de madurez el cumplimiento y la eficacia de los criterios de éxito específicos en el modelo.

Este componente es fundamental para garantizar que la implementación de los ejes estratégicos, líneas de acción y criterios de éxito no solo se lleve a cabo de manera adecuada, sino que, también, genere un impacto tangible en la concienciación en ciberseguridad dentro de las organizaciones.

Para llevar a cabo esta validación, se emplearán indicadores clave de rendimiento o *KPI's (Key Performance Indicators)*, diseñados para medir el nivel de progreso y éxito en función de las metas establecidas en cada nivel de madurez. Los indicadores están categorizados en dos tipos principales, lo que permite efectuar una evaluación integral y adaptada a diferentes dimensiones:

- Cumplimiento: Este tipo de indicador utiliza opciones binarias o escalas simplificadas (como sí, parcialmente o no) para determinar si los requisitos específicos se han cumplido.
- Periodicidad: Se expresan mediante valores temporales periódicos, proporcionando una visión precisa y medible en el tiempo del cumplimiento de los criterios de éxito.

La combinación de estas métricas proporciona una visión holística sobre el desempeño organizacional, permitiendo identificar por cada eje las fortalezas, debilidades y áreas de mejora. Además, estos indicadores se adaptan al nivel de madurez de cada organización, garantizando una evolución gradual, asumible y realista hacia mayores niveles de concienciación en ciberseguridad.

Para representar los resultados obtenidos en cada uno de los ejes estratégicos del modelo, se utilizan diagramas de *Kiviat*, también conocidos como gráficos de radar o de telaraña, debido a su característico diseño. Para ello, se emplea un plano bidimensional formado por, al menos, tres ejes con características cuantificadas que parten del mismo punto céntrico del polígono que se conforma.

En esta ocasión, en cada uno de los ejes del gráfico se representan los criterios de éxito evaluados en el eje al que pertenecen en el modelo, tomando un total de cuatro posibles valores en función del nivel de madurez alcanzado (alto, medio o bajo) para dicho criterio o, si se diera el caso, un cuarto valor en el que no se haya cumplido el criterio evaluado, situado en el punto central del diagrama.

5.10 APLICACIÓN Y EVALUACIÓN DEL MODELO

Como se ha señalado en apartados anteriores, el modelo se caracteriza por poseer un enfoque progresivo, en el cual se debe comenzar estudiando su aplicación desde los niveles inferiores. Debido a este planteamiento, las organizaciones pueden abordar inicialmente los conceptos más básicos y desarrollar gradualmente aquellas actividades y capacidades más avanzadas, garantizando así una implementación sólida y eficaz del proceso.

La aplicación del modelo además de que persigue cumplir con los criterios de éxito definidos, también pretende integrarlos dentro de la operativa diaria de la organización. Para ello, es necesario el compromiso desde la alta dirección hasta el resto de los equipos operativos, asegurando una coordinación efectiva entre todos los niveles y satisfaciendo los cinco principios rectores del modelo.

Adicionalmente, las organizaciones deben evaluar periódicamente su desempeño mediante las métricas establecidas en el modelo, permitiendo identificar áreas de mejora y garantizar una evolución continua en su nivel de madurez en concienciación en ciberseguridad.

Para la evaluación del modelo se auditará el cumplimiento individualizado de cada uno de los criterios de éxito, en función de las métricas exigidas para cada nivel de madurez. Este proceso de auditoría permitirá a las organizaciones identificar de manera clara y precisa su posición actual dentro del modelo, así como determinar las temáticas en las que deben enfocar sus esfuerzos de mejora.

La validación del modelo contempla tanto las evaluaciones internas, realizadas por los propios responsables de ciberseguridad y tecnologías de la organización, como auditorías externas llevadas a cabo por terceras entidades especializadas.

Para realizar la valoración se facilita un artefacto en un documento Excel a modo de plantilla, abierto y disponible para su descarga en el siguiente repositorio de GitHub del alumno: <https://github.com/mdelacal/muii-tfm>. Este documento incluye una hoja por cada eje estratégico del modelo para su validación, así como otras de información, informe final y cuadro de mandos.

Se llevará a cabo una evaluación del modelo de madurez tomando de ejemplo el contexto de una Administración Pública, como podría ser la Universidad de Castilla-La Mancha o el Gobierno de Castilla-La Mancha, al tratarse de organizaciones bien conocidas para el tutor y autor de este TFM.

Además, según el último informe de panorama de amenazas publicado en el año 2024 por ENISA [15], se ha observado que las Administraciones Públicas se posicionan en el sector que registró más incidentes de seguridad en la Unión Europea (19% del total entre julio de 2023 y junio de 2024) con una amplia diferencia respecto al segundo sector más afectado (ver *Figura 5.9*). Este dato, combinado con el párrafo anterior, crea una atmósfera idónea para evaluar el modelo en un caso de uso.

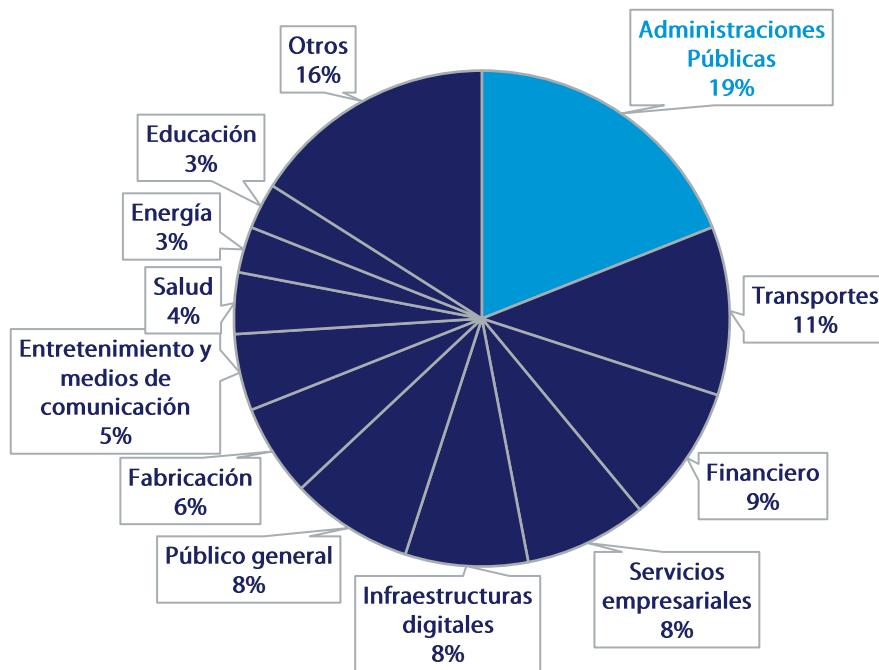


Figura 5.9: Incidentes de seguridad por sectores

Es importante y oportuno aclarar que los resultados exhibidos en este trabajo no son vinculantes a las instituciones públicas citadas, mostrando en su lugar datos sintéticos con el motivo de mantener la confidencialidad, privacidad y otras cuestiones de seguridad de la información en dichas entidades.

Gracias a este caso de uso, se puede llevar a cabo una aplicación realista de los múltiples componentes definidos en el modelo junto con la posterior validación de los indicadores y métricas requeridas para, así, auditar finalmente el nivel de cumplimiento en el escenario estudiado.

Una vez acometidas las valoraciones de todos los criterios de éxito que forman parte del modelo, se procede a mostrar los resultados obtenidos en el contexto del caso de uso implantado por cada eje. Para mayor detalle, en el *Anexo C. Resultados del caso de uso* se presentan completamente las valoraciones obtenidas en la evaluación de cada uno de los criterios de éxito.

En el primer eje, correspondiente a ingeniería social, a continuación, en la *Tabla 5.4* se resumen los resultados obtenidos en la evaluación:

Componente	ID	Nombre	Nivel
Eje 1	isoc	Ingeniería social	
Línea de acción	isoc.1	Ingeniería social a través del correo electrónico	
	Criterio de éxito	isoc.1.a) Píldoras formativas correo electrónico	MEDIO
	Criterio de éxito	isoc.1.b) Reportes de correos sospechosos	MEDIO
	Criterio de éxito	isoc.1.c) Campañas de phishing corporativas	ALTO
Línea de acción	isoc.2	Ingeniería social a través del teléfono	
	Criterio de éxito	isoc.2.a) Píldoras formativas llamadas telefónicas	MEDIO
	Criterio de éxito	isoc.2.b) Reportes de llamadas sospechosas	MEDIO
	Criterio de éxito	isoc.2.c) Simulaciones de llamadas fraudulentas	ALTO
Línea de acción	isoc.3	Redes sociales	
	Criterio de éxito	isoc.3.a) Píldoras formativas redes sociales	MEDIO
	Criterio de éxito	isoc.3.b) Talleres prácticos de fraudes digitales	-
Línea de acción	isoc.4	Redes sociales	
	Criterio de éxito	isoc.4.a) Píldoras de bulos y noticias falsas	MEDIO
	Criterio de éxito	isoc.4.b) Píldoras de contenidos manipulados con IA	-

Tabla 5.4: Evaluación de criterios de éxito en el eje 1

Se comienza realizando un análisis de resultados del primer eje, por cada línea de acción:

- isoc.1: Se consigue alcanzar el nivel medio en los dos primeros criterios de éxito y un nivel alto en el tercero, por lo que ya no es posible para la organización alcanzar el nivel de madurez más alto en la evaluación del modelo de manera global.
- isoc.2: De nuevo, se cumplen los dos primeros criterios de éxito con las métricas requeridas para nivel medio, mientras que el restante se satisface para nivel alto.
- isoc.3: En el primer criterio se alcanza el nivel medio y en el segundo, exigible únicamente para nivel alto, no se consigue validar favorablemente, lo cual se denota con el signo ortográfico de un guion (-).
- isoc.4: De la misma manera, en la cuarta línea de acción se logra el nivel medio en el primero de los criterios, mientras que en el segundo no se alcanza el nivel alto exigido.
- Por lo tanto, el resultado obtenido en este primer eje del modelo para los criterios de éxito y métricas asociadas se corresponde con el nivel de madurez MEDIO.

En el segundo eje, correspondiente a programas software, a continuación, en la *Tabla 5.5* se resumen los resultados obtenidos en la evaluación:

Componente	ID	Nombre	Nivel
Eje 2	sw	Programas software	
Línea de acción	sw.1	Seguridad en el software	
Criterio de éxito	sw.1.a)	Actualizaciones de seguridad	MEDIO
Criterio de éxito	sw.1.b)	Programas antivirus o similares	ALTO
Criterio de éxito	sw.1.c)	Copias de seguridad	ALTO
Línea de acción	sw.2	Programas software dañinos	
Criterio de éxito	sw.2.a)	Píldoras formativas malware	MEDIO
Criterio de éxito	sw.2.b)	Identificar los tipos de malware	ALTO
Criterio de éxito	sw.2.c)	Descarga de sitios oficiales y fiables	ALTO
Criterio de éxito	sw.2.d)	Simulación de ataques internos	-

Tabla 5.5: Evaluación de criterios de éxito en el eje 2

Seguidamente, se realiza un análisis, por cada línea de acción, de resultados del eje número dos:

- sw.1: Se compone de tres criterios de éxito exigibles desde nivel bajo, alcanzando el nivel medio en el primero. En el segundo y el tercero se cosecha un nivel de madurez alto.
- sw.2: Formado por cuatro criterios de éxito, donde los tres primeros son requeridos desde el nivel bajo y, el cuarto de ellos, exclusivamente para el nivel de madurez alto. El primero cumple con las métricas requeridas en el nivel medio, mientras que el segundo y el tercero hacen lo propio para el nivel alto y el último de ellos no se ratifica satisfactoriamente.
- Así, en la evaluación del segundo eje se obtiene un nivel de madurez MEDIO.

En el tercer eje, correspondiente a identidades digitales, a continuación, en la *Tabla 5.6* se resumen los resultados obtenidos en la evaluación:

Componente	ID	Nombre	Nivel
Eje 3	id	Identidades digitales	
Línea de acción	id.1	Credenciales de acceso	
Criterio de éxito	id.1.a)	Píldoras formativas contraseñas	ALTO
Criterio de éxito	id.1.b)	Cambio de contraseñas	ALTO
Línea de acción	id.2	Autenticación más segura	
Criterio de éxito	id.2.a)	Segundo factor de autenticación	ALTO
Criterio de éxito	id.2.b)	Tercer factor de autenticación	-
Línea de acción	id.3	Gestión de cuentas corporativas	
Criterio de éxito	id.3.a)	Píldoras formativas brechas de seguridad	MEDIO
Criterio de éxito	id.3.b)	Gestores de contraseñas	-
Criterio de éxito	id.3.c)	Reporte de accesos sospechosos	ALTO

Tabla 5.6: Evaluación de criterios de éxito en el eje 3

Posteriormente, se realiza un estudio de resultados del tercer eje, por cada línea de acción:

- id.1: Compuesto por dos criterios de éxito, se adquiere un nivel de madurez alto en ambos, dando lugar a la primera línea de acción en la que se consigue este hito.
- id.2: Nuevamente, se compone de dos criterios de éxito, aunque esta vez con distinto resultado. En el primero se obtiene un nivel alto mientras que, en el segundo, exclusivo para el nivel de madurez más alto, no se cumplimenta finalmente.
- id.3: Para cerrar el tercer eje se evalúan tres criterios de éxito, consiguiendo que el primero tuviese nivel medio, el segundo de ellos no se cumple con éxito ya que sólo aplica a nivel alto y el tercero sí se alcanza para el nivel de madurez alto.
- Consecuentemente, el nivel de madurez alcanzado para el eje tres es MEDIO.

En el cuarto y último eje, que versa sobre los comportamientos en la red, a continuación, en la *Tabla 5.7* se resumen los resultados obtenidos en la evaluación:

Componente	ID	Nombre	Nivel
 Eje 4	red	Comportamientos en la red	
 Línea de acción	red.1	Redes públicas	
	Criterio de éxito red.1.a)	Píldoras sobre navegación por Internet	MEDIO
	Criterio de éxito red.1.b)	Conexión a redes Wi-Fi públicas	ALTO
	Criterio de éxito red.1.c)	Otras conexiones inalámbricas	MEDIO
 Línea de acción	red.2	Teletrabajo	
	Criterio de éxito red.2.a)	Píldoras sobre teletrabajo	MEDIO
	Criterio de éxito red.2.b)	Redes privadas virtuales	MEDIO
 Línea de acción	red.3	Seguridad de la información	
	Criterio de éxito red.3.a)	Píldoras seguridad de la información corporativa	MEDIO
	Criterio de éxito red.3.b)	Compartición de documentos	MEDIO
	Criterio de éxito red.3.c)	Cifrado de archivos y mensajes	-
	Criterio de éxito red.3.d)	Exposición de metadatos	-

Tabla 5.7: Evaluación de criterios de éxito en el eje 4

Por último, se realiza un examen de los resultados por cada línea de acción del eje número cuatro:

- red.1: En la primera línea de acción, se observa la consecución de nivel medio en dos de los tres criterios de éxito definidos, mientras que en el restante se consigue un nivel alto.
- red.2: Constituida por dos criterios de éxito, que aplican a partir del nivel medio, en ambos se consigue superar el nivel de madurez medio.
- red.3: En la última línea de acción del modelo, formada por cuatro criterios de éxito, de los cuales los dos primeros aplican a partir de nivel medio, y el resto para nivel alto, se alcanza el nivel de madurez medio en los dos primeros, mientras que en los dos restantes no se consigue alcanzar el nivel alto exigido para su cumplimiento.

- Finalmente, se determina que, para el último eje del modelo, nuevamente se ha conseguido superar el nivel de madurez MEDIO.

Más abajo, en la *Figura 5.10*, *Figura 5.11*, *Figura 5.12* y *Figura 5.13* se representan visualmente mediante diagramas de Kiviat o de telaraña los resultados obtenidos en la evaluación de cada uno de los criterios de éxito del modelo, de manera ordenada en función del eje estratégico al que pertenecen.

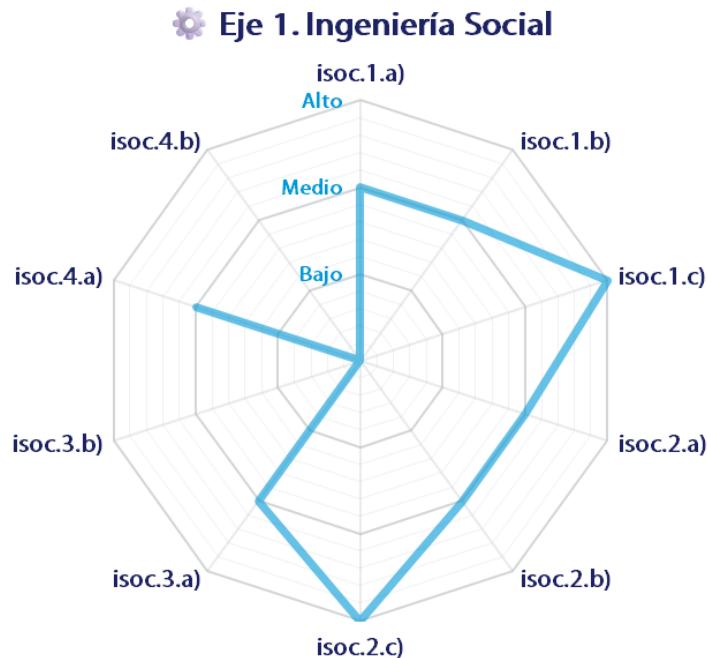


Figura 5.10: Diagrama de Kiviat de resultados del eje 1

Eje 2. Programas software

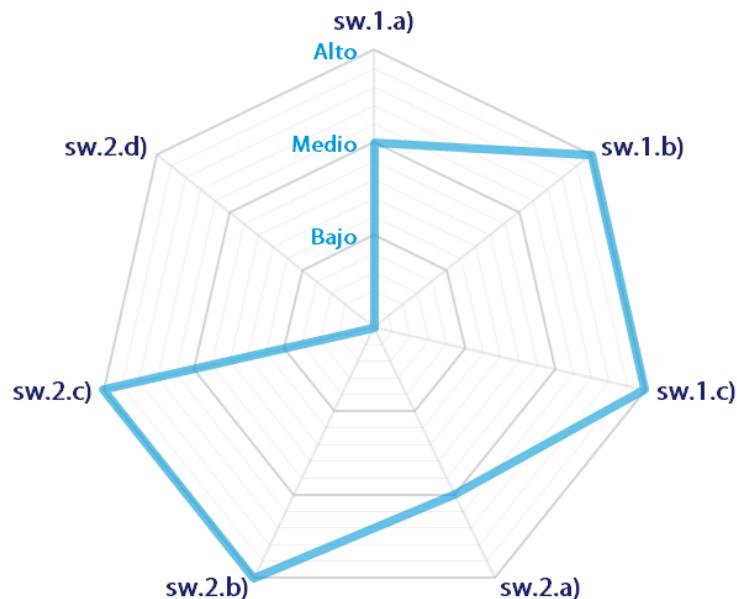


Figura 5.11: Diagrama de Kiviat de resultados del eje 2

Eje 3. Identidades digitales

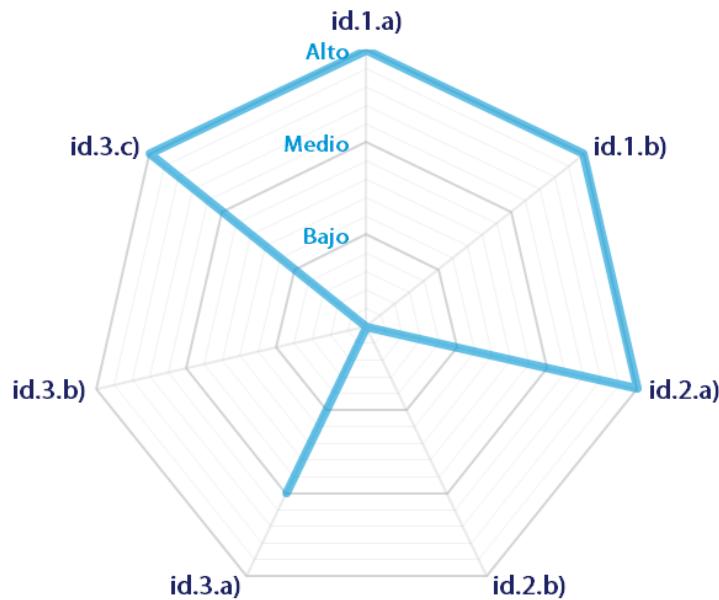


Figura 5.12: Diagrama de Kiviat de resultados del eje 3

Eje 4. Comportamientos en la red

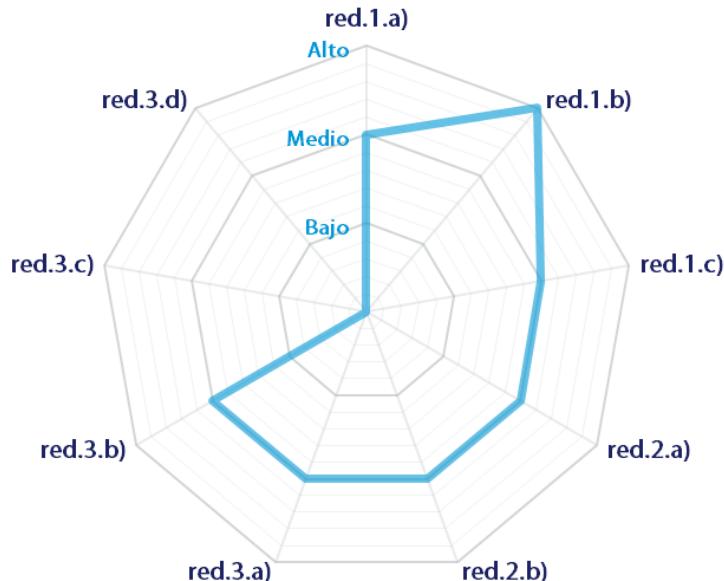


Figura 5.13: Diagrama de Kiviat de resultados del eje 4

En conclusión, y tras haber completado el análisis de cumplimiento global, en el que se ha alcanzado el nivel medio de madurez en todos y cada uno de los ejes estratégicos que conforman el modelo, la evaluación final correspondiente a la organización para la concienciación de sus usuarios en materia de ciberseguridad en este caso de uso se corresponde con el nivel de madurez MEDIO.

En la *Tabla 5.8* se expone el informe final de resultados agregados por ejes y niveles en la evaluación realizada de los criterios de éxito del modelo (donde “T” significa “total” de criterios):

Eje	Criterios de éxito								Nivel de madurez				
	BAJO				MEDIO								
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	T	%	<input checked="" type="checkbox"/>	<input type="checkbox"/>	T	%	<input checked="" type="checkbox"/>	<input type="checkbox"/>	T	%	
1	2	0	2	100	7	0	7	100	2	8	10	20,0	MEDIO
2	6	0	6	100	6	0	6	100	4	3	7	57,1	MEDIO
3	1	0	1	100	5	0	5	100	4	3	7	57,1	MEDIO
4	2	0	2	100	7	0	7	100	1	8	9	11,1	MEDIO
Total	11	0	11	100	25	0	25	100	11	22	33	33,3	MEDIO

Tabla 5.8: Informe final de resultados en el caso de uso

Como se puede observar, en el caso de uso contemplado se lograría alcanzar el nivel de madurez MEDIO, dado que se han cumplido el 100% de los criterios de éxito requeridos para los niveles bajo y medio. En esta situación, la organización habría conseguido cumplir con las métricas establecidas en 25 de los 33 criterios de éxito totales del modelo para alcanzar el nivel medio.

Seguidamente, la entidad estaría en disposición de comprobar cuáles son los siguientes pasos para subir hasta el nivel de madurez alto. En este escenario, de los 33 criterios de éxito que se exigen para conseguir dicho nivel, únicamente estaría cumpliendo con 11 de ellos, lo que, consecuentemente, representa un alcance del 33,3% sobre el total de los criterios de éxito para el nivel más alto.

A continuación, se desglosa la evaluación de los resultados por los cuatro ejes del modelo para la consecución del nivel de madurez alto, ordenados de mejor a peor en función del porcentaje logrado:

- En primer lugar, se observa que para el eje 2 se habrían obtenido resultados favorables en cuatro de los siete criterios de éxito, lo que representa un 57,1% y lo sitúa como un eje candidato para cubrir próximamente el nivel más alto.
- Empatado con el anterior, se encuentra el eje 3 con un 57,1% de criterios de éxito cumplidos, lo cual supone haber superado favorablemente cuatro sobre los siete criterios evaluados en dicho eje y estar de nuevo a sólo tres criterios de éxito alcanzar el nivel alto.
- En tercera posición, tenemos el eje 1, donde se han cubierto exitosamente un 20% de los criterios, es decir, se ha conseguido superar dos de los diez criterios de éxito que se establecieron en este eje.
- Por último, los peores resultados se han registrado en el eje 4, cosechando apenas un 11,1% de los criterios de éxito, lo que se traduce en el cumplimiento de un único criterio de los nueve existentes y la amplia necesidad de mejorar para su futura consecución.

Para finalizar, en la *Figura 5.14*, *Figura 5.15*, *Figura 5.16* y *Figura 5.17*, se muestran los resultados agregados del cumplimiento por nivel de madurez para cada uno de los ejes estratégicos en gráficos de tarta:

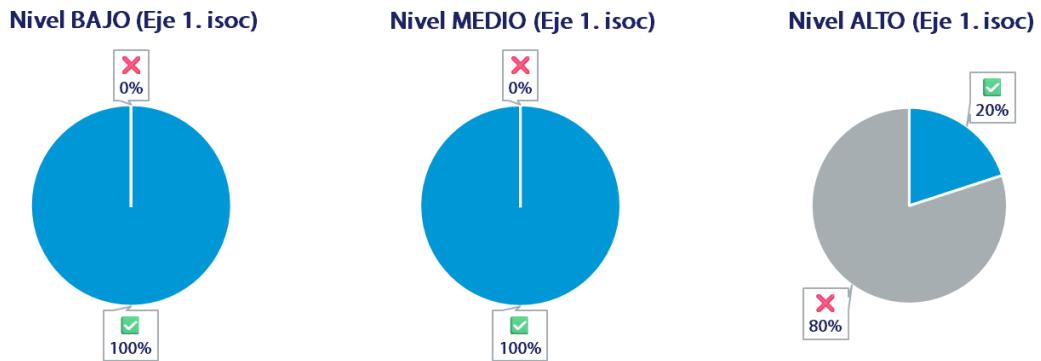


Figura 5.14: Resultados agregados por niveles en el eje 1

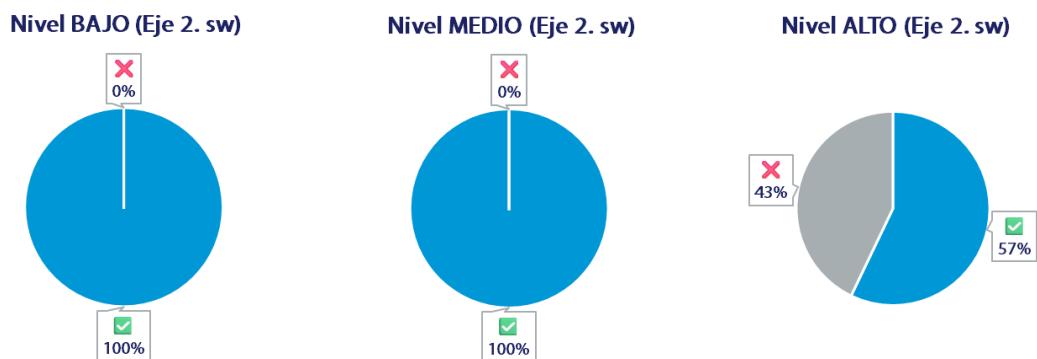


Figura 5.15: Resultados agregados por niveles en el eje 2

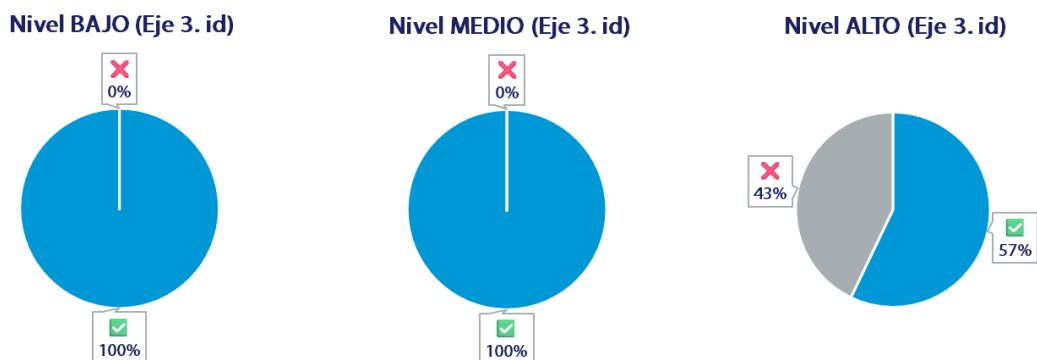


Figura 5.16: Resultados agregados por niveles en el eje 3

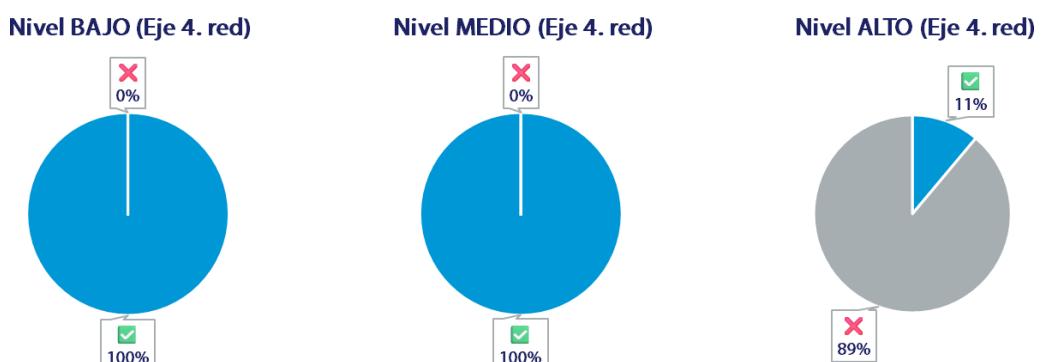


Figura 5.17: Resultados agregados por niveles en el eje 4

CAPÍTULO 6. CONCLUSIONES Y PROPUESTAS

En este penúltimo capítulo, se exponen una serie de conclusiones y propuestas de interés de cara al futuro, así como los resultados, competencias y beneficios obtenidos.

6.1 ANÁLISIS DE RESULTADOS OBTENIDOS

Los resultados conseguidos durante el TFM se corresponden con el conjunto de objetivos establecidos al inicio del proyecto en el *Capítulo 2. Objetivos*, aportando novedades significativas en tiempo y forma bajo el contexto estudiado. En la *Tabla 6.1*, se realiza suavemente un análisis de los resultados alcanzados en este proyecto:

Objetivo	Resultados
[OG] Diseñar y establecer las bases y elementos esenciales de un marco de trabajo o modelo de madurez enfocado en la concienciación de las personas de una organización en ciberseguridad, aumentando las capacidades de los empleados para hacer frente y evitar potenciales incidentes que pudieran comprometer los datos de los sistemas de información de las organizaciones.	✓ Completado con éxito. Se ha cumplido satisfactoriamente con todos los objetivos determinados en las sucesivas fases del desarrollo del TFM, partiendo desde su concepción inicial, análisis previos, diseño y definición del modelo, evaluación y refinamiento continuo, obteniendo rápido un PMV que ha sido mejorado en cada iteración hasta su versión final, siguiendo una metodología ágil.
[OP1] Analizar y estudiar los escenarios, tácticas, técnicas y procedimientos más frecuentes en ciberataques e incidentes de ciberseguridad sufridos por los empleados de las organizaciones en la actualidad.	✓ Completado con éxito. Se ha obtenido una visión general que permite conocer algunos datos de interés y las principales amenazas, riesgos, peligros y consecuencias para las personas en el uso de la tecnología a través del ciberespacio.
[OP2] Analizar y estudiar las principales normativas, planes y estrategias en ciberseguridad desde una perspectiva enfocada en la concienciación, sensibilización y capacitación de los usuarios finales en esta materia.	✓ Completado con éxito. Se han comprendido las demandas regulatorias y necesidades actuales desde el plano de gobierno y gestión de ciberseguridad, así como las acciones para satisfacerlas, incluyendo un análisis de las actividades formativas y artículos científicos relacionados.
[OP3] Diseñar y establecer las bases y fundamentos por los que se debería regir un marco de trabajo o modelo de madurez que permita fomentar la concienciación y formación en ciberseguridad del personal dentro de una organización.	✓ Completado con éxito. Se han definido los conceptos, principios y requisitos primordiales, junto con un análisis íntegro del contexto en el que se enmarca el proyecto desarrollado.
[OP4] Diseñar y establecer los elementos esenciales correspondientes como niveles, ejes, líneas de acción, medidas necesarias, métricas e indicadores.	✓ Completado con éxito. Se han determinado y estructurado los distintos elementos y sus relaciones en el modelo siguiendo una metodología de naturaleza iterativa y mejora continua.
[OP5] Evaluar y validar el método en base a su aplicación en un caso de uso dentro del contexto de una organización.	✓ Completado con éxito. Se ha evaluado el modelo de madurez aplicando los criterios de éxito y métricas establecidas en un caso de uso realista, dentro de un contexto similar al de una Administración Pública regional.

Tabla 6.1: Resultados obtenidos

6.2 ANÁLISIS DE COMPETENCIAS ADQUIRIDAS

Completando lo anterior, en este apartado se examina rigurosamente la consecución de las diferentes competencias específicas previamente fijadas, analizando su aplicación práctica y su relevancia en el desarrollo del modelo propuesto en este TFM.

- [CE1] Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.

Se cumple esta competencia mediante la definición de un modelo que aborda con carácter general los aspectos más fundamentales de la ciberseguridad en el uso de la tecnología, aplicaciones y sistemas de información, desde varias perspectivas y enfocada en concienciar a las personas en el contexto de un caso de uso dentro de una organización.

- [CE2] Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.

Se adquiere esta competencia con el diseño de un modelo que tiene una visión y misión estratégica claramente definida, acompañada de cinco principios rectores por los que se rigen los sucesivos componentes y criterios. Además, se sigue una metodología de trabajo que permite trabajar de manera ágil, con una planificación temporal adecuada al ámbito del problema y estimación realista de los costes económicos totales del proyecto realizado.

- [CE6] Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.

Se ha alcanzado esta competencia mediante la creación de un modelo que incluye los mecanismos necesarios para garantizar su oportuno cumplimiento, gracias a un exhaustivo estudio de la normativa y situación actual. Se tiene un seguimiento estructurado y enfoque progresivo de los criterios de éxito y las métricas asociadas a los niveles de madurez, para cada uno de los ejes estratégicos y líneas de acción a los que pertenecen.

- [CE7] Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

Se satisface esta competencia llevando a cabo un análisis, diseño, implementación y validación de un modelo que cuenta con los instrumentos necesarios para avalar la concienciación en ciberseguridad de las personas dentro de una organización a todos sus niveles, incluyendo el acceso, compartición y difusión de manera consciente y responsable de la información disponible a través de los sistemas y tecnologías de la información.

6.3 PROPUESTAS DE FUTURO

Propuesta 1: Apertura a nivel crítico y nuevos elementos

Dado que la cultura en ciberseguridad se encuentra en continua evolución, se abre la posibilidad de ampliar el modelo con nuevos criterios y métricas de evaluación con un cuarto nivel de madurez más crítico, pensado específicamente para el personal de las FCSE o de las infraestructuras críticas.

Igualmente, se podrían introducir actualizaciones en forma de nuevos ejes, líneas de acción y criterios de éxito, dadas las necesidades actuales para reforzar la concienciación en ciberseguridad. Asimismo, en una futura versión del modelo se aspira a ampliar horizontalmente las distintas tablas de los criterios de éxito, añadiendo algunos indicadores de riesgo o *Key Risk Indicator (KRI)*, combinados con una relación de medidas compensatorias de seguridad recomendadas en cada caso.

Propuesta 2: Adaptación y pruebas en entidades de distinto tipo y tamaño

Se propone ajustar las bases y elementos del presente modelo de madurez al tipo y tamaño de las distintas entidades, de una manera similar a la que se formula en el Esquema Nacional de Seguridad mediante, por ejemplo, las guías de adecuación e implantación en universidades y entidades locales.

En esta dirección, se estudiará la oportunidad de evaluar y validar el modelo desarrollado mediante una serie de pruebas piloto adaptadas a organismos de diversas características, centrándose los esfuerzos especialmente en aquellas que cuentan con menos capacidades y recursos para la concienciación en ciberseguridad de los distintos equipos de trabajo.

Propuesta 3: Aproximación a una norma UNE y certificación

Al igual que existe una normativa UNE para el cumplimiento de accesibilidad en sitios web y aplicaciones móviles (UNE-EN 301549), se podría valorar el potencial encaje del modelo presentado en una norma con su correspondiente certificación oficial, añadiendo un toque de gamificación.

Asimismo, este proyecto podría presentarse ante el Centro Criptológico Nacional y en el grupo de trabajo de “cultura de ciberseguridad” del Foro Nacional de Ciberseguridad, como una iniciativa de actuación para la alfabetización digital y promoción de la concienciación en ciberseguridad.

6.4 CONCLUSIONES Y LECCIONES APRENDIDAS

El campo de la ciberseguridad adquiere a pasos agigantados una mayor importancia estratégica y de utilidad para el personal de las organizaciones en un mundo cada vez más conectado y vulnerable. En este proyecto, se ha demostrado la inexcusable necesidad de concienciar y formar de manera efectiva a las personas frente a las amenazas que rodean el ciberespacio en el ámbito laboral.

Para cumplir con este propósito, se ha desarrollado un modelo de madurez integral, contando con los instrumentos necesarios enfocados por y para todas las personas, como punta de lanza para alcanzar una concienciación efectiva por niveles en ciberseguridad. Igualmente, este TFM pretende servir de incentivo para futuros proyectos, líneas de investigación y tesis doctorales, ante el imparable crecimiento de ataques cibernéticos debidos al factor humano observados en los últimos años.

Durante esta experiencia se han realizado una serie de actividades que me han permitido poner en práctica los conocimientos aprendidos en el máster, desde una perspectiva organizativa, tecnológica y humanista. Este proyecto final, con características innovadoras en la esfera de la transformación digital, además, procura cumplir con las estrategias y demandas regulatorias actuales.

La transferencia tecnológica juega un papel crucial para la sociedad, satisfaciendo con este trabajo una necesidad real y de valiosa aplicación en el plano regional y nacional. En este sentido, la colaboración con el tutor ha sido determinante gracias a su gran interés y experiencia en el sector de la ciberseguridad, un área que a ambos nos apasiona y en la que hemos logrado mantener una muy buena sintonía, facilitando la consecución de los objetivos perseguidos a lo largo del desarrollo.

Realizar este proyecto tras llevar varios años trabajando profesionalmente en esta materia me ha aportado una visión holística, sumando claridad de ideas y rigor en la toma de decisiones. Por ello, ha sido posible detectar las exigencias que afloran continuamente y labrar los puntos clave en pro de establecer un ecosistema de ciberseguridad que pone en el centro a las personas.

La finalización de este TFM supone no sólo un hito capital en mi vida, completando los estudios de máster en la universidad pública de la región, sino también la conclusión de una etapa extraordinaria que me anima a seguir aprendiendo y evolucionando en el excitante panorama que vive la ingeniería informática.

Miguel de la Cal Bravo

Ciudad Real, a 28 de enero de 2025

BIBLIOGRAFÍA

- [1] BOE. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. URL: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963> (Última consulta: 12/10/2024).
- [2] BOE. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. URL: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389> (Última consulta: 17/10/2024).
- [3] BOE. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. URL: <https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191> (Última consulta: 17/10/2024).
- [4] BOE. Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero. URL: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962> (Última consulta: 19/10/2024).
- [5] Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. URL: <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf> (Última consulta: 24/12/2024).
- [6] CCN-CERT. Abierto el plazo de inscripción para los cursos STIC 2024 del segundo semestre. URL: <https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/12961-aberto-el-plazo-de-inscripcion-para-los-cursos-stic-2024-del-segundo-semestre.html> (Última consulta: 17/10/2024).
- [7] CCN-CERT. Cerca de 33.000 usuarios registrados en Ángeles, el portal de formación del Centro Criptológico Nacional. URL: <https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/12884-cerca-de-33-000-usuarios-registrados-en-angeles-el-portal-de-formacion-del-centro-criptologico-nacional.html> (Última consulta: 17/10/2024).
- [8] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Elsevier. Computer Science Review, Volume 50, 100592. URL: <https://doi.org/10.1016/j.cosrev.2023.100592> (Última consulta: 25/12/2024).

- [9] CISA. DAMS SECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) Version 2.0. URL: <https://www.cisa.gov/sites/default/files/2023-01/dams-c2m2-2022-508.pdf> (Última consulta: 09/11/2024).
- [10] CVE Details. Browse Vulnerabilities By Date. URL: <https://www.cvedetails.com/browse-by-date.php> (Última consulta: 02/01/2025).
- [11] D.School Stanford. Get Started with Design Thinking. URL: <https://dschool.stanford.edu/resources/getting-started-with-design-thinking> (Última consulta: 11/11/2024).
- [12] Departamento de Seguridad Nacional. Estrategia de Seguridad Nacional 2021. URL: <https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021> (Última consulta: 25/10/2024).
- [13] Departamento de Seguridad Nacional. Estrategia Nacional de Ciberseguridad 2019. URL: <https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019> (Última consulta: 25/10/2024).
- [14] Departamento de Seguridad Nacional. Informe Anual de Seguridad Nacional 2023. URL: <https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2023> (Última consulta: 19/10/2024).
- [15] ENISA. ENISA Threat Landscape 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (Última consulta: 12/12/2024).
- [16] European Commission. The EU's Cybersecurity Strategy for the Digital Decade. URL: <https://ec.europa.eu/newsroom/dae/redirection/document/72164> (Última consulta: 27/10/2024).
- [17] Gobierno de Castilla-La Mancha. El Gobierno de Castilla-La Mancha destaca la ejecución de más del 85 por ciento del Plan de Capacitación Digital a la Ciudadanía. URL: <https://www.castillalamancha.es/actualidad/notasdeprensa/el-gobierno-de-castilla-la-mancha-destaca-la-ejecuci%C3%B3n-de-m%C3%A1s-del-85-por-ciento-del-plan-de> (Última consulta: 18/10/2024).
- [18] Gobierno de Castilla-La Mancha. El Gobierno regional impulsa un potente proyecto para reforzar la sensibilización y el talento en ciberseguridad en Castilla-La Mancha. URL: <https://www.castillalamancha.es/actualidad/notasdeprensa/el-gobierno-regional-impulsa->

[un-potente-proyecto-para-reforzar-la-sensibilizaci%C3%B3n-y-el-talento-en](#) (Última consulta: 26/10/2024).

- [19] Gobierno de Castilla-La Mancha. El Gobierno regional ultima el desarrollo de una ambiciosa estrategia integral de Ciberseguridad para garantizar un uso seguro y fiable de los servicios públicos. URL: <https://www.castillalamancha.es/actualidad/notasdeprensa/el-gobierno-regional-ultima-el-desarrollo-de-una-ambiciosa-estrategia-integral-de-ciberseguridad> (Última consulta: 07/01/2025).
- [20] Google Trends. Interest over time on Google Trends for cybersecurity - Worldwide, 01/01/2019 - 31/12/2024. URL: <https://trends.google.com/trends/explore?date=2019-01-01%202024-12-31&q=cybersecurity&hl=en-GB> (Última consulta: 02/01/2025).
- [21] Google Trends. Interest over time on Google Trends for social engineering - Worldwide, 01/01/2019 - 31/12/2024. URL: <https://trends.google.com/trends/explore?date=2019-01-01%202024-12-31&q=social%20engineering&hl=en-GB> (Última consulta: 02/01/2025).
- [22] IBM. The Framework. Design thinking re-envisioned for the modern enterprise. URL: <https://www.ibm.com/design/thinking/page/framework> (Última consulta: 12/11/2024).
- [23] IBM. Toolkit. Guidance to hone your design thinking skills. URL: <https://www.ibm.com/design/thinking/page/toolkit> (Última consulta: 12/11/2024).
- [24] INCIBE. Catálogos de formación en ciberseguridad. URL: <https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad> (Última actualización: 19/10/2024).
- [25] INCIBE. Ciberseguridad para microempresas y autónomos. URL: <https://www.incibe.es/empresas/formacion/ciberseguridad-para-micropymes-y-autonomos> (Última consulta: 18/10/2024).
- [26] INCIBE. Ingeniería social. URL: <https://www.incibe.es/aprendeciberseguridad/ingenieria-social> (Última consulta: 23/10/2024).
- [27] INCIBE. Redes Territoriales de Especialización Tecnológica (RETECH). URL: <https://www.incibe.es/retech> (Última consulta: 26/10/2024).
- [28] ISACA. Glossary. URL: <https://www.isaca.org/-/media/files/isacadv/project/isaca/resources/glossary/glossary.pdf> (Última consulta: 23/10/2024).

- [29] Kaspersky. Redefining the Human Factor in Cybersecurity. URL: <https://media.kasperskydaily.com/wp-content/uploads/sites/92/2023/11/22070742/KasperskyHumanFactor360Report2023.pdf> (Última consulta: 12/10/2024).
- [30] Michael Page. Estudio de remuneración 2024. Insights claves sobre las tendencias de contratación y comparativas salariales. URL: https://b2beu.page.com/l/782393/2024-03-21/367pgt/782393/1711032174VIBjaB6O/ER_TECH_2024.pdf (Última consulta: 10/11/2024).
- [31] Ministerio del Interior. Informe sobre la criminalidad en España 2023. URL: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf (Última consulta: 19/10/2024).
- [32] Mitnick, K. & Simon, W. (2003). The Art of Deception. Controlling the Human Element of Security. ISBN: 978-0764542800.
- [33] MITRE ATT&CK®. URL: <https://attack.mitre.org/> (Última consulta: 12/10/2024).
- [34] Piki, A., Stavrou, E., Procopiou, A., & Demosthenous, A. (2023). Fostering cybersecurity awareness and skills development through digital game-based learning. In 2023 10th International Conference on Behavioural and Social Computing (BESC), pp. 1-9. URL: <https://doi.org/10.1109/BESC59560.2023.10386988> (Última actualización: 31/12/2024).
- [35] Plan de Recuperación, Transformación y Resiliencia. Componente 15: Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G. URL: <https://planderecuperacion.gob.es/politicas-y-componentes/componente-15-conectividad-digital-impulso-de-la-ciberseguridad-y> (Última consulta: 10/11/2024).
- [36] Plataforma de Contratación del Sector Público. ESTUDIO ECONÓMICO DEL CONTRATO QUE TIENE POR OBJETO: “PROGRAMA DE ACCELERACIÓN DE ECOSISTEMAS DE EMPRENDIMIENTO E INNOVACIÓN BASADOS EN GEMELOS DIGITALES: RETECH, EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA-NEXT GENERATION EU”. N.º Expediente PICOS: 2024/000333. URL: <https://contrataciondelestado.es/FileSystem/servlet/GetDocumentByIdServlet?DocumentIdParam=v76yfliyHHj%2BOAbBwOrI2sGFO6R3GyNVeQRGF5WGHw0wDis8%2BH03>

<https://i8PiHWUAsoaK3OE2GmfpdBPEQnuB4gYchZmBTJFQ/bO1D7/o9KAm%2BNU%3D&cifrado=QUC1GjXXSiLkydRHJBmbpw%3D%3D> (Último acceso: 17/11/2024).

- [37] Plataforma de Contratación del Sector Público. ESTUDIO ECONÓMICO DEL CONTRATO QUE TIENE POR OBJETO: “DESARROLLO DE ESPACIO DE DATOS Y CASOS DE USO PARA INTELIGENCIA ARTIFICIAL (IA) EN EL SECTOR HOTELERO DE CASTILLA-LA MANCHA DEL PROGRAMA SPAIN LIVING LAB: RETECH, EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA- NEXT GENERATION EU”. N.º Expediente PICOS: 2024/000375. URL: <https://contrataciondelestado.es/FileSystem/servlet/GetDocumentByIdServlet?DocumentIdParam=Ld48kHrca/C19uVJkFXfTixTQ99/8nZ0SIdcmyAR%2Bu3ohVIBm1PUSDQ5zymG131TiGeTFTHq5qoPNT61aILiLKLj9Xck82rJMHY8M7uh5oQ%3D&cifrado=QUC1GjXXSiLkydRHJBmbpw%3D%3D> (Último acceso: 17/11/2024).
- [38] Plataforma de Contratación del Sector Público. Secretaría General de la Consejería de Hacienda, Administraciones Públicas y Transformación Digital de la Junta de Comunidades de Castilla-La Mancha. URL: https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfljU1JTC3Iy87KtCIKL0jJznPPzSooSSxLzSIL1w_Wj9KMyU5wK9CN9I5Kd0svSg019sgO9jUJc0yLcK7UdbW31C3JzHQFwILxm/ (Último acceso: 17/11/2024).
- [39] Quayyum, F. (2023). Collaboration between parents and children to raise cybersecurity awareness. ACM. EICC '23: Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference. Pages 149 – 152. URL: <https://doi.org/10.1145/3590777.3590802> (Última consulta: 25/12/2024).
- [40] ResearchGate. Stanford d.school Design Thinking Process. URL: https://www.researchgate.net/figure/Stanford-dschool-Design-Thinking-Process-Schmarzo-2017_fig2_338741533 (Última consulta: 13/11/2024).
- [41] SANS. Leveraging the SANS Security Awareness Maturity Model® to Effectively Manage Human Risk. URL: <https://sansorg.egnyte.com/dl/muipL303AS> (Última consulta: 09/11/2024).
- [42] Stanford. A Design Thinking Process. URL: https://web.stanford.edu/class/me113/d_thinking.html (Último acceso: 13/11/2024).

- [43] U.S. Department of Defense. Chief Information Officer. About CMMC. URL: <https://dodcio.defense.gov/cmmc/About/> (Última consulta: 09/11/2024).
- [44] UCLM. La UCLM y el Gobierno regional crean una cátedra para promover la cultura de la seguridad cibernética. URL: https://www.uclm.es/noticias/noticias2024/octubre/toledo/catedra_ciberseguridad (Última consulta: 20/10/2024).
- [45] UCLM. La UCLM y el Incibe forman al estudiantado en seguridad digital. URL: https://www.uclm.es/noticias/noticias2024/octubre/ciudad-real/taller_cyberseguridad_uclm_incibe (Última consulta: 05/11/2024).
- [46] UCLM. On-Store. URL: <https://area.tic.uclm.es/Difusion/tc/tc-estudiantes/ServiciosON/ON-Store> (Última consulta: 23/11/2024).
- [47] Unitel. Éxito en el Webinar ‘Concienciación. Riesgos en el teletrabajo’. Centro Regional de Innovación Digital. URL: <https://unitel-tc.com/webinar-concienciacion-riesgos-en-el-teletrabajo/> (Última consulta: 19/10/2024).
- [48] Verizon. 2024 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/T212/reports/2024-dbir-data-breach-investigations-report.pdf> (Última consulta: 12/10/2024).
- [49] Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. Elsevier. Journal of Systems and Software, Volume 210, 111946. URL: <https://doi.org/10.1016/j.jss.2023.111946> (Última consulta: 25/12/2024).

ANEXO A. RELACIÓN DE COMPONENTES DEL MODELO

En el primer anexo de la memoria escrita se incluyen un total de cuatro tablas, donde se especifican los componentes del modelo de madurez y sus relaciones por cada uno de los ejes estratégicos definidos, incluyendo sus líneas de acción y criterios de éxito pertenecientes para su cumplimiento en los distintos niveles de madurez.

Tal y como se describió anteriormente, para la elaboración de las tablas se sigue la convención de columnas descrita a continuación:

- a) Para comenzar, en la primera columna se determina un identificador del componente descrito en la fila, bien sea una línea de acción o un criterio de éxito.
- b) En la segunda columna, se especifica el nombre de dicho componente del modelo.
- c) La tercera columna muestra el nivel mínimo requerido para cada criterio de éxito.
- d) En las columnas cuarta, quinta y sexta se establecen las métricas exigidas para cada criterio de éxito en los niveles de madurez bajo, medio y alto, respectivamente.
- e) En la séptima y última columna se declara el tipo del rango de valores de las métricas.

Con el objeto de cubrir toda la información necesaria en las tablas y por limitaciones de espacio, dichas tablas se orientan de forma horizontal, quedando centradas en cada página.

En concreto, en este anexo se incluyen las cuatro siguientes tablas:

- Tabla A.1: Relación de componentes en el eje 1. Ingeniería social (isoc)
- Tabla A.2: Relación de componentes en el eje 2. Programas software (sw)
- Tabla A.3: Relación de componentes en el eje 3. Identidades digitales (id)
- Tabla A.4: Relación de componentes en el eje 4. Comportamientos en la red (red)

ID	Nombre	Nivel mínimo	BAJO	MEDIO	ALTO	Rango de valores
isoc.1 Ingeniería social a través del correo electrónico						
isoc.1.a)	Ingeniería social a través del correo electrónico	Bajo	Anual	Semestral	Trimestral	Periodicidad
isoc.1.b)	Reportes de correos sospechosos	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No
isoc.1.c)	Campañas de phishing corporativas	Medio	n.a.	Anual	Semestral	Periodicidad
isoc.2 Ingeniería social a través del teléfono						
isoc.2.a)	Pildoras formativas llamadas telefónicas	Bajo	Anual	Semestral	Trimestral	Periodicidad
isoc.2.b)	Reportes de llamadas sospechosas	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No
isoc.2.c)	Simulaciones de llamadas fraudulentas	Alto	n.a.	n.a.	Bienal	Periodicidad
isoc.3 Redes sociales						
isoc.3.a)	Pildoras formativas redes sociales	Medio	n.a.	Anual	Semestral	Periodicidad
isoc.3.b)	Talleres prácticos de fraudes digitales	Alto	n.a.	n.a.	Anual	Periodicidad
isoc.4 Bulos y noticias falsas						
isoc.4.a)	Pildoras de bulos y noticias falsas	Medio	n.a.	Anual	Semestral	Periodicidad
isoc.4.b)	Pildoras de contenidos manipulados con IA	Alto	n.a.	n.a.	Anual	Periodicidad

ID	Nombre	Nivel mínimo	BAJO	MEDIO	ALTO	Rango de valores
sw.1 Seguridad en el software						
sw.1.a)	Actualizaciones de seguridad	Bajo	Trimestral	Mensual	Quincenal	Periodicidad
sw.1.b)	Programas antivirus o similares	Bajo	Sí	Sí	Sí	Sí/Parcialmente/No
sw.1.c)	Copias de seguridad	Bajo	Parcialmente	Sí	Sí	Sí/Parcialmente/No
sw.2 Programas software dañinos						
sw.2.a)	Pildoras formativas malware	Bajo	Semestral	Trimestral	Mensual	Periodicidad
sw.2.b)	Identificar los tipos de malware	Bajo	Parcialmente	Sí	Sí	Sí/Parcialmente/No
sw.2.c)	Descarga de sitios oficiales y fiables	Bajo	Sí	Sí	Sí	Sí/Parcialmente/No
sw.2.d)	Simulación de ataques internos	Alto	n.a.	n.a.	Bienal	Periodicidad

Tabla A.2: Relación de componentes en el eje 2. Programas software (sw)

ID	Nombre	Nivel mínimo	BAJO	MEDIO	ALTO	Rango de valores
id.1 Credenciales de acceso						
id.1.a)	Pildoras formativas contraseñas	Bajo	Anual	Semestral	Trimestral	Periodicidad
id.1.b)	Cambio de contraseñas	Medio	n.a.	Anual	Semestral	Periodicidad
id.2 Autenticación más segura						
id.2.a)	Segundo factor de autenticación	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No
id.2.b)	Tercer factor de autenticación	Alto	n.a.	n.a.	Sí	Sí/Parcialmente/No
id.3 Gestión de cuentas corporativas						
id.3.a)	Pildoras formativas brechas de seguridad	Medio	n.a.	Annual	Semestral	Periodicidad
id.3.b)	Gestores de contraseñas	Alto	n.a.	n.a.	Sí	Sí/Parcialmente/No
id.3.c)	Reporte de accesos sospechosos	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No

Tabla A.3: Relación de componentes en el eje 3. Identidades digitales (id)

ID	Nombre	Nivel mínimo	BAJO	MEDIO	ALTO	Rango de valores
red.1 Redes públicas						
red.1.a)	Pildoras sobre navegación por Internet	Medio	Anual	Semestral	Trimestral	Periodicidad
red.1.b)	Conexión a redes Wi-Fi públicas	Bajo	Sí	Sí	Sí	Sí/Parcialmente/No
red.1.c)	Otras conexiones inalámbricas	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No
red.2 Teletrabajo						
red.2.a)	Pildoras sobre teletrabajo	Medio	n.a.	Annual	Semestral	Periodicidad
red.2.b)	Redes privadas virtuales	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No
red.3 Seguridad de la información						
red.3.a)	Pildoras seguridad de la información corporativa	Medio	n.a.	Annual	Semestral	Periodicidad
red.3.b)	Compartición de documentos	Medio	n.a.	Parcialmente	Sí	Sí/Parcialmente/No
red.3.c)	Cifrado de archivos y mensajes	Alto	n.a.	n.a.	Sí	Sí/Parcialmente/No
red.3.d)	Exposición de metadatos	Alto	n.a.	n.a.	Sí	Sí/Parcialmente/No

Tabla A.4: Relación de componentes en el eje 4. Comportamientos en la red (red)

ANEXO B. CRITERIOS DE ÉXITO

isoc.1.a) Píldoras formativas correo electrónico

El correo electrónico constituye uno de los vectores de entrada a las organizaciones más atractivos para los atacantes del ciberespacio. Por ello, es necesario conocer las buenas prácticas para garantizar un uso más seguro del servicio de correo electrónico corporativo (ver *Tabla B.1*).

Criterio de éxito	Píldoras formativas correo electrónico		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	Anual	Semestral	Trimestral

Tabla B.1: Relación de métricas del criterio de éxito isoc.1.a)

Aplicación del criterio de éxito:

- Nivel BAJO: Se deben remitir píldoras formativas de carácter básico a todas las personas de la organización, al menos, con una periodicidad anual.
- Nivel MEDIO: Se deben remitir píldoras formativas de carácter básico a todas las personas de la organización, al menos, con una periodicidad semestral.
- Nivel ALTO: Se deben remitir píldoras formativas básicas y más avanzadas a todas las personas de la organización, al menos, con una periodicidad trimestral.

isoc.1.b) Reportes de correos sospechosos

El resultado deseado en esta línea de acción consiste en que las personas sean capaces de detectar y reportar los correos como potencialmente sospechosos. De esta manera, los equipos de ciberseguridad podrán advertir y orquestar respuestas frente a los correos maliciosos recibidos dentro de la organización, mejorando la postura de seguridad corporativa (ver *Tabla B.2*).

Criterio de éxito	Reportes de correos sospechosos		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.2: Relación de métricas del criterio de éxito isoc.1.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Un grupo muy reducido de personas son capaces de reportar los correos sospechosos recibidos en la organización.
- Nivel ALTO: Un grupo más amplio de personas de diferentes departamentos son capaces de reportar con éxito los correos maliciosos recibidos en la organización.

isoc.1.c) Campañas de phishing corporativas

De manera complementaria a las píldoras formativas, se exigirá a las organizaciones, a partir del nivel de madurez medio, la realización de actividades de simulacro de *phishing* a través del correo electrónico corporativo. Gracias a estas campañas internas, se podrá tener un seguimiento de los grupos de usuarios para los que se deberían reforzar los esfuerzos de concienciación (ver *Tabla B.3*).

Criterio de éxito	Campañas de phishing corporativas		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.3: Relación de métricas del criterio de éxito isoc.1.c)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se deben realizar campañas de phishing genéricas a un grupo de personas de algunos departamentos de la organización, al menos, con una periodicidad anual.
- Nivel ALTO: Se deben realizar campañas de phishing personalizadas a grupos de personas de la mayoría de los departamentos de la organización, al menos, con una periodicidad semestral.

isoc.2.a) Píldoras formativas llamadas telefónicas

Cada vez es más frecuente recibir llamadas telefónicas fraudulentas en el puesto de trabajo, lo cual es conocido bajo el término *vishing* o *phishing* mediante voz. Estas estafas cada vez son más sofisticadas, puesto que, en ocasiones, buscan suplantar a altos cargos de las compañías para extraer información secreta, datos bancarios o incluso datos de carácter personal (ver *Tabla B.4*).

Criterio de éxito	Píldoras formativas llamadas telefónicas		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	Anual	Semestral	Trimestral

Tabla B.4: Relación de métricas del criterio de éxito isoc.2.a)

Aplicación del criterio de éxito:

- Nivel BAJO: Se deben remitir píldoras formativas básicas a todas las personas de la organización, al menos, con una periodicidad anual.
- Nivel MEDIO: Se deben remitir píldoras formativas básicas a todas las personas de la organización, al menos, con una periodicidad semestral.
- Nivel ALTO: Se deben remitir píldoras formativas básicas y avanzadas a todas las personas de la organización, al menos, con una periodicidad trimestral.

isoc.2.b) Reportes de llamadas fraudulentas

El resultado perseguido en esta línea de acción trata de que los usuarios sean capaces de advertir y reportar las potenciales llamadas fraudulentas. De esta manera, los equipos de tecnologías de la información de la corporación podrán actuar para aplicar los mecanismos y medidas preventivas de seguridad adecuadas (ver *Tabla B.5*).

Criterio de éxito	Reportes de llamadas fraudulentas		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.5: Relación de métricas del criterio de éxito isoc.2.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Un grupo muy reducido de personas son capaces de reportar las llamadas sospechosas recibidas en la organización.
- Nivel ALTO: Un grupo más amplio de personas de diferentes departamentos son capaces de reportar con éxito las llamadas fraudulentas recibidas en la organización.

isoc.2.c) Simulaciones de llamadas fraudulentas

Para completar esta línea de acción se propone llevar a cabo ejercicios de simulación de llamadas fraudulentas controladas dentro de las organizaciones, con el objetivo de poner a prueba al personal en estas situaciones y mejorar su preparación para futuras ocasiones reales (ver *Tabla B.6*).

Criterio de éxito	Simulaciones de llamadas fraudulentas		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	n.a.	Bienal

Tabla B.6: Relación de métricas del criterio de éxito isoc.2.c)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Se deben realizar simulacros de llamadas telefónicas fraudulentas personalizadas sobre asuntos laborales a un grupo reducido de personas de algunos departamentos de la organización, al menos, con una periodicidad bienal.

isoc.3.a) Píldoras formativas redes sociales

Las redes sociales generan nuevas oportunidades para las organizaciones, sin embargo, estas generan un paradigma con nuevas amenazas y riesgos para la plantilla del organismo, por lo que se detecta la necesidad general de concienciación para garantizar un uso más seguro y responsable de las redes sociales (ver *Tabla B.7*).

Criterio de éxito	Píldoras formativas redes sociales		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.7: Relación de métricas del criterio de éxito isoc.3.a)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad anual.
- Nivel ALTO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad semestral.

isoc.3.b) Talleres prácticos de fraudes digitales

A fin de poner en práctica la sensibilización sobre diversos fraudes digitales, las organizaciones pueden preparar talleres informativos sobre casos destacados de estafas de actualidad. Esto permite conocer algunas de las tácticas y técnicas empleadas por la mayoría de los ciberdelincuentes, para que los usuarios puedan reaccionar exitosamente ante determinados escenarios fraudulentos vigentes (ver *Tabla B.8*).

Criterio de éxito	Talleres prácticos de fraudes digitales		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	n.a.	Anual

Tabla B.8: Relación de métricas del criterio de éxito isoc.3.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Se deben realizar talleres prácticos para grupos reducidos de personas de la organización, al menos, con una periodicidad anual.

isoc.4.a) Píldoras de bulos y noticias falsas

Continuando en la línea de los criterios anteriores respecto a las redes sociales, adquieren gran relevancia los bulos y noticias falsas propagadas a través de los distintos medios digitales. Así, se consigue una alfabetización digital a la hora de detectar y evitar la difusión de estas (ver *Tabla B.9*).

Criterio de éxito	Píldoras de bulos y noticias falsas		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.9: Relación de métricas del criterio de éxito isoc.4.a)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad anual.
- Nivel ALTO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad semestral.

isoc.4.b) Píldoras de contenidos manipulados con IA

En la parte más avanzada de la presente línea de acción, se incluye la formación en cuanto a la sospecha y detección de contenidos manipulados con herramientas de Inteligencia Artificial (IA). Entre este material destacan los archivos multimedia, como imágenes, audios y vídeos, los cuales son cada vez más realistas y, por ende, más difíciles de diferenciar de aquellos generados por los seres humanos (ver *Tabla B.10*).

Criterio de éxito	Píldoras de contenidos manipulados con IA		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	n.a.	Anual

Tabla B.10: Relación de métricas del criterio de éxito isoc.4.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad anual.

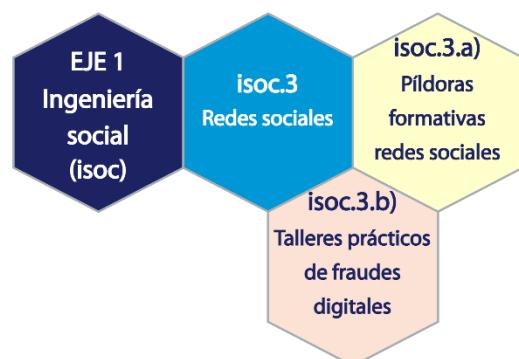
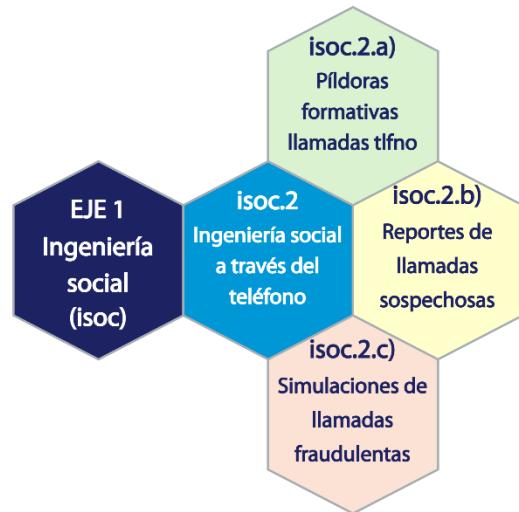


Figura B.1: Eje estratégico 1, líneas de acción y criterios de éxito

sw.1.a) Actualizaciones de seguridad

Uno de los aspectos más importantes a la hora de hablar de seguridad en el software trata sobre aplicar las actualizaciones publicadas regularmente en canales oficiales. Las nuevas versiones no solo añaden nuevas funcionalidades, sino que, también, corrigen vulnerabilidades (ver *Tabla B.11*).

Criterio de éxito	Actualizaciones de seguridad		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	Trimestral	Mensual	Quincenal

Tabla B.11: Relación de métricas del criterio de éxito sw.1.a)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe concienciar para actualizar el software de los dispositivos de todas las personas de la organización, al menos, con una periodicidad trimestral.
- Nivel MEDIO: Se debe concienciar para actualizar el software de los dispositivos de todas las personas de la organización, al menos, con una periodicidad mensual.
- Nivel ALTO: Se debe concienciar para actualizar el software de los dispositivos de todas las personas de la organización, al menos, con una periodicidad quincenal, así como desinstalar las aplicaciones y programas que no sean utilizados frecuentemente.

sw.1.b) Programas antivirus o similares

Además de las actualizaciones del software, también se puede aumentar la seguridad en los puestos de trabajo finales gracias al uso de herramientas antivirus, *EDR (Endpoint Detection and Response)* o similares, así como la actualización y configuración apropiada de estos programas (ver *Tabla B.12*).

Criterio de éxito	Programas antivirus o similares		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	Sí	Sí	Sí

Tabla B.12: Relación de métricas del criterio de éxito sw.1.b)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe concienciar a todas las personas de la organización para que activen y utilicen adecuadamente los programas de seguridad corporativos de los equipos.
- Nivel MEDIO: Se debe concienciar a todas las personas de la organización para que activen y utilicen adecuadamente los programas de seguridad corporativos de los equipos.
- Nivel ALTO: Se debe concienciar a todas las personas de la organización para que activen y utilicen adecuadamente los programas de seguridad corporativos de los equipos, evitando la instalación de cualquier software de terceros no permitido para este fin.

sw.1.c) Copias de seguridad

Proteger la información de los equipos corporativos es muy necesario, algo que también se puede realizar frecuentemente son las copias de seguridad de los archivos del dispositivo, ya que ciertos usuarios pueden manejar información sensible en su operativa diaria (ver *Tabla B.13*).

Criterio de éxito	Copias de seguridad		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	Parcialmente	Sí	Sí

Tabla B.13: Relación de métricas del criterio de éxito sw.1.c)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe fomentar la realización de copias de seguridad de la información en los equipos corporativos de algunas de las personas de la organización.
- Nivel MEDIO: Se debe fomentar la realización de copias de seguridad de la información en los equipos corporativos de la mayoría de las personas de la organización.
- Nivel ALTO: Se debe fomentar la realización de copias de seguridad de la información de manera habitual en los equipos corporativos de la mayoría de las personas de la organización.

sw.2.a) Píldoras formativas malware

Los programas dañinos o *malware* permiten a los ciberdelincuentes conseguir acceso a la información de los integrantes de las organizaciones, en ocasiones, sin que se puedan dar cuenta. Por esta razón, es necesario sensibilizar sobre los riesgos que pueden originarse (ver *Tabla B.14*).

Criterio de éxito	Píldoras formativas malware		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	Semestral	Trimestral	Mensual

Tabla B.14: Relación de métricas del criterio de éxito sw.2.a)

Aplicación del criterio de éxito:

- Nivel BAJO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad semestral.
- Nivel MEDIO: Se deben remitir píldoras formativas a todas las personas de la organización, al menos, con una periodicidad trimestral.
- Nivel ALTO: Se deben remitir píldoras formativas a todas las personas de la organización de carácter más avanzado, al menos, con una periodicidad mensual.

sw.2.b) Identificar los tipos de malware

Una vez conocidos los riesgos que entrañan los programas maliciosos, igualmente se requiere que los usuarios puedan reconocer con éxito los diferentes tipos de malware, sus características y peligros asociados en cada caso, con el desafío de identificar situaciones reales donde se pueden materializar (ver *Tabla B.15*).

Criterio de éxito	Identificar los tipos de malware		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	Parcialmente	Sí	Sí

Tabla B.15: Relación de métricas del criterio de éxito sw.2.b)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe concienciar a las personas de la organización para que sean capaces de reconocer parcialmente las distintas clasificaciones de programas dañinos.
- Nivel MEDIO: Se debe concienciar a las personas de la organización para que sean capaces de reconocer las principales categorías de programas dañinos.
- Nivel ALTO: Se debe concienciar a las personas de la organización para que sean capaces de reconocer las principales categorías de programas dañinos.

sw.2.c) Descarga de sitios oficiales y fiables

Como consecuencia de los criterios de éxito anteriores, es clave la concienciación para que las personas descarguen programas software exclusivamente a través de los canales oficiales de los fabricantes, donde se garantice su fiabilidad y que estén libres de malware (ver *Tabla B.16*).

Criterio de éxito	Descarga de sitios oficiales y fiables		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	Sí	Sí	Sí

Tabla B.16: Relación de métricas del criterio de éxito sw.2.c)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe sensibilizar a las personas de la organización para que únicamente descarguen los programas software de las fuentes oficiales.
- Nivel MEDIO: Se debe sensibilizar a las personas de la organización para que únicamente descarguen los programas software de las fuentes oficiales.
- Nivel ALTO: Se debe sensibilizar a las personas de la organización para que únicamente descarguen los programas software de las fuentes oficiales.

sw.2.d) Simulación de ataques internos

Para poner en práctica la capacitación sobre los programas malignos la organización desarrollará talleres en forma de simulacros de ataques internos, con el objetivo de concienciar a las personas en los riesgos patentes en el ámbito de las descargas de software procedente de fuentes no confiables y sus posibles consecuencias (ver *Tabla B.17*).

Criterio de éxito	Simulación de ataques internos		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	n.a.	Bienal

Tabla B.17: Relación de métricas del criterio de éxito sw.2.d)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Se deben realizar simulaciones de ataques internos con software malicioso a una parte de la organización, al menos, con una periodicidad bienal.

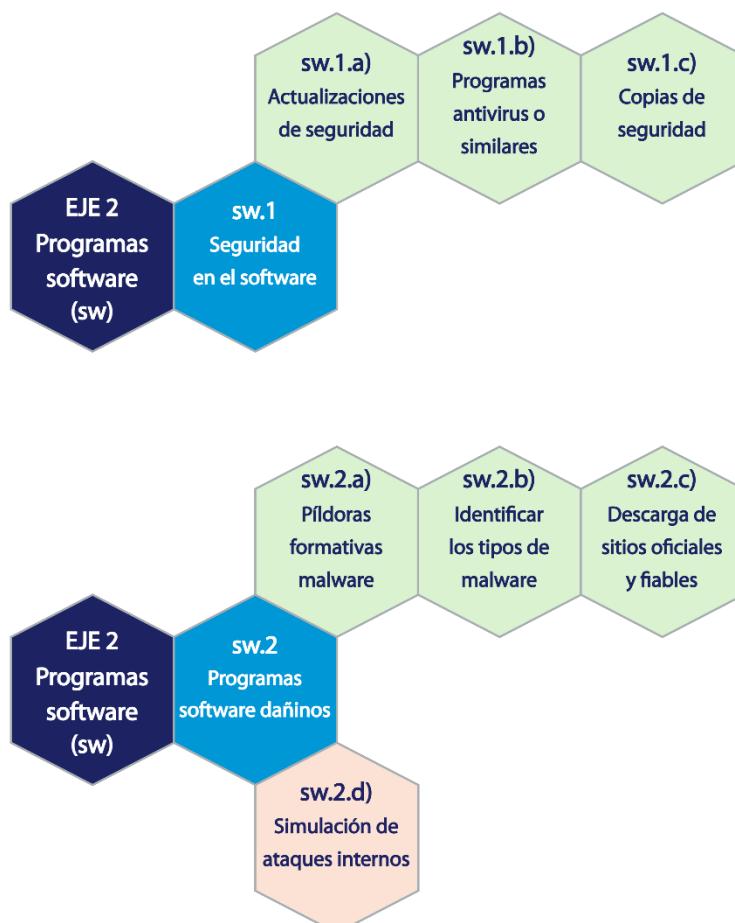


Figura B.2: Eje estratégico 2, líneas de acción y criterios de éxito

id.1.a) Píldoras formativas contraseñas

La primera barrera de protección del acceso a las cuentas corporativas se consigue a través del establecimiento de las credenciales de usuario. Garantizar la seguridad en este paso es imprescindible para evitar accesos no deseados a la información de la organización, para lo cual se deben tener presentes los riesgos y buenas prácticas a la hora de crear contraseñas robustas, evitar compartirlas con otras personas y tampoco reutilizar la misma contraseña en diferentes cuentas (ver *Tabla B.18*).

Criterio de éxito	Píldoras formativas contraseñas		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	Anual	Semestral	Trimestral

Tabla B.18: Relación de métricas del criterio de éxito id.1.a)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe concienciar sobre un uso más seguro de las contraseñas corporativas a todas las personas de la organización, al menos, con una periodicidad anual.
- Nivel MEDIO: Se debe concienciar sobre un uso seguro de las contraseñas corporativas a todas las personas de la organización, al menos, con una periodicidad semestral.
- Nivel ALTO: Se debe concienciar sobre un uso seguro de las contraseñas corporativas a todas las personas de la organización, al menos, con una periodicidad trimestral.

id.1.b) Cambio de contraseñas

Además de los aspectos fundamentales en la creación y uso de las contraseñas, es crucial reciclarlas cada cierto tiempo. Por ello, se fomentará y formará sobre el cambio periódico de las contraseñas corporativas, con el objetivo de que, en caso de ser filtradas en una brecha de seguridad, se mantenga más protegido el acceso a las cuentas empresariales (ver *Tabla B.19*).

Criterio de éxito	Cambio de contraseñas		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.19: Relación de métricas del criterio de éxito id.1.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se debe formar para llevar a cabo cambios de contraseñas periódicamente a las personas de la organización, al menos, con una periodicidad anual.
- Nivel ALTO: Se debe formar para llevar a cabo cambios de contraseñas periódicamente a las personas de la organización, con una periodicidad semestral.

id.2.a) Segundo factor de autenticación

Como segunda barrera de protección (2FA o MFA) de las identidades corporativas encontramos varios mecanismos que permiten dotar de una mayor seguridad, al tener que proporcionar una autenticación adicional a las contraseñas tradicionales. Como alternativas existen el envío de un código por SMS, llamada telefónica o mediante una aplicación de autenticación (ver *Tabla B.20*).

Criterio de éxito	Segundo factor de autenticación		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.20: Relación de métricas del criterio de éxito id.2.a)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Las personas de la organización deben ser conscientes de los beneficios de utilizar al menos un segundo factor de autenticación de los citados, especialmente las cuentas corporativas que posean permisos de administración de manera privilegiada.
- Nivel ALTO: Las personas de la organización deben ser conscientes de los beneficios de utilizar al menos un segundo factor de autenticación de los citados, con independencia de los permisos que tengan asignados en sus cuentas corporativas.

id.2.b) Tercer factor de autenticación

En algunas organizaciones, por sus características, puede ser de interés añadir un tercer factor de autenticación en el acceso a las cuentas corporativas de los usuarios. De esta manera, además de la contraseña y el 2FA se añade una tercera capa de seguridad, en la que, entre otras opciones, se pueden emplear mecanismos biométricos como la huella dactilar, el reconocimiento facial o de iris, teniendo siempre presente el cumplimiento exigido en materia de protección de datos (ver *Tabla B.21*).

Criterio de éxito	Tercer factor de autenticación		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	n.a	Sí

Tabla B.21: Relación de métricas del criterio de éxito id.2.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Las personas de la organización conocen las ventajas de añadir un tercer factor de autenticación en escenarios determinados para mejorar su seguridad.

id.3.a) Píldoras formativas brechas de seguridad

Las credenciales empleadas en los servicios de terceros presentan un riesgo de seguridad añadido para las personas de la organización, aumentando los peligros en el caso de registrar el correo electrónico corporativo en otros recursos externos. Para ello, se sensibilizará regularmente en materia de brechas de seguridad de la información para un uso apropiado de las cuentas (ver *Tabla B.22*).

Criterio de éxito	Píldoras formativas brechas de seguridad		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.22: Relación de métricas del criterio de éxito id.3.a)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: La organización procurará formar con carácter básico a las personas para lograr un uso adecuado de la cuenta de correo empresarial, al menos, de manera anual.
- Nivel ALTO: La organización procurará formar con un nivel avanzado a las personas para lograr un uso adecuado de la cuenta de correo empresarial, al menos, de manera semestral.

id.3.b) Gestores de contraseñas

A medida que el personal de la corporación tiene acceso a más servicios y herramientas, tanto de forma interna, como de manera externa, aumenta la necesidad de recordar las cuentas y contraseñas establecidas para cada recurso. Aquí, es donde aparecen los programas que permiten centralizar y gestionar las diferentes credenciales digitales para facilitar esta necesidad (ver *Tabla B.23*).

Criterio de éxito	Gestores de contraseñas		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	n.a	Sí

Tabla B.23: Relación de métricas del criterio de éxito id.3.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: La organización promoverá el uso de gestores de contraseñas corporativas entre sus empleados, aplicando de manera general a todos los niveles.

id.3.c) Reporte de accesos sospechosos

Como último criterio de éxito en el tercer eje estratégico, se comprueban los resultados recopilados a partir de los informes e incidencias emitidas por los usuarios de la organización sobre aquellos intentos de acceso ilegítimos a sus cuentas corporativas. Esto permite evaluar si las credenciales han podido verse comprometidas en el pasado, pudiendo actuar en consecuencia para subsanar el problema (ver *Tabla B.24*).

Criterio de éxito	Reporte de accesos sospechosos		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.24: Relación de métricas del criterio de éxito id.3.c)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Un grupo muy reducido de personas reportan esporádicamente los intentos de acceso sospechosos a sus cuentas corporativas de manera indebida.
- Nivel ALTO: Un grupo más amplio de personas de diferentes departamentos reportan con mayor frecuencia los intentos de acceso ilegítimos a sus cuentas corporativas.

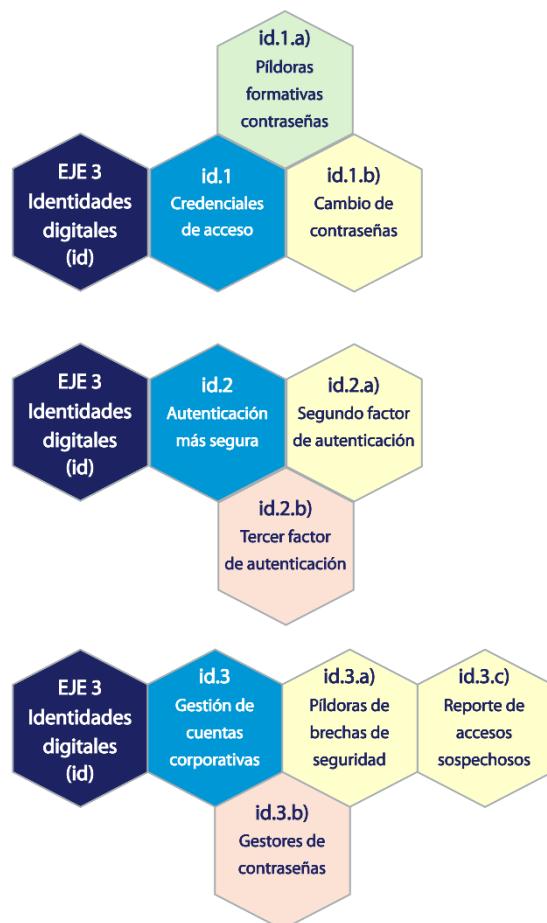


Figura B.3: Eje estratégico 3, líneas de acción y criterios de éxito

red.1.a) Píldoras sobre navegación por Internet

La seguridad de los usuarios al navegar por la red es un aspecto clave para, en la medida de lo posible, evitar poner en peligro datos relevantes de la plantilla y de la propia organización. El acceso a Internet en el puesto de trabajo brinda un amplio abanico de posibilidades a la hora de acceder a la información, pero debiendo ser consciente de los peligros que pueden aparecer (ver *Tabla B.25*).

Criterio de éxito	Píldoras sobre navegación por Internet		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	Anual	Semestral	Trimestral

Tabla B.25: Relación de métricas del criterio de éxito red.1.a)

Aplicación del criterio de éxito:

- Nivel BAJO: Se deben remitir píldoras formativas básicas a todas las personas de la organización, al menos, con una periodicidad anual.
- Nivel MEDIO: Se deben remitir píldoras formativas básicas a todas las personas de la organización, al menos, con una periodicidad semestral.
- Nivel ALTO: Se deben remitir píldoras formativas básicas y más avanzadas a todas las personas de la organización, al menos, con una periodicidad trimestral.

red.1.b) Conexión a redes Wi-Fi públicas

Para navegar por la red se requiere una conexión a Internet que, en muchas ocasiones, se realiza a través de redes Wi-Fi de manera inalámbrica. En este caso, se fomentará el uso único de las redes corporativas habilitadas o, en su defecto, el acceso a través de una red doméstica, evitando siempre que sea posible la conexión a redes Wi-Fi abiertas de manera pública (ver *Tabla B.26*).

Criterio de éxito	Conexión a redes Wi-Fi públicas		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	Sí	Sí	Sí

Tabla B.26: Relación de métricas del criterio de éxito red.1.b)

Aplicación del criterio de éxito:

- Nivel BAJO: Se debe sensibilizar a las personas de la organización para evitar en todo momento el acceso a Internet mediante redes Wi-Fi públicas.
- Nivel MEDIO: Se debe sensibilizar a las personas de la organización para evitar en todo momento el acceso a Internet mediante redes Wi-Fi públicas.
- Nivel ALTO: Se debe sensibilizar a las personas de la organización para evitar en todo momento el acceso a Internet mediante redes Wi-Fi públicas.

red.1.c) Otras conexiones inalámbricas

Además de los accesos a la red vía Wi-Fi, los dispositivos poseen habitualmente otro tipo de conexiones inalámbricas. Unos ejemplos son las conexiones de datos móviles, Bluetooth, NFC, etc, que los usuarios deben desactivar mientras que no las utilicen para su cometido y así evitar posibles riesgos de seguridad, debidos a vulnerabilidades conocidas de estas (ver *Tabla B.27*).

Criterio de éxito	Otras conexiones inalámbricas		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.27: Relación de métricas del criterio de éxito red.1.c)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se recomendará a las personas que eviten dejar activas algunas de las principales conexiones inalámbricas cuando los dispositivos no estén en uso.
- Nivel ALTO: Se recomendará a las personas que eviten dejar activas las principales conexiones inalámbricas cuando los dispositivos no estén en uso.

red.2.a) Píldoras sobre teletrabajo

El auge del teletrabajo o trabajo híbrido a distancia abre a los empleados la oportunidad de trabajar desde el domicilio o cualquier lugar en el que se disponga de acceso a Internet. Algo que en principio es beneficioso para los usuarios, por otro lado, puede entrañar nuevos peligros de ciberseguridad si no se toman las medidas adecuadas, que deben ser conocidas dentro y fuera de las corporaciones (ver *Tabla B.28*).

Criterio de éxito	Píldoras sobre teletrabajo		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.28: Relación de métricas del criterio de éxito red.2.a)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se deben remitir píldoras formativas básicas a las personas de la organización, al menos, con una periodicidad anual.
- Nivel ALTO: Se deben remitir píldoras formativas básicas y avanzadas a las personas de la organización, al menos, con una periodicidad semestral.

red.2.b) Redes privadas virtuales

Uno de los principales componentes que aparecen a la hora de teletrabajar son las conocidas redes privadas virtuales o *Virtual Private Networks (VPN)*. Gracias a las VPN, los usuarios pueden conectarse a las redes internas de la organización, lo cual se convierte en un punto de entrada muy crítico, a la vez que un vector de ataque bastante atractivo para los delincuentes en el ciberespacio (ver *Tabla B.29*).

Criterio de éxito	Redes privadas virtuales		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.29: Relación de métricas del criterio de éxito red.2.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se concienciará y formará a algunas de las personas que teletrabajan de los principales problemas de ciberseguridad que presentan las VPN.
- Nivel ALTO: Se concienciará y formará a todas las personas que teletrabajan de los problemas de ciberseguridad que presentan las VPN.

red.3.a) Píldoras seguridad de la información corporativa

Al exponer nuestra identidad y compartir información personal y profesional en la red, los usuarios velarán por su confidencialidad y privacidad en todo momento. En esta línea, se persigue la capacitación necesaria para conocer los fundamentos básicos en materia de seguridad de la información como la autenticidad, confidencialidad, integridad y trazabilidad (ver *Tabla B.30*).

Criterio de éxito	Píldoras seguridad de la información corporativa		
Nivel de madurez	BAJO	MEDIO	ALTO
Periodicidad	n.a.	Anual	Semestral

Tabla B.30: Relación de métricas del criterio de éxito red.3.a)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se deben difundir píldoras formativas en materia de seguridad de la información a las personas de la organización, al menos, con una periodicidad anual.
- Nivel ALTO: Se deben difundir píldoras formativas en materia de seguridad de la información a las personas de la organización, al menos, con una periodicidad semestral.

red.3.b) Compartición de documentos

A la hora de trabajar con otros usuarios en línea es habitual compartir documentos en servicios típicos como el correo electrónico, aplicaciones de mensajería, repositorios de archivos en la nube o recursos de red corporativa. En cualquiera de estos casos, es elemental estar al tanto de los riesgos que se presentan en los escenarios donde se comparte información sensible, para realizarlo de manera segura y únicamente puedan acceder los destinatarios que se desean (ver *Tabla B.31*).

Criterio de éxito	Compartición de documentos		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	Parcialmente	Sí

Tabla B.31: Relación de métricas del criterio de éxito red.3.b)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: Se fomentará el uso de las principales plataformas corporativas para la compartición segura de documentos internos.
- Nivel ALTO: Se fomentará el uso de manera exclusiva de las plataformas corporativas para la compartición segura de documentos internos, evitando, en cualquier caso, el uso de otras plataformas no autorizadas por el organismo.

red.3.c) Cifrado de archivos y mensajes

Completando el criterio de éxito anterior, y para alcanzar un nivel alto de madurez, la organización formará e incentivará con carácter general en el uso de herramientas complementarias que permitan el intercambio de archivos y mensajes mediante cifrado asimétrico o tecnologías de criptografía de clave pública (ver *Tabla B.32*).

Criterio de éxito	Cifrado de archivos y mensajes		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	n.a.	Sí

Tabla B.32: Relación de métricas del criterio de éxito red.3.c)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Se promocionará el uso extendido de mecanismos de cifrado de los archivos y mensajes de manera segura, en los casos donde se pueda requerir por la naturaleza de la información compartida.

red.3.d) Exposición de metadatos

Finalmente, como parte de la seguridad de la información encontramos la exposición de metadatos (datos que describen a otros datos) en una variedad de documentos compartidos entre los usuarios o publicados por la organización. Para cumplir este criterio de éxito se capacitará sobre los tipos de metadatos e información complementaria que puede aparecer en los principales tipos de documentos ofimáticos y en los contenidos multimedia expuestos en la red (ver *Tabla B.33*).

Criterio de éxito	Exposición de metadatos		
Nivel de madurez	BAJO	MEDIO	ALTO
Cumplimiento	n.a.	n.a.	Sí

Tabla B.33: Relación de métricas del criterio de éxito red.3.d)

Aplicación del criterio de éxito:

- Nivel BAJO: No aplica.
- Nivel MEDIO: No aplica.
- Nivel ALTO: Las personas de la organización deben detectar y ser conscientes de la importancia de la información que puede verse expuesta en los metadatos en el caso de difundir documentos corporativos u otro tipo de contenidos en la red.

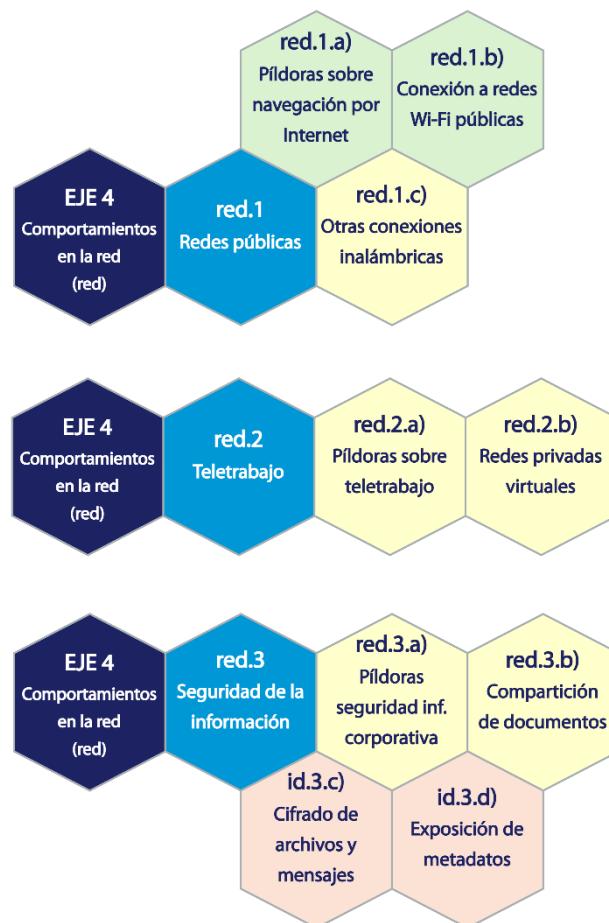


Figura B.4: Eje estratégico 4, líneas de acción y criterios de éxito

ANEXO C. RESULTADOS DEL CASO DE USO

En el presente anexo se muestran las tablas correspondientes a los resultados obtenidos en la evaluación del caso de uso determinado, por cada uno de los criterios de éxito que constituyen los cuatro ejes estratégicos del modelo.

Para la elaboración de las tablas se utiliza el convenio de columnas definido a continuación:

- a) Para comenzar, en la primera columna se determina un identificador del componente descrito en la fila, bien sea una línea de acción o un criterio de éxito.
- b) En la segunda columna, se especifica el nombre de dicho componente del modelo.
- c) La tercera columna muestra el nivel mínimo requerido para cada criterio de éxito.
- d) En la cuarta columna se declara el rango de valores de las métricas.
- e) En la quinta columna se expone la valoración obtenida en el criterio de éxito.
- f) Finalmente, en la sexta y última columna se puntuiza el nivel de madurez alcanzado para el cumplimiento de cada uno de los criterios de éxito.

Al objeto de reunir la información anterior en las tablas y con motivo de limitaciones de espacio, dichas tablas quedan orientadas horizontalmente, quedando centradas en cada página.

En total, el anexo queda compuesto por las siguientes cuatro tablas:

- Tabla C.1: Resultados del eje 1. Ingeniería social (isoc)
- Tabla C.2: Resultados del eje 2. Programas software (sw)
- Tabla C.3: Resultados del eje 3. Identidades digitales (id)
- Tabla C.4: Resultados del eje 4. Comportamientos en la red (red)

ID	Nombre	Nivel mínimo	Rango de valores	Valoración	Nivel alcanzado
isoc.1 Ingeniería social a través del correo electrónico					
isoc.1.a)	Ingeniería social a través del correo electrónico	Bajo	Periodicidad	Semestral	MEDIO
isoc.1.b)	Reportes de correos sospechosos	Medio	Sí/Parcialmente/No	Parcialmente	MEDIO
isoc.1.c)	Campañas de phishing corporativas	Medio	Periodicidad	Semestral	ALTO
isoc.2 Ingeniería social a través del teléfono					
isoc.2.a)	Pildoras formativas llamadas telefónicas	Bajo	Periodicidad	Semestral	MEDIO
isoc.2.b)	Reportes de llamadas sospechosas	Medio	Sí/Parcialmente/No	Parcialmente	MEDIO
isoc2.c)	Simulaciones de llamadas fraudulentas	Alto	Periodicidad	Bienal	ALTO
isoc.3 Redes sociales					
isoc.3.a)	Pildoras formativas redes sociales	Medio	Periodicidad	Anual	MEDIO
isoc.3.b)	Talleres prácticos de fraudes digitales	Alto	Periodicidad	No cumple	-
isoc.4 Bulos y noticias falsas					
isoc.4.a)	Pildoras de bulos y noticias falsas	Medio	Periodicidad	Anual	MEDIO
isoc.4.b)	Pildoras de contenidos manipulados con IA	Alto	Periodicidad	No cumple	-

Tabla C.1: Resultados del eje 1. Ingeniería social (isoc)

ID	Nombre	Nivel mínimo	Rango de valores	Valoración	Nivel alcanzado
sw.1 Seguridad en el software					
sw.1.a)	Actualizaciones de seguridad	Bajo	Periodicidad	Mensual	MEDIO
sw.1.b)	Programas antivirus o similares	Bajo	Sí/Parcialmente/No	Sí	ALTO
sw.1.c)	Copias de seguridad	Bajo	Sí/Parcialmente/No	Sí	ALTO
sw.2 Programas software dañinos					
sw.2.a)	Píldoras formativas malware	Bajo	Periodicidad	Trimestral	MEDIO
sw.2.b)	Identificar los tipos de malware	Bajo	Sí/Parcialmente/No	Sí	ALTO
sw.2.c)	Descarga de sitios oficiales y fiables	Bajo	Sí/Parcialmente/No	Sí	ALTO
sw.2.d)	Simulación de ataques internos	Alto	Periodicidad	No cumple	-

Tabla C.2: Resultados del eje 2. Programas software (sw)

ID	Nombre	Nivel mínimo	Rango de valores	Valoración	Nivel alcanzado
id.1 Credenciales de acceso					
id.1.a)	Píldoras formativas contraseñas	Bajo	Periodicidad	Trimestral	ALTO
id.1.b)	Cambio de contraseñas	Medio	Periodicidad	Semestral	ALTO
id.2 Autenticación más segura					
id.2.a)	Segundo factor de autenticación	Medio	Sí/Parcialmente/No	Sí	ALTO
id.c)	Tercer factor de autenticación	Alto	Sí/Parcialmente/No	No cumple	-
id.3 Gestión de cuentas corporativas					
id.3.a)	Píldoras formativas brechas de seguridad	Medio	Periodicidad	Anual	MEDIO
id.3.b)	Gestores de contraseñas	Alto	Sí/Parcialmente/No	No cumple	-
id.3.c)	Reporte de accesos sospechosos	Medio	Sí/Parcialmente/No	Sí	ALTO

Tabla C.3: Resultados del eje 3. Identidades digitales (id)

ID	Nombre	Nivel mínimo	Rango de valores	Valoración	Nivel alcanzado
red.1 Redes públicas					
red.1.a)	Píldoras sobre navegación por Internet	Medio	Periodicidad	Semestral	MEDIO
red.1.b)	Conexión a redes Wi-Fi públicas	Bajo	Sí/Parcialmente/No	Sí	ALTO
red.1.c)	Otras conexiones inalámbricas	Medio	Sí/Parcialmente/No	Parcialmente	MEDIO
red.2 Teletrabajo					
id.2.a)	Píldoras sobre teletrabajo	Medio	Periodicidad	Anual	MEDIO
id.c)	Redes privadas virtuales	Medio	Sí/Parcialmente/No	Parcialmente	MEDIO
red.3 Seguridad de la información					
red.3.a)	Píldoras seguridad de la información corporativa	Medio	Periodicidad	Anual	MEDIO
red.3.b)	Compartición de documentos	Medio	Sí/Parcialmente/No	Parcialmente	MEDIO
red.3.c)	Cifrado de archivos y mensajes	Alto	Sí/Parcialmente/No	No cumple	-
red.3.d)	Exposición de metadatos	Alto	Sí/Parcialmente/No	No cumple	-

Tabla C.4: Resultados del eje 4. Comportamientos en la red (red)

ANEXO D. ACCESIBILIDAD DEL PROYECTO

En este anexo final se recogen los resultados de cumplimiento y validación de accesibilidad en el trabajo realizado y la documentación entregada, con el fin de hacer accesible el proyecto a aquellas personas con discapacidad en la máxima medida de lo posible.

Primeramente, se habilitaron las opciones de accesibilidad de las herramientas de Microsoft 365 empleadas para ofimática, es decir, Excel y Word, para advertir problemas de accesibilidad de los documentos al objeto de investigarlos y corregirlos debidamente. En la *Figura D.1*, se observan las opciones seleccionadas para activar las funciones de accesibilidad que incorpora Microsoft Word, siendo extensibles al resto de herramientas de la cartera de Microsoft 365 utilizadas en el proyecto.

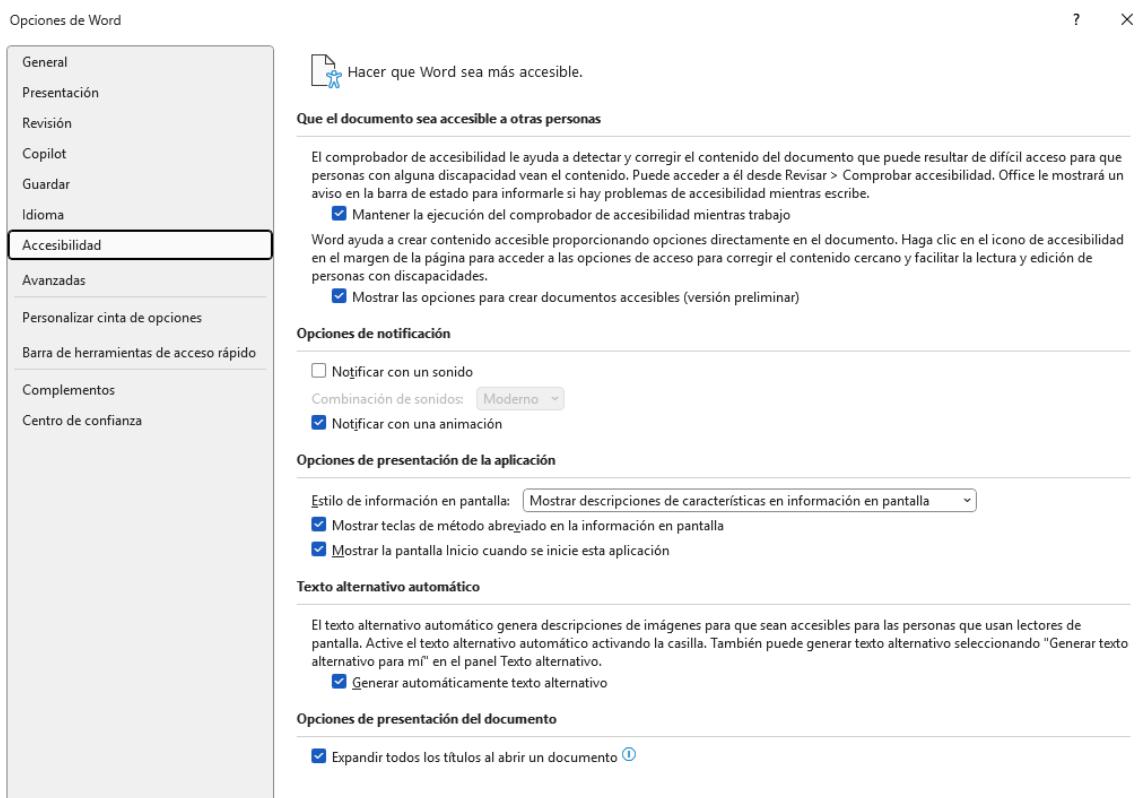


Figura D.1: Configuraciones de accesibilidad en documentos Microsoft

Con las configuraciones de accesibilidad activas, en la parte inferior de cada documento deberá aparecer el estado de cumplimiento de requisitos de accesibilidad. En el caso de existir algún problema de accesibilidad, se mostrará el mensaje: “*Accesibilidad: es necesario investigar*”, tal y como se denota en la *Figura D.2* a continuación:

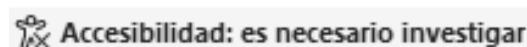


Figura D.2: Advertencia de problemas de accesibilidad en documentos Microsoft

Si pulsamos con el ratón sobre la sección de accesibilidad presentada en la figura anterior, se deberá abrir una ventana en la parte derecha de la pantalla con el asistente de accesibilidad que incluye nativamente la herramienta. En esta zona, se incluirá un resumen de los aspectos validados automáticamente por el asistente, divididos en cinco apartados:

- Color y contraste
- Elementos multimedia e ilustraciones
- Tablas
- Estructura del documento
- Acceso al documento

En el caso de existir alguna sugerencia para la mejora de la accesibilidad del documento (ver *Figura D.3*), se mostrarán en cada uno de los apartados anteriores con su solución correspondiente al pulsar sobre los mismos, tal y como muestra, por ejemplo, la *Figura D.4* en la siguiente página.

Finalmente, una vez corregidos todos los problemas para cumplir con la accesibilidad de los documentos de Microsoft, se deberá actualizar la sección de la parte inferior indicando el mensaje: “*Accesibilidad: todo correcto*” (ver *Figura D.5*), sin haber propuestas de mejora en los distintos apartados evaluados por el asistente de accesibilidad (ver *Figura D.6*) para el documento Excel.

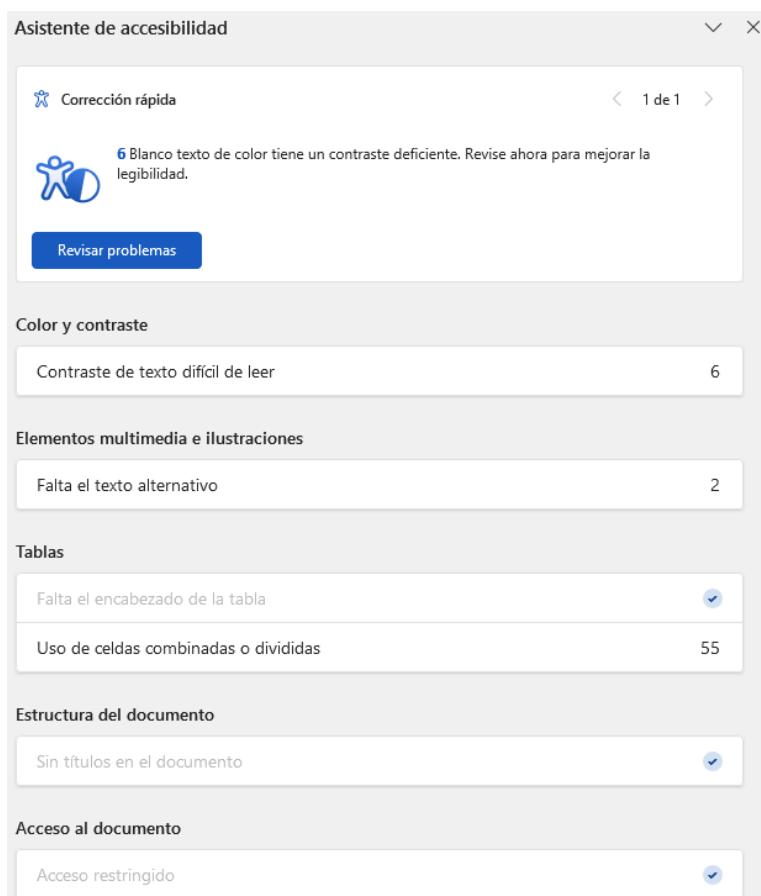


Figura D.3: Problemas de accesibilidad a investigar en un documento

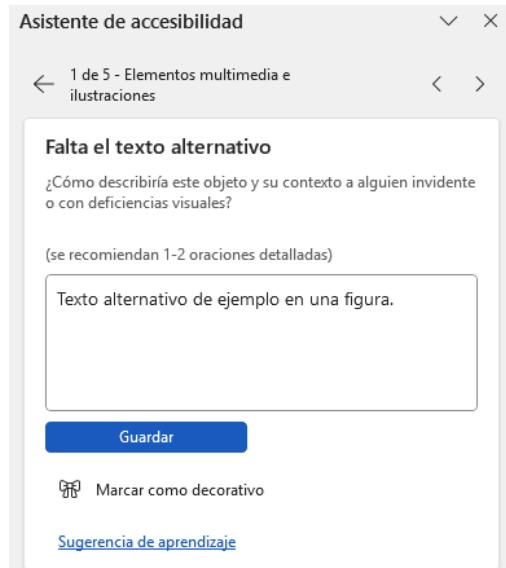


Figura D.4: Solución de accesibilidad para textos alternativos en figuras

Accesibilidad: todo correcto

Figura D.5: Cumplimiento de accesibilidad en el documento

The screenshot shows the Microsoft Word Accessibility Assistant tool with a green checkmark icon at the top. A message says '¡Esto se ve bien! No se encontraron propuestas.' Below are several sections with green checkmarks:

- Color y contraste**: 'Contraste de texto difícil de leer' and 'Evitar el formato en rojo'.
- Elementos multimedia e ilustraciones**: 'Falta el texto alternativo'.
- Tablas**: 'Falta el encabezado de la tabla' and 'Uso de celdas combinadas'.
- Estructura del documento**: 'Nombre de hoja predeterminado'.
- Acceso al documento**: 'Acceso restringido'.

Figura D.6: Cumplimiento en todos los apartados de accesibilidad

Corregidos los problemas de accesibilidad en el documento de Microsoft Word pertenecientes a las secciones de *color* y *contraste*, así como de los *elementos multimedia e ilustraciones*, para la sugerencia de evitar el *uso de celdas combinadas o divididas* en las tablas se propone como medida compensatoria la descripción y explicación textual de toda la información contenida en las mismas.

De esta manera, se procura describir toda la información representada en figuras y tablas mediante párrafos de texto redactados e incluidos en la propia memoria o bien, empleando textos alternativos.

Por último, tras analizar el documento de Microsoft Word con la herramienta PAC 2024 (*PDF Accessibility Checker*), se observa que se ha conseguido cumplir la accesibilidad en la totalidad de los requerimientos básicos, así como se superan mayoritariamente en el resto de los controles de accesibilidad de estructura lógica para PDF/UA, tal y como se muestra en la *Figura D.7*.

No obstante, hay una serie de controles de accesibilidad evaluados por la herramienta PAC 2024 que, para ser subsanados, tras exportar el documento Word a formato PDF, requieren de la utilización de una herramienta adicional como podría ser, por ejemplo, Adobe Acrobat Pro, a la cual el alumnado no dispone de acceso de manera gratuita. De esta manera, sería posible hacer el documento universalmente accesible, cumpliendo con el estándar ISO 14289, conocido como PDF/UA.

CONTROL	APROBADO	PREVENIDO	HA FALLADO
Requerimientos Básicos			
Sintaxis PDF	23135	0	0
Fuentes	26	0	0
Contenido	264691	0	0
Archivos Incorporados	0	0	0
Idioma Natural	119890	0	0
Estructura Lógica			
Elementos de Estructura	949	92	551
Árbol de Estructura	22097	780	0
Mapeo de Roles	22931	0	0
Descripciones Alternativas	29	0	413
Metadatos y Configuración			
Metadatos	2	0	1
Configuración de Documentos	3	0	79

Figura D.7: Resultados de la evaluación de accesibilidad en PAC 2024

En conclusión, el documento PDF de la actual memoria escrita es parcialmente accesible al haber más controles aprobados que no superados, siendo lo más habitual encontrar sitios web de diversas instituciones públicas (por ejemplo: https://www.lamoncloa.gob.es/Paginas/es_Accesibilidad.aspx) que en su declaración de accesibilidad indican que también son *parcialmente conformes*. Por su parte, el documento correspondiente a la plantilla del modelo de madurez en formato Microsoft Excel se considera totalmente accesible por el asistente de accesibilidad incluido en dicha herramienta.

