2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

CÓDIGO	COMPETENCIAS
C01	Capacidad para diseñar e implementar estrategias de ciberseguridad alineadas con los objetivos organizacionales y normativas vigentes.
C02	Competencia en la gestión de riesgos, incluyendo la identificación, evaluación y mitigación de amenazas cibernéticas.
C03	Aplicar los procesos según el cumplimiento de normativas internacionales como GDPR, ISO 27001 y ENS, así como en la realización de auditorías de seguridad.
C04	Capacidad para gestionar incidentes cibernéticos, diseñar planes de continuidad del negocio y garantizar la resiliencia operativa.
C05	Competencia para analizar y anticipar tendencias en ciberseguridad, integrando innovación en la toma de decisiones estratégicas.
CÓDIGO	HABILIDADES O DESTREZAS
H01	Capacidad para analizar riesgos y diseñar soluciones prácticas y sostenibles para la protección de activos digitales.
H02	Habilidad para comunicar estrategias de ciberseguridad a diferentes audiencias, incluyendo equipos técnicos, directivos y stakeholders externos.
H03	Liderazgo en la creación de políticas y procedimientos efectivos de seguridad de la información.
H04	Capacidad para priorizar inversiones en ciberseguridad y evaluar el retorno de la inversión (ROI).
H05	Habilidad para coordinar y ejecutar simulacros de respuesta a incidentes cibernéticos.
H06	Capacidad para integrar marcos de gobernanza y gestión en los procesos organizacionales.
H07	Habilidad para fomentar el aprendizaje continuo y la adaptación a nuevas tecnologías y amenazas.
CÓDIGO	CONOCIMIENTOS O CONTENIDOS
CC1	Conocer los procedimientos técnicos de ciberseguridad, incluyendo conceptos básicos de redes, sistemas operativos y arquitectura de TI.
CC2	Conocer las metodologías de análisis y gestión de riesgos (ISO 27005, NIST, OCTAVE).
CC3	Dominar el marco legal y regulatorio de la ciberseguridad (GDPR, ISO 27001, ENS).
CC4	Conocer las estrategias de continuidad del negocio y recuperación ante desastres.
CC5	Conocimiento sobre las principales tecnologías emergentes (IA, *blockchain*, *big data*, *IoT*) y su impacto en la ciberseguridad.
CC6	Conocer os modelos de gobernanza en ciberseguridad y el rol del CISO en las organizaciones.
CC7	Conocimiento sobre los métodos de evaluación del impacto financiero de proyectos de ciberseguridad y priorización de inversiones.