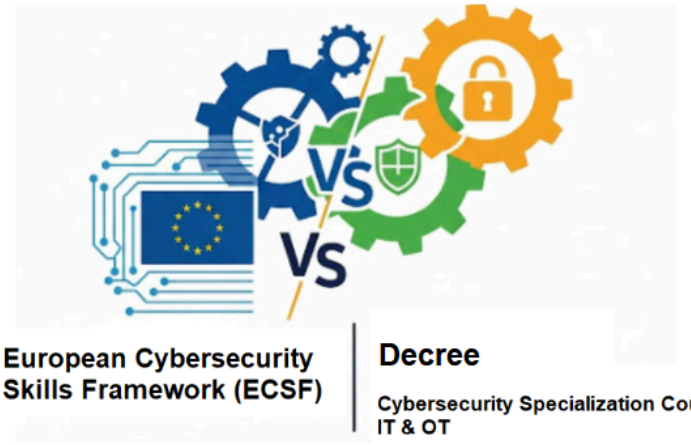


# Competencias Europeas y Contenidos del Cursos de especialización en ciberseguridad IT/OT

## 2025-2026

**ÍNDICE**

# 1. Objetivo y Alcance del Documento de Comparación

**Enisa es** la agencia de Ciberseguridad Europea y desde la misma han definido los roles y perfiles de los técnicos en ciberseguridad necesarios para cubrir el ámbito de la ciberseguridad en las empresas y organismos.El objetivo principal de este marco es crear un entendimiento común entre personas, empleadores y proveedores de programas de formación en los Estados miembros de la UE

**Se han definido 12 perfiles** junto con sus títulos, misiones, tareas, habilidades, conocimientos y competencias que podríamos agrupar en diferentes grupos , unos perfiles de gestión (CISO) y normativa, perfiles de gestor de riesgos, incidentes y amenazas , perfiles técnicos de diseño de arquitectura, auditoría técnica , forense o pentesting y perfiles de formador e investigador

La tarea realizada desde el grupo de ciberseguridad de **Tknika ha sido analizar dichos perfiles y relacionarlos con los Decretos existentes** que regulan los cursos de especialización en ciberseguridad en los ámbitos IT y OT comparando misión,tareas, habilidades y conocimientos de los perfiles con Competencias, resultados de aprendizaje y contenidos de los diferentes módulos.

# 2. Presentación de Enisa y del Marco Europeo de Competencias en Ciberseguridad (ECSF)

## 2.1. ENISA

ENISA (por sus siglas en inglés: European Union Agency for Cybersecurity) es la agencia de ciberseguridad de la Unión Europea. Fue establecida en 2004 y tiene sede en Atenas y Heraclión (Grecia).Es el organismo oficial encargado de **mejorar la ciberseguridad en la Unión Europea**. Su misión principal es ayudar a los Estados miembros, instituciones europeas y al sector privado a **fortalecer sus capacidades** frente a amenazas cibernéticas, promoviendo una cultura común de seguridad digital.

Principales labores de ENISA:

1. Asesoramiento estratégico y técnico
    - Aconseja a la Comisión Europea y a los gobiernos nacionales sobre políticas de ciberseguridad.
    - Colabora en la elaboración y aplicación de legislaciones clave, como el Reglamento NIS2 y la Ley de Ciberresiliencia.
2. Gestión de riesgos y políticas
    - Desarrolla guías, estándares y buenas prácticas para gestionar riesgos tecnológicos y de seguridad.
    - Publica marcos de competencias, como el ECSF (European Cybersecurity Skills Framework).
3. Capacitación y concienciación
    - Apoya la formación de profesionales y promueve campañas para aumentar la conciencia pública sobre ciberseguridad.
    - Organiza eventos como el Mes Europeo de la Ciberseguridad (Cybersecurity Month).
4. Apoyo a los CSIRT
    - Colabora con los Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de los países miembros.
    - Mejora la coordinación en caso de ciberataques transfronterizos.
5. Investigación y análisis de amenazas
    - Publica informes periódicos sobre tendencias en ciberamenazas, vulnerabilidades y ataques emergentes.

- Facilita la compartición de información de ciberinteligencia entre gobiernos y empresas.

6. Certificación en ciberseguridad
    - Supervisa y coordina el Marco Europeo de Certificación de Ciberseguridad, que promueve estándares comunes para productos, servicios y procesos TIC.

## 2.2. Marco Europeo de Competencias en Ciberseguridad (ECSF)

El Marco Europeo de Competencias en Ciberseguridad —en inglés, European Cybersecurity Skills Framework (ECSF)— es una iniciativa desarrollada por ENISA (la Agencia de Ciberseguridad de la Unión Europea) para establecer un lenguaje común sobre las funciones, habilidades y conocimientos necesarios en el campo de la ciberseguridad dentro de Europa.

El ECSF es un modelo estructurado que define y clasifica los roles profesionales de ciberseguridad, describiendo para cada uno:

- Sus principales funciones y tareas,
- Las habilidades técnicas y no técnicas que requiere,
- Los conocimientos fundamentales asociados.

Está diseñado para alinear la oferta educativa, las necesidades del mercado laboral y las políticas públicas de formación en ciberseguridad.

### *Objetivos del ECSF:*

A. Establecer un lenguaje común entre empresas, instituciones educativas y administraciones públicas.
B. Identificar y clasificar roles profesionales en ciberseguridad.
C. Facilitar el diseño de programas formativos y certificaciones basadas en necesidades reales del sector.
D. Apoyar la planificación de carreras para profesionales y la contratación para empleadores.
E. Reducir la brecha de talento en ciberseguridad en Europa.

¿A quién va dirigido?

- Empresas y empleadores: para definir descripciones de puesto y necesidades de contratación.
- Formadores y universidades: para alinear programas educativos con el mercado laboral.

- Profesionales: para orientar el desarrollo de sus habilidades y su carrera.

- Políticos y reguladores: para crear políticas coherentes en competencias digitales.

### *Contenido del ECSF*

El ECSF identifica 12 roles profesionales clave en ciberseguridad.Cada uno viene acompañado de una descripción detallada de funciones, habilidades requeridas, conocimientos y herramientas asociadas.

1. **Director de seguridad de la información (Ciso)** (**Chief Information Security Officer (CISO))**

   Dirige la estrategia de ciberseguridad y alinea políticas y recursos con los objetivos de negocio.

2. **Respuesta a incidentes cibernéticos (Cyber Incident Responder)**
   Detecta, analiza, contiene y recupera incidentes para minimizar el impacto operativo y reputacional.
3. **Responsable de políticas, cumplimiento y asuntos jurídicos cibernéticos (Cyber Legal, Policy & Compliance Officer)**
   Asegura el cumplimiento de leyes, normas y políticas internas relacionadas con la seguridad.
4. **Especialista en inteligencia contra amenazas cibernéticas (Cyber Threat Intelligence Specialist**)

   Recopila y correlaciona información sobre actores, tácticas y campañas para anticipar ataques.

5. **Arquitecto de ciberseguridad (Cybersecurity Architect)**
   Diseña arquitecturas, controles y soluciones seguras que soportan los requisitos de negocio.
6. **Auditor de ciberseguridad (Cybersecurity Auditor)**
   Evalúa la eficacia de los controles y emite recomendaciones para mejorar la postura de seguridad.
7. **Educador en ciberseguridad (Cybersecurity Educator)**
   Desarrolla e imparte formación, concienciación y programas de capacitación en ciberseguridad.
8. **Implementador de ciberseguridad (Cybersecurity Implementer)**
   Integra, configura y mantiene soluciones técnicas (firewalls, IAM, EDR, etc.) conforme a la política de la organización.

9. **Investigador en ciberseguridaD (Cybersecurity Researcher)**
   Conduce investigación básica y aplicada, genera innovación y publica resultados que amplían el estado del arte.
10. **Gerente de riesgos de ciberseguridaD (Cybersecurity Risk Manager)**
    Identifica, analiza y trata riesgos de ciberseguridad para mantenerlos dentro del umbral aceptable.
11. **Investigador forense digital (Digital Forensics Investigator)**
    Recoge y analiza evidencias digitales, documenta hallazgos y los presenta ante las partes interesadas .
12. **Probador de penetración (Penetration Tester**)Realiza pruebas de intrusión controladas para descubrir vulnerabilidades y recomendar medidas de remediación.


## *Resumen*

El ECSF (Marco Europeo de Competencias en Ciberseguridad) es una herramienta estratégica de la UE para armonizar, profesionalizar y fortalecer el ecosistema europeo de ciberseguridad, ayudando a formar, contratar y desarrollar a los expertos que necesita el continente para enfrentar las crecientes amenazas digitales.

# 3. Presentación del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de Información

Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo.

DECRETO BOPV 83/2023, de 6 de junio, por el que se establecen los currículos correspondientes al curso de especialización en Ciberseguridad en entornos de las Tecnologías de la Información,

## *Identificación*

**Denominación**: Ciberseguridad en Entornos de las Tecnologías de la Información.

**Nivel**: Formación Profesional de Grado Superior.

**Duración**: 900 horas

**Familia Profesional**: Informática y Comunicaciones (únicamente a efectos de clasificación de las enseñanzas de Formación Profesional).

**Rama de conocimiento**: Ingeniería y Arquitectura.

**Créditos ECTS**: 43.

## *Competencia general:*

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las edidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

*Módulos profesionales.*

| Código | Módulo Profesional | Asignación horaria |
|---|---|---|
| 5021 | Incidentes de ciberseguridad | 105 |
| 5022 | Bastionado de redes y sistema | 240 |
| 5023 | Puesta en producción segura | 150 |
| 5024 | Análisis forense informático | 120 |
| 5025 | Hacking ético | 150 |
| 5026 | Normativa de ciberseguridad | 60 |
| E300 | Fundamentos básicos | 75 |
| | Total | 900 |

# 4. Presentación del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de Operación

Real Decreto 478/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de operación

DECRETO BOVP 83/2023, de 6 de junio, por el que se establecen los currículos correspondientes al curso de especialización en Ciberseguridad en Entornos de las Tecnologías de Operación

## *Identificación*

**Denominación**: Ciberseguridad en Entornos de las Tecnologías de Operación.
**Nivel**: Formación Profesional de Grado Superior.
**Duración**: 900 horas.
**Familia Profesional**: Electricidad y Electrónica (únicamente a efectos de clasificación de las enseñanzas de Formación Profesional).
**Rama de conocimiento**: Ingeniería y Arquitectura.
**Créditos ECTS**: 43.

## *Competencia general*

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en las organizaciones e infraestructuras industriales realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

## *Módulos profesionales*

| Código | Módulo Profesional | Asignación horaria |
|---|---|---|
| 5027 | Ciberseguridad en proyectos industriales | 150 |
| 5028 | Sistemas de control industrial seguros | 180 |
| 5029 | Redes de comunicaciones industriales seguras | 210 |
| 5030 | Análisis forense en ciberseguridad industrial | 240 |
| 5031 | Seguridad integral | 120 |
| | Total | 900 |

# 5. ANALIZAR RELACIÓN ENTRE PERFILES DEL MARCO EUROPEO Y LAS COMPETENCIAS PROFESIONALES DE LOS DECRETOS IT/OT

Se ha realizado un análisis comparativo entre el Marco Europeo de Competencias en Ciberseguridad (ECSF) de ENISA y el contenido curricular (Decreto) del Curso de Especialización en Ciberseguridad en Entornos de Tecnologías de la Información.

Se han relacionado en cada perfil las tareas principales (Main task) con los resultados de aprendizaje (RA) de cada módulo , las habilidades clave (Key Skills) con las competencias profesionales personales y sociales y los conocimientos clave (Key knowledge) con los contenidos de cada módulo.

- Main Task > Módulo (RA)
- Key skills > Competencias profesionales personal y sociales
- Key knowledge > Módulos ( Contenidos )

## 5.1. Análisis ECSF & Decreto IT

### 5.1.1. Perspectivas generales

Tras el estudio realizado —y antes de pasar a verlo en detalle en apartados posteriores—, vamos a plasmar a modo de visión general en qué medida concluímos que se tratan los perfiles el ECSF en nuestro Decreto.

| ECSF | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Decreto | 55% | 54% | 63% | 58% |

Como veremos, los perfiles con mayor puntuación se asocian a conocimientos más técnicos, mientras que los que tienen puntuaciones más bajas tienen mayor relación con funciones de gestión o pedagógicas, lo cual es totalmente entendible dada la naturaleza de los cursos de especialización.

### 5.1.2. Información más detallada

La puntuación total por perfil (suma de tareas, habilidades y conocimiento) nos permite estimar la alineación. Valores más altos indican una mayor adecuación del Decreto al marco europeo. A continuación, se muestra una tabla ordenada según el porcentaje de alineación total por perfil:

| Perfil | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Analista de Penetración | 81% | 77% | 88% | 82% |
| Gestor de Riesgos de Ciberseguridad | 75% | 92% | 65% | 77% |
| Investigador Forense Digital | 88% | 70% | 73% | 77% |
| Implementador de Ciberseguridad | 70% | 64% | 75% | 70% |
| Agente Legal, de Políticas y de Cumplimiento Cibernético | 56% | 53% | 70% | 60% |
| Investigador de Ciberseguridad | 58% | 64% | 50% | 58% |
| Responsable de Respuesta a Incidentes Cibernéticos | 61% | 46% | 63% | 57% |
| Auditor de Ciberseguridad | 38% | 50% | 72% | 53% |
| Arquitecto de Ciberseguridad | 46% | 40% | 62% | 49% |
| Director de Seguridad de la Información | 32% | 41% | 52% | 42% |
| Especialista en Inteligencia de Amenazas Cibernéticas | 46% | 33% | 42% | 40% |
| Educador de Ciberseguridad | 13% | 19% | 47% | 26% |

### 5.1.3. Clasificación según alineación

#### *Alineación más fuerte: Funciones técnicas y prácticas*

Las tasas de coincidencia más altas se encuentran en perfiles centrados en perfiles que requieren de mayores conocimientos técnicos que hayan podido llevarse a la práctica en el aula.

| Perfil | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Analista de Penetración | 81% | 77% | 88% | 82% |
| Gestor de Riesgos de Ciberseguridad | 75% | 92% | 65% | 77% |
| Investigador Forense Digital | 88% | 70% | 73% | 77% |
| Implementador de Ciberseguridad | 70% | 64% | 75% | 70% |

#### *Alineación moderada: estratégica y orientada a la gobernanza perfiles*

Varios perfiles muestran niveles moderados de alineación; son los perfiles cuyos detalles se han podido tratar en el aula, pero que son más difíciles de tratar en entornos simulados como los que se utilizan en el aula.

| Perfil | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Agente Legal, de Políticas y de Cumplimiento Cibernético | 56% | 53% | 70% | 60% |
| Investigador de Ciberseguridad | 58% | 64% | 50% | 58% |
| Responsable de Respuesta a Incidentes Cibernéticos | 61% | 46% | 63% | 57% |
| Auditor de Ciberseguridad | 38% | 50% | 72% | 53% |
| Arquitecto de Ciberseguridad | 46% | 40% | 62% | 49% |

#### *Alineación inferior: perfiles especializados o de gestión*

Como era de esperar, los perfiles más específicos, que tienen un mayor componente de gestión o que están relacionados con la divulgación estratégica tienen un nivel de alineación inferior.

| Perfil | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Director de Seguridad de la Información | 32% | 41% | 52% | 42% |
| Especialista en Inteligencia de Amenazas Cibernéticas | 46% | 33% | 42% | 40% |
| Educador de Ciberseguridad | 13% | 19% | 47% | 26% |

### 5.1.4. Conclusiones

Los datos muestran que el Decreto cubre más del 50% de los detalles de los perfiles definidos por el ECSF en general. Yendo al detalle, hay 4 perfiles que se alinean de manera fuerte (70% ó más), 5 de manera moderada (45% ó más) y 3 de manera débil (menos del 45%). Además, de los 12 perfiles, 8 superan el 50% de alineación y 3 de ellos superan el 75%.

Creemos que, tratándose de un curso de especialización de un curso de duración, los datos demuestran que el currículum es ajustado y alineado en gran medida con las funciones técnicas clave de la ciberseguridad europea.

## 5.2. Análisis ECSF & Decreto OT

### 5.2.1. Perspectivas generales

Tras el estudio realizado —y antes de pasar a verlo en detalle en apartados posteriores—, vamos a plasmar a modo de visión general en qué medida concluímos que se tratan los perfiles el ECSF en nuestro Decreto.

| ECSF | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Decreto | 54% | 56% | 59% | 56% |

Los datos muestran distintos niveles de coincidencia entre los perfiles profesionales y las necesidades del entorno OT. Las funciones con mayor puntuación combinada indican una alineación más sólida con las operaciones técnicas, mientras que otras destacan por componentes estratégicos o especialización temática.

### 5.2.2. Información detallada

La puntuación total por rol (suma de tareas, habilidades y conocimiento) nos permite estimar la alineación. Valores más altos indican una mayor adecuación al ámbito OT, tanto técnico como funcional. A continuación, se muestra el total por rol ordenado de manera descendente:

| OT | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Gestor de Riesgos de Ciberseguridad | 94% | 88% | 75% | 86% |
| Implementador de Ciberseguridad | 83% | 75% | 68% | 75% |
| Evaluador de Penetración | 78% | 70% | 77% | 75% |
| Investigador Forense Digital | 58% | 70% | 52% | 60% |
| Arquitecto de Ciberseguridad | 67% | 48% | 62% | 59% |
| Responsable de Ciberincidentes | 59% | 50% | 65% | 58% |
| Investigador de Ciberseguridad | 52% | 71% | 45% | 56% |
| Especialista en Inteligencia de Amenazas Cibernéticas | 46% | 48% | 48% | 47% |
| Director de Seguridad de la Información | 37% | 47% | 57% | 47% |
| Asesoramiento Legal, de Políticas y de Cumplimiento Cibernético | 35% | 34% | 70% | 46% |
| Auditor de Ciberseguridad | 27% | 38% | 53% | 39% |
| Educador de Ciberseguridad | 6% | 28% | 41% | 25% |

### 5.2.3. Clasificación según alineación

## *Alineación más fuerte: Funciones técnicas y prácticas*

Roles con mayor puntuación total, orientados a implementación y operación en OT:

Las tasas de coincidencia más altas se encuentran en perfiles centrados en perfiles que requieren de mayores conocimientos técnicos que hayan podido llevarse a la práctica en el aula.

| | | | | |
|---|---|---|---|---|
| Gestor de Riesgos de Ciberseguridad | 94% | 88% | 75% | 86% |
| Implementador de Ciberseguridad | 83% | 75% | 68% | 75% |
| Evaluador de Penetración | 78% | 70% | 77% | 75% |

## *Alineación moderada: Estratégica y orientada a la gobernanza*

Roles con enfoque mixto entre técnica y gestión política:

Varios perfiles muestran niveles moderados de alineación; son los perfiles cuyos detalles se han podido tratar en el aula, pero que son más difíciles de tratar en entornos simulados como los que se utilizan en el aula.

| | | | | |
|---|---|---|---|---|
| Investigador Forense Digital | 58% | 70% | 52% | 60% |
| Arquitecto de Ciberseguridad | 67% | 48% | 62% | 59% |
| Responsable de Ciberincidentes | 59% | 50% | 65% | 58% |
| Investigador de Ciberseguridad | 52% | 71% | 45% | 56% |
| Especialista en Inteligencia de Amenazas Cibernéticas | 46% | 48% | 48% | 47% |
| Director de Seguridad de la Información | 37% | 47% | 57% | 47% |
| Asesoramiento Legal, de Políticas y de Cumplimiento Cibernético | 35% | 34% | 70% | 46% |

*Alineación inferior: Roles especializados o de nicho*

Orientados a contextos particulares, educativos o auditores, con menor peso OT en general:

Como era de esperar, los perfiles más específicos, que tienen un mayor componente de gestión o que están relacionados con la divulgación estratégica tienen un nivel de alineación inferior.

| | | | | |
|---|---|---|---|---|
| Auditor de Ciberseguridad | 27% | 38% | 53% | 39% |
| Educador de Ciberseguridad | 6% | 28% | 41% | 25% |

### 5.2.4. Conclusiones

Los datos muestran que el Decreto cubre más del 50% de los detalles de los perfiles definidos por el ECSF en general. Yendo al detalle, hay 3 perfiles que se alinean de manera fuerte (70% ó más), 7 de manera moderada (45% ó más) y 2 de manera débil (menos del 45%). Además, de los 12 perfiles, 7 superan el 50% de alineación y 3 de ellos superan el 75%.

La mayoría de los roles analizados muestran una buena alineación con las exigencias OT, especialmente los centrados en la implementación técnica, arquitectura de seguridad y respuesta a incidentes. Los perfiles mixtos entre técnica y gestión política estarían en la zona intermedia y los perfiles orientados a la educación, la política o el análisis forense tienen una contribución más acotada, aunque relevante en contextos específicos.

Esta diferencia respecto a los valores de IT tiene su logíca si atendemos a la diferente naturaleza de las instalaciones. En el aspecto OT prima la importancia de la arquitectura, la gestión de incidentes y la gestión de riesgos dado que es una instalación en producción. Queda en un segundo plano la parte de gestión y auditoría.

Creemos que, tratándose de un curso de especialización de un curso de duración, los datos demuestran que el currículum es ajustado y alineado en gran medida con las funciones técnicas clave de la ciberseguridad europea.

# 6. Tablas de relación entre perfiles y Decreto

**CHIEF INFORMATION SECURITY OFFICER (CISO)** Director de seguridad de la información (CISO)

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 32% | 37% |
| Key Skill(s) | 41% | 47% |
| Key Knowledge | 52% | 57% |
| | 42% | 47% |

**CYBER INCIDENT RESPONDER** Respuesta a incidentes cibernéticos

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 61% | 59% |
| Key Skill(s) | 46% | 50% |
| Key Knowledge | 63% | 65% |
| | 57% | 58% |

**CYBER LEGAL, POLICY & COMPLIANCE OFFICER** Responsable de políticas, cumplimiento y asuntos jurídicos cibernético

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 56% | 35% |
| Key Skill(s) | 53% | 34% |
| Key Knowledge | 70% | 70% |
| | 60% | 46% |

**CYBER THREAT INTELLIGENCE SPECIALIST** Especialista en inteligencia contra amenazas cibernéticas

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 46% | 46% |
| Key Skill(s) | 33% | 48% |
| Key Knowledge | 42% | 48% |
| | 40% | 47% |

**CYBERSECURITY ARCHITECT** Arquitecto de ciberseguridad

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 46% | 67% |
| Key Skill(s) | 40% | 48% |
| Key Knowledge | 62% | 62% |
| | 49% | 59% |

**CYBERSECURITY AUDITOR** Auditor de ciberseguridad

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 38% | 27% |
| Key Skill(s) | 50% | 38% |
| Key Knowledge | 72% | 53% |
| | 53% | 39% |

**CYBERSECURITY EDUCATOR** Educador en ciberseguridad

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 13% | 6% |
| Key Skill(s) | 19% | 28% |
| Key Knowledge | 47% | 41% |
| | 26% | 25% |

**CYBERSECURITY IMPLEMENTER** Implementador de ciberseguridad

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 70% | 83% |
| Key Skill(s) | 64% | 75% |
| Key Knowledge | 75% | 68% |
| | 70% | 75% |

**CYBERSECURITY RESEARCHER** Investigador en ciberseguridad

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 58% | 52% |
| Key Skill(s) | 64% | 71% |
| Key Knowledge | 50% | 45% |
| | 58% | 56% |

**CYBERSECURITY RISK MANAGER** Gestor de riesgos de ciberseguridad

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 75% | 94% |
| Key Skill(s) | 92% | 88% |
| Key Knowledge | 65% | 75% |
| | 77% | 85% |

**DIGITAL FORENSICS INVESTIGATOR** Investigador forense digital

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 88% | 58% |
| Key Skill(s) | 70% | 70% |
| Key Knowledge | 73% | 52% |
| | 77% | 60% |

**PENETRATION TESTER** Probador de penetración

| CONCEPT | MATCH RATE IN Decreto IT | MATCH RATE IN Decreto OT |
|---|---|---|
| Main Task(s) | 81% | 78% |
| Key Skill(s) | 77% | 70% |
| Key Knowledge | 88% | 77% |
| | 82% | 75% |

## *Tabla resumen %*

| | IT | | | | | OT | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Main task(s) | Key skill(s) | Key knowledge | Total % | | Main task(s) | Key skill(s) | Key knowledge | Total % |
| Director de seguridad de la información (CISO) | 32% | 41% | 52% | 42% | | 37% | 47% | 57% | 47% |
| Respuesta a incidentes cibernéticos | 61% | 46% | 63% | 57% | | 59% | 50% | 65% | 58% |
| Responsable de políticas, cumplimiento y asuntos jurídicos cibernético | 56% | 53% | 70% | 60% | | 35% | 34% | 70% | 46% |
| Especialista en inteligencia contra amenazas cibernéticas | 46% | 33% | 42% | 40% | | 46% | 48% | 48% | 47% |
| Arquitecto de ciberseguridad | 46% | 40% | 62% | 49% | | 67% | 48% | 62% | 59% |
| Auditor de ciberseguridad | 38% | 50% | 72% | 53% | | 27% | 38% | 53% | 39% |
| Educador en ciberseguridad | 13% | 19% | 47% | 26% | | 6% | 28% | 41% | 25% |
| Implementador de ciberseguridad | 70% | 64% | 75% | 70% | | 83% | 75% | 68% | 75% |
| Investigador en ciberseguridad | 58% | 64% | 50% | 58% | | 52% | 71% | 45% | 56% |
| Gestor de riesgos de ciberseguridad | 75% | 92% | 65% | 77% | | 94% | 88% | 75% | 85% |
| Investigador forense digital | 88% | 70% | 73% | 77% | | 58% | 70% | 52% | 60% |
| Probador de penetración | 81% | 77% | 88% | 82% | | 78% | 70% | 77% | 75% |

## *Perfiles (ECSF) % IT*

| IT | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Analista de Penetración | 81% | 77% | 88% | 82% |
| Gestor de Riesgos de Ciberseguridad | 75% | 92% | 65% | 77% |
| Investigador Forense Digital | 88% | 70% | 73% | 77% |
| Implementador de Ciberseguridad | 70% | 64% | 75% | 70% |
| Agente Legal, de Políticas y de Cumplimiento Cibernético | 56% | 53% | 70% | 60% |
| Investigador de Ciberseguridad | 58% | 64% | 50% | 58% |
| Responsable de Respuesta a Incidentes Cibernéticos | 61% | 46% | 63% | 57% |
| Auditor de Ciberseguridad | 38% | 50% | 72% | 53% |
| Arquitecto de Ciberseguridad | 46% | 40% | 62% | 49% |
| Director de Seguridad de la Información | 32% | 41% | 52% | 42% |
| Especialista en Inteligencia de Amenazas Cibernéticas | 46% | 33% | 42% | 40% |
| Educador de Ciberseguridad | 13% | 19% | 47% | 26% |

## *Perfiles (ECSF) % OT*

| OT | Main task(s) | Key skill(s) | Key knowledge | Total % |
|---|---|---|---|---|
| Gestor de Riesgos de Ciberseguridad | 94% | 88% | 75% | 86% |
| Implementador de Ciberseguridad | 83% | 75% | 68% | 75% |
| Evaluador de Penetración | 78% | 70% | 77% | 75% |
| Investigador Forense Digital | 58% | 70% | 52% | 60% |
| Arquitecto de Ciberseguridad | 67% | 48% | 62% | 59% |
| Responsable de Ciberincidentes | 59% | 50% | 65% | 58% |
| Investigador de Ciberseguridad | 52% | 71% | 45% | 56% |
| Especialista en Inteligencia de Amenazas Cibernéticas | 46% | 48% | 48% | 47% |
| Director de Seguridad de la Información | 37% | 47% | 57% | 47% |
| Asesoramiento Legal, de Políticas y de Cumplimiento Cibernético | 35% | 34% | 70% | 46% |
| Auditor de Ciberseguridad | 27% | 38% | 53% | 39% |
| Educador de Ciberseguridad | 6% | 28% | 41% | 25% |

# 7. BIBLIOGRAFIA


Enisa*:* https://www.enisa.europa.eu/

El Marco Europeo de Competencias en Ciberseguridad (ECSF)

https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Instituto Vasco del conocimiento de la formación professional IVAC EEI

https://ivac-eei.eus/es/

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

https://ivac-eei.eus/es/familias-profesionales/informatica-y-comunicaciones-ifc/especializaciones/curso-de-especializacion-en-ciberseguridad-en-entornos-de-las-tecnologias-de-la-informacion.html

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE OPERACIÓN

https://ivac-eei.eus/es/familias-profesionales/electricidad-y-electronica-ele/especializaciones/curso-de-especializacion-en-ciberseguridad-en-entornos-de-las-tecnologias-de-operacion.html

# ➢ ANEXO *I:* RELACIÓN COMPLETA PERFILES & DECRETO

Se ha cuantificado el nivel de cumplimiento (RATE) en el decreto de cada "Detail" del ECSF teniendo en cuenta la siguiente escala: 0% - 25% - 50% - 75% - 100%

**1-Chief Information Security Officer** Director de Seguridad de la Información

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea principal** | Definir, implementar, comunicar y mantener objetivos, requisitos, estrategias y políticas de ciberseguridad alineados con la estrategia empresarial para respaldar los objetivos organizacionales. | M1:RA1(Ea);M2:RA 3(Ef) | 50% | M1:RA1(Ea,Eb, Ed),RA2(Ec.Ed); M2:RA5(Ed) | 50% |
| | Preparar y presentar la visión, las estrategias y las políticas de ciberseguridad para su aprobación por la alta dirección de la organización y garantizar su ejecución. | | 0% | M4:RA1(Ef,Eg) | 25% |
| | Supervisar la aplicación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) | | 0% | M1:RA4(Ea,Ec, Ef);M5:RA5(Ea, Eb,Ec,Ee) | 25% |
| | Educar a la alta dirección sobre los riesgos y amenazas de ciberseguridad y su impacto en la organización. | M1:RA1(Eb,Ec);M2: RA3(Ea),RA10(Ea) | 75% | M5:RA2(Ea,Ed, Eg) | 25% |
| | Asegúrese de que la alta dirección apruebe los riesgos de ciberseguridad de la organización. | M2:RA3(Ec);M6:RA 2(Ec) | 50% | M5:RA5(Ed,eE) | 25% |
| | Desarrollar planes de ciberseguridad | | 0% | M1:RA1(Ee),RA 3(EC) | 75% |
| | Desarrollar relaciones con autoridades y comunidades relacionadas con la ciberseguridad | M1:RA3(Ee); M6:RA1(Ee) | 50% | M5:RA2(Ef,Eg); RA3(Ec,Ed) | 50% |
| | Informar a la alta dirección sobre incidentes, riesgos y hallazgos de ciberseguridad. | M1:RA2(Ec,Ed,Ee),R A5(Eb) | 50% | M4:RA1(Ef),RA 4(Ef) | 50% |


Tknika | Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

| | | | | | |
|---|---|---|---|---|---|
| | Monitorear los avances en ciberseguridad | M1:RA2(Eb,Ed);M2:RA7(Eh); M3:RA7(Ed);M5:RA1(Ei) | 100% | M3:RA9(Ea,Ed, EE) | 100% |
| | Asegurar recursos para implementar la estrategia de ciberseguridad | M2:RA3(e) | 25% | M1:RA2(Ea,Eb) | 25% |
| | Negociar el presupuesto de ciberseguridad con la alta dirección | | 0% | M1:RA2(Ed,Ef) | 0% |
| | Garantizar la resiliencia de la organización ante incidentes cibernéticos | M1:RA4(Ea,Eb,Ed) | 50% | M4:RA6(Mib,Ec,Eg) | 50% |
| | Gestionar el desarrollo continuo de capacidades dentro de la organización | | 0% | M5:RA1(Ea,Ee), RA2(Ee,Ef) | 25% |
| | Revisar, planificar y asignar recursos de ciberseguridad adecuados | | 0% | M1:RA2(Mib,Ed) | 0% |
| | Nivel de cumplimiento | | 32% | | 38% |
| **Habilidad(es) clave** | Evaluar y mejorar la postura de ciberseguridad de una organización | Ca | 25% | Ca,Cb | 35% |
| | Analizar e implementar políticas, certificaciones, estándares, metodologías y marcos de ciberseguridad. | Ce, Ck | 75% | Cb,Cg | 75% |
| | Analizar y cumplir con las leyes, regulaciones y legislaciones relacionadas con la ciberseguridad. | Ca,Cl,Cm | 100% | Ck | 100% |
| | Implementar recomendaciones y mejores prácticas de ciberseguridad | Cb,Cc | 100% | Cj,Ch | 100% |
| | Gestionar recursos de ciberseguridad | | 0% | Cl,Cm | 25% |
| | Desarrollar, defender y liderar la ejecución de una estrategia de ciberseguridad | Cb,Cc | 25% | Cm,Cn | 25% |
| | Influir en la cultura de ciberseguridad de una organización | Ca,Cl | 25% | Cn | 25% |
| | Diseñar, aplicar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) ya sea directamente o liderando su externalización. | | 0% | Ch,Cc | 25% |
| | Revisar y mejorar los documentos de seguridad, informes, SLA y garantizar los objetivos de seguridad. | | 0% | Cc, Ck | 25% |
| | Identificar y resolver problemas relacionados con la ciberseguridad | Cf,Ci | 100% | Ci,Cm | 75% |
| | Establecer un plan de ciberseguridad | Ca,Cc | 50% | Cd,Ca | 50% |
| | Comunicarse, coordinarse y cooperar | Cñ | 50% | Cg,Cn | 50% |

| | | | | | |
|---|---|---|---|---|---|
| | con las partes interesadas internas y externas | | | | |
| | Anticipar los cambios necesarios en la estrategia de seguridad de la información de la organización y formular nuevos planes | Cc | 50% | Ce,Cf | 50% |
| | Definir y aplicar modelos de madurez para la gestión de la ciberseguridad | | 0% | Cf | 25% |
| | Anticipar las amenazas, necesidades y desafíos futuros de la ciberseguridad | | 0% | Este | 50% |
| | Motivar y animar a las personas | Cñ | 50% | Cm | 25% |
| | Nivel de cumplimiento | | 41% | | 48% |
| **Conocimientos clave** | Políticas de ciberseguridad | M2:RA3(C4),RA6(C9),RA9(C8);M7:RA2(C3) | 100% | M2:RA5(C1,C2,C3);M5:RA1(C1,C2,C3),RA2(C1,C2,C3,RA3(C1,C2,C3) | 100% |
| | Estándares, metodologías y marcos de ciberseguridad | M2:RA3(C6);M3:RA6(C4);M6:RA5(C2,C5) | 100% | M3:RA2(C10);M5:RA5(C1,C2,C3) | 100% |
| | Recomendaciones y mejores prácticas de ciberseguridad | M2:RA3(C5,C7);M6:RA5(C3); | 50% | M3:RA7(C1,C5,C6);M5:RA5(C1,C3) | 100% |
| | Leyes, regulaciones y legislaciones relacionadas con la ciberseguridad | M6:RA3(C1,C2,C3),RA4(C*),RA5(C8) | 100% | M5:RA5(C2,C3) | 50% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M1:RA2(C1,C2,C4);M5:RA5(C3) | 0% |
| | Requisitos de una organización de ciberseguridad ética | M6:RA1(C1) | 25% | M2:RA1(C1,C3);M5:RA5(C1,C3) | 25% |
| | Modelos de madurez de la ciberseguridad | | 0% | M1:RA1(C1,C5) | 25% |
| | Procedimientos de ciberseguridad | M1:RA4(C1),RA5(C1);M2:RA3(C7),RA7(C17) | 100% | M1:RA5(C2,C3);M4:RA6(C1,C5) | 100% |
| | Gestión de recursos | | 0% | M1:RA2(C1,C3);M5:RA1(C3) | 25% |
| | Prácticas de gestión | | 0% | M1:RA2(C2,C3);M5:RA5(C1,C2,C3) | 25% |
| | Normas, metodologías y marcos de gestión de riesgos | M2:RA3(C1);M3:RA5(C2);M6:RA2(C3) | 100% | M5:RA5(C1,C2,C3) | 75% |
| | Nivel de cumplimiento | | 52% | | 57% |

## 2- **Cyber Incident Responder** Respuesta a incidentes cibernéticos

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea (s) principal(es)** | Contribuir al desarrollo, mantenimiento y evaluación del Plan de Respuesta a Incidentes | M1:RA5(Ea) | 25% | M4:RA6(Ea,Eb),M5:RA5(Ea,Eb,Ec,Ee) | 25% |
| | Desarrollar, implementar y evaluar procedimientos relacionados con el manejo de incidentes | M1:RA4(Ea,Eb),RA5(Ea) | 50% | M4:RA6(Ea,Eb,Ec,Ee) | 50% |
| | Identificar, analizar, mitigar y comunicar incidentes de ciberseguridad | M1:RA2(Mib),RA3(Ea,Ed),RA5(Mib,Ec,Ed,Ee) | 100% | M4:RA1(Ec,Ed),RA6(Ea,Ef,Eg) | 100% |
| | Evaluar y gestionar vulnerabilidades técnicas | M2:RA3(Ea),RA4(Eb,Ec,Ed,Ee),RA9(Eg,Eh);M3:RA6(Ec);M5:RA1(Ef,Eh),RA2(Eb,Ed,Ee,Eg),RA3(Eb,Ee,Ef),RA5(Ed,Ee,Ef,Eg) | 100% | M3:RA8(Ea,Ed,Ee) | 100% |
| | Medir la eficacia de la detección y respuesta ante incidentes de ciberseguridad | M1:RA2(Mib,Ed),RA3(Mib,Ef),RA4(Ea,Mib,Ed), | 100% | M3:RA9(EA;Ed,Ee) | 75% |
| | Evaluar la resiliencia de los controles de ciberseguridad y las acciones de mitigación adoptadas después de un incidente de ciberseguridad o violación de datos. | M1:RA4(Ea,Eb) | 25% | M4:RA6(Mib,Ec,Eg) | 25% |
| | Adoptar y desarrollar técnicas de prueba de manejo de incidentes | M1:RA2(Eb,Ec,Ed),RA3(Ed),R4(Ea,Ec) | 100% | M4:RA6(Ee,Ef) | 75% |
| | Establecer procedimientos para el análisis de los resultados de incidentes y la elaboración de informes sobre el manejo de incidentes. | M1:RA2(Ee),RA5(E*) | 75% | M4:RA4(Ea,Ec,Ed) | 75% |
| | Documentar el análisis de los resultados de los incidentes y las acciones de manejo de incidentes | M1:RA5(Ea) | 25% | M4;RA5(Ef) | 75% |
| | Cooperar con los Centros de Operaciones Seguras (SOC) y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) | M1:RA5(Ed) | 25% | M5:RA5(Ef,Eg) | 25% |
| | Cooperar con el personal clave para informar incidentes de | M1:RA3(Mib,Mie) | 50% | M4:RA6(Ef.Eg) | 25% |

| | | | | | |
|---|---|---|---|---|---|
| | seguridad de acuerdo con el marco legal aplicable. | | | | |
| | Nivel de cumplimiento | | 61% | | 59% |
| **Habilidad(es) clave** | Practicar todos los aspectos técnicos, funcionales y operativos del incidente de ciberseguridad. Manejo y respuesta | Cf | 75% | Cc, Cd, Cm, Cj, Cn | 75% |
| | Recopilar, analizar y correlacionar información sobre amenazas cibernéticas procedente de múltiples fuentes | Cb | 75% | Ca, Ch, Ci, Cg | 75% |
| | Trabajar en sistemas operativos, servidores, nubes e infraestructuras relevantes. | | 0% | Cb, Cf, Ch | 0% |
| | Trabajar bajo presión | Cñ | 75% | Cb, Cf, Ch | 75% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | Cñ | 50% | Cl,Cm | 50% |
| | Administrar y analizar archivos de registro | | 0% | Cc, Ck, Cn | 25% |
| | Nivel de cumplimiento | | 46% | | 50% |
| **Conocimientos clave** | Estándares, metodologías y marcos de gestión de incidentes | | 0% | M4:RA1(C2,C3,C4);M5:RA5(C1,C3) | 50% |
| | Recomendaciones y mejores prácticas para el manejo de incidentes | M1:RA4(C6) | 75% | M3:RA10(C1,C2,C3);M4:RA6(C1,C2,C4,C6) | 75% |
| | Herramientas de gestión de incidentes | M1:RA2(C2,C3,C4) | 50% | M3:RA9(C1,C2);M4:RA2(C7,C9) | 50% |
| | Procedimientos de comunicación para el manejo de incidentes | M1:RA3(C5),RA4(C3),RA5(C*) | 100% | M4:RA6(C4,C5,C6);M5:RA5(C3,C5) | 75% |
| | Seguridad de los sistemas operativos | M7:RA3(C1,C2) | 75% | M2:RA6(C1,C4);M3:RA11(C2,C3) | 75% |
| | Seguridad de redes informáticas | M2:RA1(C*),RA3(C*),RA6(C*);M7:RA1(C1,C2,C3) | 100% | M3:RA5(C1,C2,C4),RA6(C1,C3) | 100% |
| | amenazas cibernéticas | M1:RA3(C4);M2:RA3(C1);M3:RA5(C2) | 100% | M3:RA8(C5,C6);M4:RA2(C2,C6,C7) | 100% |
| | Procedimientos de ataque a la ciberseguridad | M5: RA2(C4,C5), RA3(C6,C7,C8), RA5(C6), | 100% | M3:RA8(C3,C4);M4:RA6(C2,C | 100% |

| | | | | | |
|---|---|---|---|---|---|
| | | RA6(C4) | | 6) | |
| | Vulnerabilidades de los sistemas informáticos | M2:RA10(C10);M3:RA6(C2, C6);M5:RA3(C6,C9),RA5(C5, C6,C7) | 100% | M4:RA2(C7,C9 ) | 100% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M1:RA2(C2,C3 );M5:RA5:C1,C 3) | 0% |
| | Leyes, regulaciones y legislaciones relacionadas con la ciberseguridad | M6:RA3(C1,C2,C3),RA4(C*), RA5(C8) | 100% | M5:RA5(C2,C3 ) | 100% |
| | Operación de los Centros de Operaciones Seguras (SOC) | M2:RA7(C19) | 25% | M3:RA9(C1,C2 );M4:RA6(C1,C 5,C6) | 25% |
| | Operación de los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) | | 0% | M4:RA6(C3,C4, C5) | 0% |
| | Nivel de cumplimiento | | 63% | | 65% |

**3- Cyber Legal, Policy & Compliance Officer** Responsable de Asuntos Legales, Políticas y Cumplimiento Cibernético

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Garantizar el cumplimiento y brindar asesoramiento y orientación legal sobre las normas, leyes y regulaciones de privacidad y protección de datos. | M2:RA4(E*);M3:RA6(Ef);M4:RA4(Ee);M6:RA4(E*) | 100% | M5:RA5(Ea,Eb,Ec,Ee) | 50% |
| | Identificar y documentar las brechas de cumplimiento | M1:RA1(Ee);M6:RA1(Ea,Ec,Ed,Ee);RA2(Ed);RA3(Ec),RA4(Ed) | 100% | M5:RA3(Ea,Eb,Ef),RA5(Ed,Ee) | 75% |
| | Realizar evaluaciones de impacto sobre la privacidad y desarrollar, mantener, comunicar y capacitar sobre las políticas y procedimientos de privacidad. | M1:RA1(Eb,Ec,Ed); M6:RA3(Eb),RA4(Ec) | 75% | M5:RA1(Ee,Ef,Eg),RA2(Eb,Ee,Eg) | 50% |
| | Hacer cumplir y defender el programa de privacidad y protección de datos de la organización | M1:RA1(Ea); M6:RA4(Ea,Eb,Ec,Ed,Ee,Ef) | 100% | M5:RA1(Ec,Ef),RA5(Eb,Ed,Ee) | 50% |
| | Garantizar que los propietarios, titulares, responsables, encargados del tratamiento, sujetos, socios y entidades internas o externas estén informados sobre sus derechos en materia de protección de datos, | M6:RA4(E1) | 25% | M5:RA2(Ea,Ed,Eg),RA5(Ee,Ef) | 25% |
| | Actuar como punto de contacto clave para gestionar consultas y quejas relativas al procesamiento de datos. | M6:RA4(Ee) | 25% | M4:RA1(Ea,Ef,Eg),RA3(Ef,Eg) | 25% |
| | Ayudar en el diseño, implementación, auditoría y actividades de pruebas de cumplimiento para garantizar el cumplimiento de la ciberseguridad y la privacidad. | M1:RA1(Ee);M6:RA4(Ec) | 50% | M4:RA1(Eb,Ec,Ee),RA3(Ec,Ee) | 25% |
| | Supervisar las auditorías y las actividades de formación relacionadas con la protección | M1:RA1(Ec,Ed,Ee) | 50% | M5:RA3(Ed,Ef,Eg),RA4(Ea,Ec) | 25% |

| | | | | | |
|---|---|---|---|---|---|
| | de datos | | | | |
| | Cooperar y compartir información con autoridades y grupos profesionales | M1:RA5(Ee) | 25% | M5:RA2(Ef,Eg) | 25% |
| | Contribuir al desarrollo de la estrategia, política y procedimientos de ciberseguridad de la organización. | M1:RA1(Ec) | 25% | M1:RA1(Ea,Eb,Ed) | 25% |
| | Desarrollar y proponer capacitaciones de concientización del personal para lograr el cumplimiento y fomentar una cultura de protección de datos dentro de la organización. | M6:RA1(Ec),RA3(Ed) | 50% | M5:RA2(Ee,Eg), RA3(Ea,Eb) | 25% |
| | Gestionar los aspectos legales de las responsabilidades de seguridad de la información y la capacidad de relacionarse con terceros para tenerlos en cuenta en los requisitos legales, reglamentarios y normativos. | M6:RA1(Ee),RA4(Ea) | 50% | M5:RA5(Mib,Ec, Ee) | 25% |
| | Nivel de cumplimiento | | 56% | | 35% |
| **Habilidad(es) clave** | Comprensión integral de la estrategia comercial, modelos y productos y capacidad para tener en cuenta los requisitos legales, regulatorios y normativos. | Ca, Cj | 50% | Ca, Ck | 25% |
| | Realizar prácticas de vida laboral en las cuestiones de protección de datos y privacidad involucradas en la implementación de los procesos organizacionales, financieros y de estrategia de negocios. | Cd,Ce | 100% | Ca, Cd, Ck | 25% |
| | Liderar el desarrollo de políticas y procedimientos de ciberseguridad y privacidad adecuados que complementen las necesidades comerciales y los requisitos legales; | Ca | 25% | Ca, Cb, Cj, Cl | 25% |

| | | | | | |
|---|---|---|---|---|---|
| | Realizar, supervisar y revisar evaluaciones de impacto sobre la privacidad utilizando estándares, marcos, metodologías y herramientas reconocidas. | Cj | 50% | Ca, Cc, Ch, Cj | 25% |
| | Explicar y comunicar temas de protección de datos y privacidad a las partes interesadas y a los usuarios. | Cñ | 50% | Cl,Cm | 50% |
| | Comprender, practicar y adherirse a los requisitos y estándares éticos. | | 0% | Cl | 25% |
| | Comprender las implicaciones de las modificaciones del marco legal en la estrategia y políticas de ciberseguridad y protección de datos de la organización. | Ca,Cm | 75% | Ca, Ck | 25% |
| | Colaborar con otros miembros del equipo y colegas. | Cñ | 75% | Cm,Cl | 75% |
| | Nivel de cumplimiento | | 53% | | 34% |
| **Conocimientos clave** | Leyes, regulaciones y legislaciones relacionadas con la ciberseguridad | M6:RA3(C1,C2,C3),RA4(C*),RA5(C8) | 100% | M4:RA6(C5,C6); M5:RA5(C3) | 100% |
| | Estándares, metodologías y marcos de ciberseguridad | M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5) | 100% | M2:RA3(C1);M5:RA5(C1,C3) | 100% |
| | Políticas de ciberseguridad | M2:RA3(C4),RA9(C8) | 50% | M1:RA4(C3,C5); M2;RA5(C1,C3) | 75% |
| | Requisitos, recomendaciones y mejores prácticas de cumplimiento legal, reglamentario y legislativo | M2:RA3(C3,C5);M6:RA5(C3) | 75% | M5:RA1(C1,C2), RA5(C2,C3) | 50% |
| | Estándares, metodologías y marcos de evaluación del impacto en la privacidad | M6:RA4(C3,C4) | 25% | M4:RA2(C5,C7); M5:RA5(C1,C3) | 25% |
| | Nivel de cumplimiento | | 70% | | 70% |

**4- Cyber Threat Intelligence Specialist** Especialista en inteligencia contra amenazas cibernéticas

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Desarrollar, implementar y gestionar la estrategia de inteligencia sobre amenazas cibernéticas de la organización. | M1:RA4(Ea,Ec),RA5(Ea) | 50% | M1:RA1(Ea,Eb,Ed);M5:RA5(Ea,Ec,Ee) | 50% |
| | Desarrollar planes y procedimientos para gestionar la inteligencia de amenazas | M1:RA4(Ea,Ec),RA5(Ea) | 50% | M5:RA5(Mib,Ed,Ef) | 50% |
| | Traducir los requisitos de negocio en requisitos de inteligencia | | 0% | M1:RA1(Ea,Ec,Ee) | 25% |
| | Implementar la recopilación de inteligencia sobre amenazas, el análisis y la producción de inteligencia procesable y su difusión a las partes interesadas en la seguridad. | | 0% | M4:RA2(Ea,Ec,Ef) | 25% |
| | Identificar y evaluar a los actores de amenazas cibernéticas que atacan a la organización | M1:RA2(Eb,Ec,Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb) | 100% | M3:RA8(Ea,Eb,Ed) | 75% |
| | Identificar, monitorear y evaluar las tácticas, técnicas y procedimientos (TTP) utilizados por los actores de amenazas cibernéticas mediante el análisis de datos e información de código abierto y de propiedad exclusiva. | M1:RA2(Mib,Ec,Ed,Ee) | 50% | M3:RA7(Ea,Ec),RA8(Ee,Eg) | 50% |
| | Producir informes prácticos basados en datos de inteligencia sobre amenazas | M4:RA1(Ef),Ra3(Ec),RA5(Eh),RA6(Ea,Eb),M5:RA2(Eg),RA3(Ef) | 100% | M4:RA4(Mib,Ec,Ed) | 75% |
| | Elaborar y asesorar sobre planes de mitigación a nivel táctico, operativo y estratégico. | M1:RA4(Ea);M5:RA2(Por ejemplo),RA3(Por ejemplo),RA5(Por ejemplo) | 100% | M5:RA5(Ed,Ee) | 100% |
| | Coordinar con las partes interesadas para compartir y consumir inteligencia sobre amenazas cibernéticas relevantes | M1:RA3(Ee) | 25% | M5:RA2(Ef,Eg) | 25% |
| | Aprovechar los datos de inteligencia para respaldar y ayudar con el modelado de amenazas, las recomendaciones para la mitigación de riesgos y la | M1:RA4(Ea),M6:RA3(Eb) | 50% | M4:RA3(Mib,Ed,Ee),RA6(Ea,Eg) | 50% |

| | | | | | |
|---|---|---|---|---|---|
| | búsqueda de amenazas cibernéticas. | | | | |
| | Articular y comunicar inteligencia de forma abierta y pública en todos los niveles | | 0% | M4:RA1(Ej.) | 0% |
| | Transmitir la severidad de seguridad adecuada explicando la exposición al riesgo y sus consecuencias a las partes interesadas no técnicas. | M2:RA3(Ec,Ee) | 25% | M4:RA4(Ea, Ef) | 25% |
| | Nivel de cumplimiento | | 46% | | 46% |
| **Habilidad(es) clave** | Colaborar con otros miembros del equipo y colegas. | Cñ | 75% | Cl,Cm | 75% |
| | Recopilar, analizar y correlacionar información sobre amenazas cibernéticas procedente de múltiples fuentes | Cb | 50% | Ca, Cb, Cc, Ch | 75% |
| | Identificar las TTP y campañas de los actores amenazantes | Cb | 25% | Ca,Cb | 50% |
| | Automatizar los procedimientos de gestión de inteligencia de amenazas | | 0% | Cg,Cl | 0% |
| | Realizar análisis técnicos e informes | Cf | 75% | Cc, Ck | 100% |
| | Identificar eventos no cibernéticos con implicaciones en actividades cibernéticas | | 0% | Ca,Cd | 50% |
| | Amenazas, actores y TTP del modelo | Cb | 25% | Ca,Cc | 25% |
| | Comunicarse, coordinarse y cooperar con las partes interesadas internas y externas | Cñ | 50% | Cm,Cn | 50% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | Cm | 25% | Cc, Ck | 50% |
| | Utilizar y aplicar plataformas y herramientas CTI | | 0% | Cg, Ch | 0% |
| | Nivel de cumplimiento | | 33% | | 48% |
| **Conocimientos clave** | Seguridad de los sistemas operativos | M7:RA3(C1,C2) | 25% | M2:RA6(C1, C4);M3:RA11(C2,C3) | 25% |
| | Seguridad de redes informáticas | M2:RA3(C5,C6),RA6(C1) | 50% | M3:RA5(C1, C2),RA6(C3) | 100% |
| | Controles y soluciones de ciberseguridad | M1:RA2(C2,C3,C4) | 50% | M2:RA4(C3, C4);M3:RA10(C3,C5) | 50% |

| | | | | | |
|---|---|---|---|---|---|
| | Programación de computadoras | M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*) | 100% | M2:RA2(C2, C6) | 75% |
| | Estándares, metodologías y marcos de intercambio de inteligencia sobre amenazas cibernéticas (CTI) | | 0% | M4:RA6(C1, C3,C5) | 0% |
| | Procedimientos de divulgación responsable de información | M1:RA3(C5) | 25% | M4:RA6(C4, C5) | 25% |
| | Conocimientos interdominios y fronterizos relacionados con la ciberseguridad | | 0% | M1:RA1(C1, C4) | 25% |
| | amenazas cibernéticas | M1:RA3(C4);M2:RA3(C1);M3:RA5(C2) | 100% | M3:RA8(C3, C5);M4:RA2(C2,C6) | 100% |
| | Actores de amenazas cibernéticas | M1:RA3(C4);M2:RA3(C1);M3:RA5(C2) | 100% | M3:RA9(C1, C2) | 100% |
| | Procedimientos de ataque a la ciberseguridad | M5: RA1(C4), RA2(C4, C5), RA3(C5, C6, C7, C8, C9), RA4(C2), RA5(C3, C6) | 100% | M3:RA8(C4, C6) | 100% |
| | Ciberamenazas avanzadas y persistentes (APT) | | 0% | M4:RA3(C5) | 25% |
| | Tácticas, técnicas y procedimientos (TTP) de los actores de amenazas | | 0% | M4:RA4(C4, C5) | 25% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M5:RA5(C3) | 0% |
| | Nivel de cumplimiento | | 42% | | 50% |

## 5- **Cybersecurity Architect** Arquitecto de ciberseguridad

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Diseñar y proponer una arquitectura segura para implementar la estrategia de la organización | M2:RA3(Ee),RA10(Eb) | 50% | M1:RA1(Ea,Ee),RA3(Eb,Ec,Ed); M5:RA5(Eb,Ec,Ed) | 50% |
| | Desarrollar la arquitectura de ciberseguridad de la organización para abordar los requisitos de seguridad y privacidad. | M6:R4(Cc),RA5(Eg) | 50% | M5:RA4(Ec,Ed),RA5(Ea,Ee) | 75% |
| | Elaborar documentación y especificaciones arquitectónicas. | M2:RA3(Ee) | 25% | M4:RA4(Mib,Ed,Ef) | 100% |
| | Presentar el diseño de la arquitectura de seguridad de alto nivel a las partes interesadas | | 0% | M4:RA4(Ea,Ec,Ef) | 50% |
| | Establecer un entorno seguro durante el ciclo de vida de desarrollo de sistemas, servicios y productos | M2:RA6(Ef),RA10(Ef) | 50% | M2:RA6(Ea,Eb,Ee) | 75% |
| | Coordinar el desarrollo, integración y mantenimiento de los componentes de ciberseguridad asegurando las especificaciones de ciberseguridad. | M2:RA10(Ej.) | 25% | M2:RA7(Mib,Ed,Eg) | 50% |
| | Analizar y evaluar la ciberseguridad de la arquitectura de la organización. | M1:RA1(Ee),M2:RA3(Eb);M3:RA8(Ee) | 100% | M3:RA3(Ea,Eb,Ed,Ee) | 100% |
| | Garantizar la seguridad de las arquitecturas de soluciones a través de revisiones de seguridad y certificación. | | 0% | M5:RA5(Ea,Ed,Ee) | 25% |
| | Colaborar con otros equipos y colegas | M4:RA1(Eg),RA3(Ed),RA4(Ef),RA5(Ei) | 100% | M5:RA2(Ef,Eg) | 100% |
| | Evaluar el impacto de las soluciones de ciberseguridad en el diseño y el rendimiento de la arquitectura de la organización. | | 0% | M3:RA7(Ec,Ee,Ef) | 25% |
| | Adaptar la arquitectura de la organización a las amenazas emergentes | M1:RA2(Ea),M2:RA3(Ea),RA10(Ea) | 75% | M1:RA4(Ea,Ed,Ef) | 75% |
| | Evaluar la arquitectura implementada para mantener un nivel de seguridad adecuado | M2:RA3(Ee),RA6(Ea);M3:RA5(Eb) | 75% | M5:RA5(Ec,Ee,Ef) | 75% |
| | Nivel de cumplimiento | | 46% | | 67% |
| **Habilidad(e** | Realizar análisis de requisitos de seguridad de usuarios y empresas | Cb | 50% | Ca, Cb, Cd | 50% |

| | | | | | |
|---|---|---|---|---|---|
| **s) clave** | Elaborar especificaciones arquitectónicas y funcionales de ciberseguridad | Cc | 50% | Cc, Ck | 50% |
| | Descomponer y analizar sistemas para desarrollar requisitos de seguridad y privacidad e identificar soluciones efectivas | Cf | 50% | Ca, Cg, Ch | 50% |
| | Diseñar sistemas y arquitecturas basados en principios de ciberseguridad de seguridad y privacidad por diseño y por defecto | Cc,Ce | 75% | Cb,Cj | 75% |
| | Guiar y comunicarse con los implementadores y el personal de TI/OT | Cñ | 25% | Cl,Cm | 25% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | | 0% | Cc, Ck | 25% |
| | Proponer arquitecturas de ciberseguridad basadas en las necesidades y el presupuesto de las partes interesadas | | 0% | Ca,Cb | 25% |
| | Seleccionar especificaciones, procedimientos y controles apropiados | Cc,Ce | 100% | Cj,Cg | 100% |
| | Desarrollar resiliencia frente a puntos de falla en toda la arquitectura | Cd | 50% | Ce,Cn | 50% |
| | Coordinar la integración de soluciones de seguridad | | 0% | Cd,Cj | 25% |
| | Nivel de cumplimiento | | 40% | | 48% |
| **Conocimientos clave** | Certificaciones relacionadas con la ciberseguridad | | 0% | M1:RA2(C2,C3);M5:RA5(C3) | 0% |
| | Recomendaciones y mejores prácticas de ciberseguridad | M2:RA3(C5);M6:RA5(C3) | 50% | M2:RA5(C1,C3);M3:RA7(C1,C2) | 50% |
| | Estándares, metodologías y marcos de ciberseguridad | M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5) | 100% | M2:RA3(C4);M5:RA5(C3) | 100% |
| | Análisis de requisitos relacionados con la ciberseguridad | | 0% | M1:RA1(C2,C5) | 25% |
| | Ciclo de vida de desarrollo seguro | | 0% | M1:RA4(C3) | 50% |
| | Modelos de referencia de arquitectura de seguridad | M2:RA6(C6);M3:RA7(C1) | 50% | M3:RA2(C1,C6) | 50% |
| | Tecnologías relacionadas con la ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10( | 100% | M2:RA2(C3);M3:RA5(C1,C4) | 100% |

| | | | | | |
|---|---|---|---|---|---|
| | | C1,C6,C8);M3:RA2(C3) | | | |
| | Controles y soluciones de ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3) | 100% | M2:RA4(C4);M3:RA10(C2,C5) | 100% |
| | Riesgos de ciberseguridad | M2:RA3(C1),M3:RA5(C2);M6:RA2(C3) | 100% | M2:RA3(C4);M5:RA5(C2,C3) | 100% |
| | amenazas cibernéticas | M1:RA3(C4);M2:RA3(C1);M3:RA5(C2) | 100% | M3:RA8(C1,C5);M4:RA2(C2,C7) | 100% |
| | Tendencias en ciberseguridad | M2:RA7(C1) | 25% | M3:RA2(C8,C10) | 50% |
| | Requisitos, recomendaciones y mejores prácticas de cumplimiento legal, reglamentario y legislativo | M2:RA3(C3,C5);M6:RA5(C3) | 50% | M5:RA1(C2) | 50% |
| | Procedimientos de ciberseguridad heredados | M6:RA1(C1,C3),RA3(C*),RA5(C3,C4,C5,C6,C7,C8) | 100% | M1:RA5(C1,C2) | 100% |
| | Tecnologías de mejora de la privacidad (PET) | M2:RA4(C1,C2);M6:RA4(C3,C4) | 75% | M5:RA5(C3) | 25% |
| | Estándares, metodologías y marcos de privacidad desde el diseño | M6: RA4(C2),RA5(C2, C4, C6, C7, C8) | 75% | M5:RA5(C1,C3) | 25% |
| | Nivel de cumplimiento | | 62% | | 62% |

## 6- **Cybersecurity Auditor** Auditor de ciberseguridad

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Desarrollar la política, los procedimientos, las normas y las directrices de auditoría de la organización. | M1:RA1(Ee);M2:RA2(Ec) | 50% | M1:RA5(Ef,Eg);M5:RA5(Eb,Ee) | 25% |
| | Establecer las metodologías y prácticas utilizadas para la auditoría de sistemas. | M3:RA7(Ec),M5:RA2(Ei),RA4(Eb) | 75% | M2:RA3(Ea,Ec);M5:RA3(Ec,Ef) | 50% |
| | Establecer el entorno objetivo y gestionar las actividades de auditoría | M3:RA7(Ec),M5:RA2(Ei),RA4(Eb) | 75% | M4:RA1(Ee,Eg);M5:RA1(Ef,Eg) | 50% |
| | Definir el alcance de la auditoría, los objetivos y los criterios para auditar | M6:RA2(Ec) | 25% | M2:RA5(Ed,Ee);M5:RA4(Ed,Ef) | 25% |
| | Desarrollar un plan de auditoría que describa los marcos, estándares, metodología, procedimientos y pruebas de auditoría. | | 0% | M1:RA3(Ed,Eh);M3:RA10(Ea,Ec) | 0% |
| | Revisar el objetivo de evaluación, los objetivos de seguridad y los requisitos en función del perfil de riesgo | M2:RA3(Ec,Ee),RA8(Ee);M3:RA5(Eb,Ed),RA6(Eb) | 100% | M1:RA1(Ec,Ee);M2:RA3(Eb,Ej) | 50% |
| | Auditar el cumplimiento de las leyes y regulaciones aplicables relacionadas con la ciberseguridad | M1:RA1(Ee) | 25% | M3:RA3(Ed,Ee);M5:RA5(Ee,Ed) | 25% |
| | Auditar la conformidad con las normas aplicables relacionadas con la ciberseguridad | | 0% | M1:RA5(Ec,Ee);M2:RA5(Ec,Ef) | 0% |
| | Ejecutar el plan de auditoría y recopilar evidencias y mediciones | M1:RA3(Ea,Eb,Ec) | 50% | M3:RA10(Mib,Ed);M4:RA2(Mi,Eg) | 50% |
| | Mantener y proteger la integridad de los registros de auditoría | M2:RA8(Eh) | 25% | M4:RA1(Ec,Ed);M5:RA5(Ef,Eg) | 25% |
| | Desarrollar y comunicar informes de evaluación de la conformidad, aseguramiento, auditoría, certificación y mantenimiento. | | 0% | M2:RA4(Mib,Ed);M4:RA1(Ef,Eg) | 0% |
| | Monitorear las actividades de remediación de riesgos | M1:RA1(Ei) | 25% | M3:RA8(Mib,Ef);M5:RA5(Ed,Ee) | 25% |

| | | | | | |
|---|---|---|---|---|---|
| | Nivel de cumplimiento | | 38% | | 27% |
| **Habilidad(es) clave** | Organizar y trabajar de forma sistemática y determinista basándose en la evidencia. | Cc,Ce | 75% | Cc,Cg | 75% |
| | Seguir y practicar marcos, estándares y metodologías de auditoría. | Cc,Ce | 75% | Ch,Ck | 50% |
| | Aplicar herramientas y técnicas de auditoría | Cb,Cf | 75% | Ca, Cb, Ci | 50% |
| | Analizar procesos de negocio, evaluar y revisar la seguridad del software o hardware, así como los controles técnicos y organizativos. | Cg | 25% | Ca, Ch, Cj | 25% |
| | Descomponer y analizar sistemas para identificar debilidades y controles ineficaces | Cb,Cf | 50% | Ck,Cm | 25% |
| | Comunicar, explicar y adaptar los requisitos legales y reglamentarios y las necesidades del negocio. | Cm | 25% | Cd,Cl | 25% |
| | Recopilar, evaluar, mantener y proteger la información de auditoría | Cb,Cf | 75% | Ca,Cm | 50% |
| | Auditar con integridad, siendo imparcial e independiente | | 0% | Cb,Cj | 0% |
| | Nivel de cumplimiento | | 50% | | 38% |
| **Conocimientos clave** | Controles y soluciones de ciberseguridad | M1:RA2(C2,C3,C4); M2:RA5(C5),RA8(C1),RA10(C1,C6,C8); M3:RA2(C3) | 100% | M2:RA4(C3,C4);M3:RA10(C2,C3,C5) | 100% |
| | Requisitos, recomendaciones y mejores prácticas de cumplimiento legal, reglamentario y legislativo | M2:RA3(C3,C5);M6:RA5(C3) | 75% | M5:RA5(C2,C3) | 50% |
| | Monitoreo, prueba y evaluación de la efectividad de los controles de ciberseguridad | M1:RA2(C2,C4);M2:RA7(C13,C14,C18) | 100% | M3:RA9(C1,C2);M5:RA5(C1,C2) | 75% |
| | Normas, metodologías y marcos de evaluación de la conformidad | M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5) | 100% | M5:RA5(c3) | 75% |
| | Normas, metodologías y marcos de auditoría | M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5) | 100% | M3:RA10(C3,C4);M4:RA6(C5,C6) | 75% |
| | Estándares, metodologías y | M1:RA4(C1);M2:R | 100% | M2:RA3(C4);M | 50% |

| | | | | | |
|---|---|---|---|---|---|
| | marcos de ciberseguridad | A3(C6);M3:RA5(C2, C4),RA6(C4);M6:RA 5(C2,C5) | | 5:RA5(C3) | |
| | Certificación relacionada con auditoría | | 0% | M5:RA5(C3) | 0% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M1:RA2(C1,C2) ;M5:RA5(C3) | 0% |
| | Nivel de cumplimiento | | 72% | | 53% |

## 7- **Cybersecurity Educator** Educador en ciberseguridad

| | Detalle | ÉL | TASA | Antiguo Testamento | TASA |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Desarrollar, actualizar y entregar currículos y material educativo sobre ciberseguridad y protección de datos para capacitación y concientización basados en el contenido, método, herramientas y necesidades de los participantes. | | 0% | M1:RA3(Eh); M5:RA5(Eb,Ee) | 0% |
| | Organizar, diseñar e impartir actividades de concienciación sobre ciberseguridad y protección de datos, seminarios, cursos y formación práctica. | M1:RA1(Ec,Ed,Ee) | 50% | M2:RA4(Ed,Ee);M5:RA5(Ef,Eg) | 25% |
| | Monitorear, evaluar e informar sobre la eficacia de la capacitación | | 0% | M4:RA1(Ee,Ef),M5:RA3(Ef,Eg) | 0% |
| | Evaluar e informar el desempeño del aprendiz | | 0% | M5:RA5(Ef,Eg) | 0% |
| | Encontrar nuevos enfoques para la educación, la formación y la sensibilización | M1:RA1(Ec,Ed,Ee) | 50% | M1:RA5(Ee,Ef);M3:RA8(Ef,Eg) | 25% |
| | Diseñar, desarrollar y entregar simulaciones de ciberseguridad, laboratorios virtuales o entornos de campo cibernético. | | 0% | M2:RA2(Ec.Ed);M4:RA3(Ec,Ef) | 0% |
| | Proporcionar orientación sobre programas de certificación en ciberseguridad para personas | | 0% | M1:RA3(Eh,Ei);M5:RA5(Ee,Ef) | 0% |
| | Mantener y mejorar continuamente la experiencia; fomentar y potenciar la mejora continua de las capacidades de ciberseguridad y el desarrollo de capacidades. | | 0% | M2:RA3(Ej,Ee);M5:RA3(Eg,Ef) | 0% |
| | Nivel de cumplimiento | | 13% | | 6% |
| **Habilidad(es) clave** | Identificar necesidades de concientización, capacitación y educación en ciberseguridad | Ca | 50% | Ca,Cl | 25% |
| | Diseñar, desarrollar e impartir programas de aprendizaje para cubrir las necesidades de ciberseguridad. | Cm | 25% | Ck,Cl | 25% |


Tknika | Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

| | | | | | |
|---|---|---|---|---|---|
| | Desarrollar ejercicios de ciberseguridad que incluyan simulaciones utilizando entornos de alcance cibernético. | | 0% | Cd,Cg | 25% |
| | Proporcionar formación para obtener certificaciones profesionales en ciberseguridad y protección de datos. | | 0% | Ck,Cl | 50% |
| | Utilizar los recursos de formación existentes relacionados con la ciberseguridad | | 0% | Ca,Cl | 0% |
| | Desarrollar programas de evaluación de las actividades de sensibilización, formación y educación. | | 0% | Ck,Cl | 25% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | Cñ | 25% | Cm,Cl | 25% |
| | Identificar y seleccionar enfoques pedagógicos apropiados para el público destinatario. | Cñ | 25% | Ck,Cl | 25% |
| | Motivar y animar a las personas | Cñ | 50% | Cl,Cm | 50% |
| | Nivel de cumplimiento | | 19% | | 28% |
| **Conocimientos clave** | Estándares, metodologías y marcos pedagógicos | | 0% | M5:RA1(C1) | 0% |
| | Desarrollo de programas de concientización, educación y capacitación en ciberseguridad | M1:RA1(C3,C4) | 25% | M1:RA4(C7); M5:RA1(C3) | 25% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M1:RA2(C2); M5:RA5(C3) | 0% |
| | Estándares, metodologías y marcos de educación y capacitación en ciberseguridad | | 0% | M5:RA5(C1,C3) | 0% |
| | Leyes, regulaciones y legislaciones relacionadas con la ciberseguridad | M6:RA3(C1,C2,C3),RA4(C*),RA5(C8) | 100% | M5:RA5(C3) | 100% |
| | Recomendaciones y mejores prácticas de ciberseguridad | M2:RA3(C5,C7);M6:RA5(C3) | 50% | M2:RA5(C3); M3:RA7(C2,C5) | 50% |
| | Estándares, metodologías y marcos de ciberseguridad | M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5) | 100% | M5:RA5(C3) | 75% |
| | Controles y soluciones de ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3) | 100% | M2:RA4(C3,C4);M3:RA10(C3,C5) | 75% |
| | Nivel de cumplimiento | | 47% | | 41% |

**8- Cybersecurity Implementer** Implementador de ciberseguridad

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Desarrollar, implementar, mantener, actualizar y probar productos de ciberseguridad | M1:RA2(Eb,Ec,Ed),RA4(Ed);M2:RA1(Ec,Ed,),RA2(Ea),RA4(Ef),RA5(Ee),RA6(Ef),RA8(Ef,Eh),RA9(Ed,Ee),RA10(Ef,Eh);M3:RA6(Eh,Ej),Ra 7(Ec,Ed);M4:RA 2(*),RA3(Ea,Eb),Ra4(Cc),RA5(Eb,Ed);M5:RA1(Eh,Ej),RA2(Ea,Ed),RA3(Ec,Ee),RA4(E *),RA5(Ec,Ed,Ee,Ef),RA6(Ea,Ec,Ed) | 100% | M1:RA3(Ec,Ef); M5:RA5(Ef,Eg) | 100% |
| | Brindar soporte relacionado con la ciberseguridad a usuarios y clientes | | 0% | M2:RA4(Ec,Ed); M5:RA5(Ee,Ef) | 50% |
| | Integrar soluciones de ciberseguridad y garantizar su correcto funcionamiento | | 0% | M1:RA3Ec,Ei); M3:RA4(Eg,Eh) | 50% |
| | Configurar sistemas, servicios y productos de forma segura | M2:RA4(Ea,Eb,Ec,Ed,Ee),Ra5(Ee),RA6(Ef),RA7(Ea,Eb,Ec,Ed,Ee,Eh,Ei),Ra8(Ec,Eg,Eh),Ra9(Eb,Ed),RA10(Ed);M3:RA6(Ei),RA8(Ec);M5:RA2(Ea) | 100% | M2:RA6(Ed,Ee);M5:RA4(Ec,Ef) | 100% |
| | Mantener y actualizar la seguridad de los sistemas, servicios y productos. | M1:RA2(Eb,Ec,Ed),RA4(Ed);M2:RA1(Ec,Ed,),RA2(Ea),RA4(Ef),RA5(Ee),RA6(Ef),RA8(Ef,Eh),RA9(E | 100% | M1:RA4(Mib,Ef);M5:RA3(Mie, Eg) | 100% |

| | | | | | |
|---|---|---|---|---|---|
| | | d,Ee),RA10(Ef,Eh);M3:RA6(Eh,Ej),Ra 7(Ec,Ed);M4:RA 2(*),RA3(Ea,Eb),Ra4(Cc),RA5(Eb,Ed);M5:RA1(Eh,Ej),RA2(Ea,Ed),RA3(Ec,Ee),RA4(E*),RA5(Ec,Ed,Ee,Ef),RA6(Ea,Ec,Ed) | | | |
| | Implementar procedimientos y controles de ciberseguridad | M1:RA4(Ea),RA 5(Ea);M3:RA8(Ef);M6:RA1(Ec),RA5(Ee,Ef) | 100% | M2:RA3(Ef,Eh); M5:RA1(Eg,Eg) | 100% |
| | Monitorear y asegurar el desempeño de los controles de ciberseguridad implementados | M1:RA2(Mib,Ec,Ed) | 25% | M3:RA7(Ed,Ee);M5:RA3(Ef,Eg) | 50% |
| | Documentar e informar sobre la seguridad de los sistemas, servicios y productos | M1:RA2(Ee),RA 4(Ee);M3:RA8(Ef);M4:RA1(Ed),RA5(Ee),RA6(Ec) | 100% | M2:RA4(Mib,Ed);M4:RA1(Ed,Ef) | 100% |
| | Trabajar en estrecha colaboración con el personal de TI/OT en acciones relacionadas con la ciberseguridad | M2:RA10(E*) | 75% | M1:RA1(Eb,Ed);M2:RA1(Ef,Eg) | 75% |
| | Implementar, aplicar y administrar parches a los productos para abordar vulnerabilidades técnicas | M2:RA4(Eb,Ec,Ed,Ee),RA10Eg,Eh);M3:RA6(Ec);M5:RA2(Ee),RA3(Ee),RA5(Ed,Ee,Ef), | 100% | M2:RA6(Ea,Ed); M3:RA8(Ea,Eb) | 100% |
| | Nivel de cumplimiento | | 70% | | 83% |
| **Habilidad(es) clave** | Comunicar, presentar e informar a las partes interesadas pertinentes | Cñ | 25% | Cm, Ck | 25% |
| | Integrar soluciones de ciberseguridad a la infraestructura de la organización | Cd, Ce, Cg, Ch | 100% | Cj,Cb | 100% |
| | Configurar soluciones de acuerdo con la política de seguridad de la organización | Cd | 25% | Cf. Ch. | 100% |
| | Evaluar la seguridad y el rendimiento de las soluciones | Cf,Ci | 50% | Cc, Cd | 50% |
| | Desarrollar código, scripts y | Cg | 75% | Cl,Ce | 75% |

| | | | | | |
|---|---|---|---|---|---|
| | programas | | | | |
| | Identificar y resolver problemas relacionados con la ciberseguridad | Cf,Ci | 100% | Cm,Cg | 100% |
| | Colaborar con otros miembros del equipo y colegas. | Cñ | 75% | Cn,Cl | 75% |
| | Nivel de cumplimiento | | 64% | | 75% |
| **Conocimientos clave** | Ciclo de vida de desarrollo seguro | M3:RA8(C*) | 50% | M1:RA1(C1,C5),RA4(C3) | 50% |
| | Programación de computadoras | M3:RA1(C*),RA2(C*),RA3(C*), M7:RA4(C*) | 100% | M2:RA2(C2,C6) | 75% |
| | Seguridad de los sistemas operativos | M7:RA3(C1,C2) | 25% | M2:RA6(C1,C4);M3:RA11(C2,C3) | 25% |
| | Seguridad de redes informáticas | M2:RA3(C5,C6), RA6(C1) | 50% | M3:RA5(C1,C2,C4),RA6(C1,C3) | 75% |
| | Controles y soluciones de ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5), RA8(C1),RA10(C1,C6,C8);M3:RA2(C3) | 100% | M2:RA4(C4),M3:RA10(C2,C3,C5) | 100% |
| | Prácticas de seguridad ofensivas y defensivas | M5:RA1(C4),RA2(C*),RA3(C*) | 100% | M3:RA8(C3,C5);M4:RA6(C2,C6) | 50% |
| | Recomendaciones y mejores prácticas de codificación segura | M3: RA5(C1,C2,C3,C4), RA6(C1,C3,C4,C5,C6,C7,C8,C9,C10,C11), RA7(C1,C2,C3,C4,C5,C6), RA8(C1,C2,C3,C4,C5,C6,C7,C8,C9) | 100% | M2:RA2(C2,C3) | 75% |
| | Recomendaciones y mejores prácticas de ciberseguridad | M2:RA3(C5,C7); M6:RA5(C3); | 75% | M5:RA5(C2,C3) | 75% |
| | Estándares, metodologías y marcos de prueba | M2:RA3(C6);M3:RA6(C4);M6:RA5(C2,C5) | 100% | M3:RA9(C1,C2) | 100% |
| | Procedimientos de prueba | M5:RA1(C2,C3) | 25% | M3:RA5(C1,C4) | 25% |
| | Tecnologías relacionadas con la ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5), RA8(C1),RA10(C | 100% | M2:RA2(C2);M3:RA5(C1,C4) | 100% |

| | | | | | |
|---|---|---|---|---|---|
| | | 1,C6,C8);M3:RA2(C3) | | | |
| | Nivel de cumplimiento | | 75% | | 68% |

## 9- **Cybersecurity Researcher** Investigador en ciberseguridad

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea (s) principal(es)** | Analizar y evaluar tecnologías, soluciones, desarrollos y procesos de ciberseguridad. | M1:RA2(Eb,Ec,Ed),RA3(Eb,Ec,Ed);M2:RA10(Ee,Eg);M5:RA6(Eb,Ec) | 100% | M2:RA3(Ea,Ec); M5:RA5(Ed,Ef) | 75% |
| | Realizar trabajos de investigación, innovación y desarrollo en temas relacionados con la ciberseguridad | M1:RA2(Ed),RA3(Ed); M5:RA5(Ee,Ef) | 100% | M1:RA3(Ec,Eh); M4:RA3(Ec,Ef) | 75% |
| | Manifestar y generar ideas de investigación e innovación | | 0% | M5:RA5(Ee,Eg) | 25% |
| | Avanzar en el estado actual del arte en temas relacionados con la ciberseguridad | | 0% | M1:RA1(Ed,Ee); M4:RA3(Ed,Eg) | 25% |
| | Contribuir al desarrollo de soluciones innovadoras relacionadas con la ciberseguridad. | M3:RA4(Ee),RA5(Eb,Ec),RA6(E*),RA7(Ec,Ed) | 100% | M3:RA8(Ef,Eg); M5:RA3(Ef,Eg) | 75% |
| | Realizar experimentos y desarrollar pruebas de concepto, pilotos y prototipos para soluciones de ciberseguridad. | M5:RA2(E*),RA3(E*),RA5(E*) | 100% | M2:RA3(Ej,Eh); M4:RA2(Ee,Eg) | 75% |
| | Seleccionar y aplicar marcos, métodos, estándares, herramientas y protocolos, incluyendo la creación y prueba de una prueba de concepto para respaldar proyectos. | M5:RA2(E*),RA3(E*),RA5(E*) | 100% | M1:RA3(Ed,Ei); M3:RA10(Ea,Ed) | 100% |
| | Contribuye a ideas, servicios y | | 0% | M1:RA5 | 0% |

| | | | | | |
|---|---|---|---|---|---|
| | soluciones de negocio de ciberseguridad de vanguardia. | | | (Ef,Eg); M5:RA5 (Eg,Eh) | |
| | Contribuir al desarrollo de capacidades relacionadas con la ciberseguridad, incluyendo la concientización, la capacitación teórica, la capacitación práctica, las pruebas, la tutoría, la supervisión y el intercambio. | M1:RA1(Ec,Ed,Ee);M5: RA2(E*),RA3(E*),RA5(E *)7 | 100% | M1:RA5 (Ef,Eg); M5:RA5 (Eg,Eh) | 100% |
| | Identificar logros intersectoriales en ciberseguridad y aplicarlos en un contexto diferente o proponer enfoques y soluciones innovadores | | 0% | M1:RA5 (Ej.,Ef); M5:RA5 (Ej.,Ef) | 0% |
| | Liderar o participar en los procesos y proyectos de innovación, incluyendo la gestión de proyectos y la presupuestación. | | 0% | M2:RA1 (Ef,Eg); M3:RA2 (Ef,Eg) | 0% |
| | Publicar y presentar trabajos científicos y resultados de investigación y desarrollo | M1:RA5(Eb,Ec,Ed,Ee), M4:RA1(Ef,Eg),RA3(Ed) ,RA4(Ef),RA5(Ei) | 100% | M1:RA3 (Ed,Eh); M5:RA5 (Ee,Ef) | 75% |
| | Nivel de cumplimiento | | 58% | | 52% |
| **Habilidad(es) clave** | Generar nuevas ideas y transferir la teoría a la práctica. | Cn | 25% | Ca,Cl | 75% |
| | Descomponer y analizar sistemas para identificar debilidades y controles ineficaces | Cb, Cf, Ci | 100% | Cb,Ch | 100% |
| | Descomponer y analizar sistemas para desarrollar requisitos de seguridad y privacidad e identificar soluciones efectivas | Ce,Cf | 75% | Cc, Cd, Cf | 75% |
| | Monitorear nuevos avances en tecnologías relacionadas con la ciberseguridad | Cg, Ck | 75% | Ce,Cl | 75% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | Cñ | 25% | Ck,Cm | 25% |
| | Identificar y resolver problemas relacionados con la ciberseguridad | Cf,Ci | 75% | Cm,Cg | 75% |
| | Colaborar con otros miembros | Cñ | 75% | Cn,Cm | 75% |

| | | | | | |
|---|---|---|---|---|---|
| | del equipo y colegas. | | | | |
| | Nivel de cumplimiento | | 64% | | 71% |
| **Conocimientos clave** | Investigación, desarrollo e innovación (I+D+i) relacionados con la ciberseguridad | M6:RA1(Cd) | 25% | M1:RA1 (C1,C4); M4:RA2 (C7,C9) | 25% |
| | Estándares, metodologías y marcos de ciberseguridad | M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5) | 100% | M2.RA3(C4);M5:RA5(C3) | 100% |
| | Requisitos legales, reglamentarios y legislativos sobre la liberación o el uso de tecnologías relacionadas con la ciberseguridad | M4:RA4(C2);M6:RA4(C*),RA5(C3,C6,C7,C8) | 100% | M5:RA5 (C2,C3) | 75% |
| | Aspecto multidisciplinario de la ciberseguridad | | 0% | M1:RA1 (C2,C5); M5:RA1 (C1,C3) | 0% |
| | Procedimientos de divulgación responsable de información | M1:RA3(C5) | 25% | M4:RA6 (C4,C5) | 25% |
| | Nivel de cumplimiento | | 50% | | 45% |

**10-Cybersecurity Risk Manager** Gerente de riesgos de ciberseguridad

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea (s) principal(es)** | Desarrollar una estrategia de gestión de riesgos de ciberseguridad para una organización | M2:RA3(Ec,Ee), M3:RA5(Eb);M 6:RA4(Ee) | 100% | M1:RA1(Ed,Ee); M5:RA5(Ea,Ec) | 100% |
| | Gestionar un inventario de los activos de la organización | M5:RA3(Mib),R A5(Mib) | 50% | M1:RA1(Mib,Ec );M2:RA3(Mib,E c) | 100% |
| | Identificar y evaluar las amenazas y vulnerabilidades relacionadas con la ciberseguridad de los sistemas TIC | M1:RA2(Eb,Ec, Ed);M2:RA3(Ea) ,RA7(Ef);M3:RA 5(Ea,Eb) | 100% | M2:RA3(Ec,Ed); M3:RA8Ea,Eb) | 100% |
| | Identificación del panorama de amenazas, incluidos los perfiles de los atacantes y la estimación del potencial de los ataques. | M1:RA2(Mib,Ec ,Ed,Ee) | 50% | M4:RA2(Ef,Eg); M5:RA5(Ee,Eg) | 75% |
| | Evaluar los riesgos de ciberseguridad y proponer las opciones de tratamiento de riesgos más adecuadas, incluidos los controles de seguridad y la mitigación y prevención de riesgos que mejor aborden la estrategia de la organización. | M5:RA2(Eg),RA 3(Ef),RA5(Eg) | 75% | M1:RA3(Ed,Eh); M5:RA5(Ed,Ef) | 75% |
| | Monitorear la eficacia de los controles de ciberseguridad y los niveles de riesgo | M1:RA2(Eb,Ed); M2:RA7(Eh);M 3·:RA7(Ed);M5: RA1(Ei) | 100% | M3:RA7(Ed,Ee); M5:RA3(Ef,Eg) | 100% |
| | Asegúrese de que todos los riesgos de ciberseguridad se mantengan en un nivel aceptable para los activos de la organización. | M2:RA3(Ec,Ee) | 25% | M5:RA5(Ee,Ef) | 100% |
| | Desarrollar, mantener, informar y comunicar pautas completas del ciclo de gestión de riesgos y garantizar el cumplimiento de las regulaciones y estándares. | M2:RA3(Ec,Ee), M3:RA5(Eb);M 6:RA4(Ee) | 100% | M1:RA3(Ei,Eh); M4:RA1(Ef,Eg) | 100% |
| | Nivel de cumplimiento | | 75% | | 94% |
| **Habilidad(es) clave** | Implementar marcos, metodologías y herramientas de gestión de riesgos de ciberseguridad. directrices y garantizar el | Ce, Cf, Ci | 100% | Ca, Cb, Cj, Cn | 100% |

| | | | | | |
|---|---|---|---|---|---|
| | cumplimiento de las regulaciones y normas | | | | |
| | Analizar y consolidar las prácticas de gestión de calidad y riesgos de la organización. | Ce, Cf, Ci, Cp | 100% | Cg,Cñ | 100% |
| | Permitir que los propietarios de activos comerciales, ejecutivos y otras partes interesadas tomen decisiones basadas en riesgos para gestionarlos y mitigarlos. | Ce, Cf, Ci | 100% | Cm,Cl | 100% |
| | Construir un entorno consciente de los riesgos de ciberseguridad | Ce, Cf, Ci | 100% | Ce,Cc | 100% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | Cñ | 75% | Ck,Cm | 25% |
| | Proponer y gestionar opciones de reparto de riesgos | Ce, Cf, Ci | 75% | Cd,Ch | 100% |
| | Nivel de cumplimiento | | 92% | | 88% |
| **Conocimientos clave** | Normas, metodologías y marcos de gestión de riesgos | M2:RA3(C1); M3:RA5(C2);M6:RA2(C3) | 25% | M2:RA3(C3);M5:RA5(C1) | 50% |
| | Herramientas de gestión de riesgos | M6:RA2(C3) | 25% | M2:RA3(C7);M3:RA3(C2) | 50% |
| | Recomendaciones y mejores prácticas de gestión de riesgos | M2:RA3(C1);M3:RA5(C2),M6:RA2(C3) | 100% | M5:RA5(C2) | 100% |
| | amenazas cibernéticas | M1:RA3(C4);M2:RA3(C1);M3:RA5(C2) | 100% | M2:RA3(C2) | 100% |
| | Vulnerabilidades de los sistemas informáticos | M2:RA10(C10); M3:RA6(C2,C6);M5:RA3(C6,C9),RA5(C5,C6,C7) | 100% | M3:RA8(C1) | 100% |
| | Controles y soluciones de ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3) | 100% | M2:RA4(C5,C6) | 100% |
| | Riesgos de ciberseguridad | M2:RA3(C1); M3:RA5(C2);M6:RA2(C3); | 25% | M1:RA2(C3);M5:RA5(C3) | 75% |
| | Monitoreo, prueba y evaluación de la efectividad de los controles de ciberseguridad | M1:RA2(C2,C4);M2:RA7(C13,C14,C18) | 75% | M1:RA4(C5);M3:RA9(C2) | 75% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M5:RA5(C3) | 0% |

| | | | | | |
|---|---|---|---|---|---|
| | Tecnologías relacionadas con la ciberseguridad | M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3) | 100% | M1:RA3(C4);M2:RA1(C3) | 100% |
| | Nivel de cumplimiento | | 65% | | 75% |

**11-Digital Forensics Investigator** Investigador forense digital

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Desarrollar políticas, planes y procedimientos de investigación forense digital | M4:RA1(Ea,Eb,Ec,Ed,Ee),RA2(E*),RA3(Ea,Eb),RA4(Ea,Eb,Ec),RA5(Ea,Eb,Ec,Ed,Ee,Ef,Eg) | 100% | M4:RA1(Ea,Ed);M5:RA5(Ec,Ef) | 75 |
| | Identificar, recuperar, extraer, documentar y analizar evidencia digital | M4:RA1(Ea,Eb,Ee),RA3(Ea),RA5(Ea,Eb,Ec,Ed,Ef) | 75% | M3:RA9(Ea,Ed);M4:RA2(Eb,Ec) | 75 |
| | Preservar y proteger la evidencia digital y ponerla a disposición de las partes interesadas autorizadas | M4:RA1(Ea,Eb,Ee),RA3(Ea),RA5(Ea,Eb,Ec,Ed,Ef) | 75% | M4:RA1(Ec,Ee);M5:RA1(Ef,Eg) | 25 |
| | Inspeccionar entornos en busca de evidencia de acciones no autorizadas e ilegales. | M4:RA1(Ea,Eb,Ee),RA3(Ea),RA5(Ea,Eb,Ec,Ed,Ef) | 75% | M3:RA8(Mib,Ee);M4:RA3(Ea,Ec) | 50 |
| | Documentar, informar y presentar de forma sistemática y determinista los hallazgos y resultados del análisis forense digital. | M4:RA1(Ef,Eg),RA3(Ec,Ed),RA4(Ef),RA5(Eh,Ei),RA6(E*) | 100% | M2:RA4(Mib,Ed);M4:RA1(Ef,Eg) | 75 |
| | Seleccionar y personalizar las técnicas de pruebas, análisis e informes forenses de los actores | M4:RA1(Ea,Eb,Ec,Ed,Ee),RA2(E*),RA3(Ea,Eb),RA4(Ea,Eb,Ec),RA5(Ea,Eb,Ec,Ed,Ee,Ef,Eg) | 100% | M1:RA3(Eh,Ei):M4:RA2(Ed,Ef) | 50 |
| | Nivel de cumplimiento | | 88% | | 58,33 |
| **Habilidades clave** | Trabajar de forma ética e independiente, sin influencias ni prejuicios internos ni externos. actores | Ch,Co | 75% | Cl,Cn | 25 |
| | Recopilar información | Ch | 75% | Ci, Ck | 75 |

| | | | | | |
|---|---|---|---|---|---|
| | preservando su integridad | | | | |
| | Identificar, analizar y correlacionar eventos de ciberseguridad | Ch | 75% | Ca, Cb, Ch | 75 |
| | Explicar y presentar evidencia digital de una manera sencilla, directa y fácil de entender. | Cm | 50% | Cc, Ck | 100 |
| | Elaborar y comunicar informes de investigación detallados y razonados. | Cm | 75% | Cc,Cj | 75 |
| | Nivel de cumplimiento | | 70% | | 70 |
| **Conocimientos clave** | Recomendaciones y mejores prácticas de análisis forense digital | M4:RA1(C2,C4),RA4(C3) | 75% | M4:RA1(C2),RA4(C6) | 50 |
| | Estándares, metodologías y marcos de investigación forense digital | M4:RA1(C4),RA3(C1,C2),RA4(C3) | 100% | M4:RA1(C3) | 50 |
| | Procedimientos de análisis forense digital | M4:RA1(C7,C8,C10),RA2(C4,C5,C6,C7),RA3(C3),RA5(C3) | 100% | M4:RA1(C6);M4:RA1(C3) | 75 |
| | Procedimientos de prueba | M5:RA1(C2,C3) | 50% | M4:RA2(C10) | 50 |
| | Procedimientos, normas, metodologías y marcos de investigación criminal | | 0% | M4:RA2(C3),RA5(C4) | 25 |
| | Leyes, regulaciones y legislaciones relacionadas con la ciberseguridad | M6:RA3(C1,C2,C3),RA4(C*),RA5(C8) | 100% | M5:RA5(C2,C3) | 0 |
| | Herramientas de análisis de malware | M4:RA2(C3) | 50% | M4:RA1(C9,C10),RA6(C2,C6) | 75 |
| | amenazas cibernéticas | M1:RA3(C4);M2:RA3(C1);M3:RA5(C2) | 100% | M4:RA3(C6) | 50 |
| | Vulnerabilidades de los sistemas informáticos | M2:RA10(C10);M3:RA6(C2,C6);M5:RA3(C6,C9),RA5(C5,C6,C7) | 100% | M3:RA8(C1,C5);M4:RA5(C2,C3) | 75 |
| | Procedimientos de ataque a la ciberseguridad | M5: RA1(C4), RA2(C4, C5), RA3(C5, C6, C7, C8, C9), RA4(C2), RA5(C3, C6) | 100% | M3:RA8(C5,C6) | 75 |
| | Seguridad de los sistemas operativos | M7:RA3(C1,C2) | 75% | M2:RA6(C3,C4);M3:RA11(C3,C4) | 75 |

| | | | | | |
|---|---|---|---|---|---|
| | Seguridad de redes informáticas | M2:RA1(C*),RA3(C*),RA6(C*); M7:RA1(C1,C2,C3) | 100% | M3:RA2(C10),RA10(C2) | 75 |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | M5:RA5(C3) | 0 |
| | Nivel de cumplimiento | | 73% | | 51,92 |

## 12- **Penetration Tester** Probador de penetración

| | Detalle | ÉL | TASA DE TI | Antiguo Testamento | TASA DE OT |
|---|---|---|---|---|---|
| **Tarea(s) principal(es)** | Identificar, analizar y evaluar las vulnerabilidades técnicas y organizativas de ciberseguridad | M1:RA2(Eb,Ec,Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb) | 100% | M2:RA3(Ec,Ee);M3:RA8(Ea,Eb) | 100% |
| | Identificar vectores de ataque, descubrir y demostrar la explotación de vulnerabilidades técnicas de ciberseguridad. | M2:RA10(Eh);M3:RA5(E*);M5:RA3(Ee),RA5(Ee,Ef) | 100% | M3:RA8(Ec,Eg);M4:RA2(Eb,Ed) | 100% |
| | Sistemas de prueba y cumplimiento de operaciones con estándares regulatorios | M2:RA3(Ef),M3:RA5(Ea,Eb);M6:RA5(Ef) | 100% | M1:RA3(Eh,Ei);M5:RA5(Ee,Ef) | 100% |
| | Seleccionar y desarrollar técnicas de prueba de penetración adecuadas | M5:RA1(Ee,Ef,Eg,Eh),RA2(Ea,Ec,Ed,Ee,Ef),RA3(Ea,Eb,Ec,Ed,Ee),RA4(E*),RA5(Ea,Eb,Ec,Ed,Ee,Ef),RA6(E*) | 100% | M3:RA8(Ed,Ef);M4:RA3(Ee,Eg) | 100% |
| | Organizar planes de prueba y procedimientos para pruebas de penetración | M5:RA1(Ec),RA2(Ef),RA3(Eb),R5(Ea) | 75% | M1:RA3(Ed,Eh);M5:RA5(Ec,Ef) | 50% |
| | Establecer procedimientos para el análisis y la elaboración de informes de los resultados de las pruebas de penetración. | M5:RA2(Eg),RA3(Ef),RA5(Eg) | 75% | M2:RA4(Ed,Ef);M4:RA1(Ef,Eg) | 75% |
| | Documentar e informar los resultados de las pruebas de penetración a las partes interesadas | M1:RA3(Ee),RA4(Ee);M5:RA2(Eg),RA3(Ef),RA5(Eg) | 100% | M2:RA4(Mib,Ed);M4:RA2(Mie,Ef) | 100% |
| | Implementar herramientas de pruebas de penetración y programas de prueba | | 0% | M3:RA8(Ee,Ef);M4:RA2(Eb,Ed) | 0% |
| | Nivel de cumplimiento | | 81% | | 78% |
| **Habilidad(es) clave** | Desarrollar códigos, scripts y programas | Cg | 75% | Ch, Ck, Cl | 75% |
| | Realizar ingeniería social | Cb | 75% | Ca,Cd | 75% |
| | Identificar y explotar vulnerabilidades | Cc, Cf, Ci | 100% | Ch,Ci | 100% |
| | Realizar piratería ética | Cf | 100% | Cg,Cj | 75% |
| | Piensa de forma creativa y fuera de | Cn,Cñ | 75% | Cm | 75% |

| | | | | | |
|---|---|---|---|---|---|
| | la caja | | | | |
| | Identificar y resolver problemas relacionados con la ciberseguridad | Cf,Ci | 75% | Cm | 75% |
| | Comunicar, presentar e informar a las partes interesadas pertinentes | Cñ | 25% | Cc, Ck | 25% |
| | Utilice herramientas de pruebas de penetración de forma eficaz | Cb,Cf | 100% | Cb,Cj | 75% |
| | Realizar análisis técnicos e informes | Cf | 75% | Cc,Cl | 75% |
| | Descomponer y analizar sistemas para identificar debilidades y controles ineficaces | Cb, Cf, Ci | 100% | Ce,Cf | 75% |
| | Revisar códigos para evaluar su seguridad | Cg | 50% | Cb,Ck | 50% |
| | Nivel de cumplimiento | | 77% | | 70% |
| **Conocimientos clave** | Procedimientos de ataque a la ciberseguridad | M5: RA1(C4), RA2(C4, C5), RA3(C5, C6, C7, C8, C9), RA4(C2), RA5(C3, C6) | 100% | M3:RA8(C5); M4:RA6(C1,C2) | 100% |
| | Dispositivos de tecnología de la información (TI) y tecnología operativa (OT) | M2:RA10(C*) | 75% | M2:RA1(C1,C2,C3) | 75% |
| | Procedimientos de seguridad ofensivos y defensivos | M5:RA1(C4),RA2(C*),RA3(C*) | 100% | M3:RA8(C5,C6);M5:RA1(C3) | 75% |
| | Seguridad de los sistemas operativos | M7:RA3(C1,C2) | 75% | M2:RA6(C3,C4);M3:RA11(C3,C4) | 75% |
| | Seguridad de redes informáticas | M2:RA1(C*),RA3(C*),RA6(C*);M7:RA1(C1,C2,C3) | 100% | M3:RA10(C2,C4) | 75% |
| | Procedimientos de pruebas de penetración | M5:RA1(C3,C4), RA2(C5),RA3(C*),RA4(C2,C3),RA5(C3,C5,C6),RA6(C4) | 100% | M3:RA8(C4); M4:RA2(C10) | 75% |
| | Estándares, metodologías y marcos de pruebas de penetración | M5:RA1(C3,C4), RA2(C5),RA3(C*),RA4(C2,C3),RA5(C3,C5,C6),RA6(C4) | 100% | M4:RA2(C9,C10) | 75% |
| | Herramientas de pruebas de penetración | M2:RA10(C15); M3:RA6(C10),RA8(C8);M5:RA1(C | 100% | M3:RA6(C3) | 75% |

| | | | | | |
|---|---|---|---|---|---|
| | | 7,C8),RA3(C6),RA5(C6),RA6(C*) | | | |
| | Programación de computadoras | M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*) | 100% | M3:RA5(C2,C3),RA8(C1,C2) | 100% |
| | Vulnerabilidades de los sistemas informáticos | M2:RA10(C10); M3:RA6(C2,C6); M5:RA3(C6,C9), RA5(C5,C6,C7) | 100% | M5:RA5(C2,C3) | 100% |
| | Recomendaciones y mejores prácticas de ciberseguridad | M2:RA3(C5);M6:RA5(C3) | 100% | M5:RA5(C3) | 100% |
| | Certificaciones relacionadas con la ciberseguridad | | 0% | | 0% |
| | Nivel de cumplimiento | | 88% | | 77% |

Tknika

Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre