

## 6.2. ITINERARIOS

Se establecen tres itinerarios de aprendizaje:

N.º	Perfil	Horas Bloq. 1	Horas Bloq. 2	Horas Bloq. 3	Total horas	Modalidad	plazas presencia	plazas online	Inicio	Fin	Certificación	Mínimo alumnos modalidad presencial	Mínimo alumnos online
1	Sin conocimientos en redes	225	175	300	700	Presencial/online	25	50-75	Octubre	Junio	<ul style="list-style-type: none"> <li>• CCNA 200/301 Associate</li> <li>• CiberOps 200/201</li> <li>• Fortinet básico</li> </ul>	20	0
2	Conocimientos en redes	30	150	275	455	Solo online	0	40-50	Octubre	Abril	<ul style="list-style-type: none"> <li>• CCNA 200/301 Associate</li> <li>• CiberOps 200/201</li> <li>• Fortinet básico</li> </ul>	0	20
3	Altos conocimientos(Con CCNA previo)	0	0	250	250	Solo online	0	40-50	Mayo	Junio	<ul style="list-style-type: none"> <li>• CiberOps 200/201 básico</li> <li>• FCP (NSE4+Fortianalyzer)</li> </ul>	0	20

Notas:

- **El horario de impartición es tardes ( de 16.30 a 21.30 de lunes a viernes), a fin de lograr la conciliación con el horario de trabajo de los miembros del ET.**
- En el itinerario 1, el alumno que empieza en una modalidad no se puede pasar a otra una vez arrancado el curso.
- En caso de que no se consiga un grupo mínimo de participantes, Tajamar se reserva el derecho de no iniciar la acción formativa.
- Las certificaciones ofrecidas puede sufrir variaciones en el tiempo, siempre que suponga una mejora o actualización de las existentes.
- Se aumentan las plazas hasta 200 (25 presenciales y un máximo de 175 online).

## - BLOQUE-1 INTRODUCCIÓN

### OBJETIVOS

- Ser capaz de comprender y aplicar conceptos básicos de redes y en la explicación de tecnologías fundamentales en seguridad.

### CONTENIDOS

1. Modelo OSI y TCP/IP
2. Concepto de redes conmutadas
3. Vlan
4. Acl
5. Enrutamiento
  - a. Estático
  - b. Dinámico (protocolos de enrutamiento)
6. Vpn
7. Firewall por zonas

## - BLOQUE-2 CONCEPTOS GENERALES DE CIBERSEGURIDAD

### OBJETIVOS

- Ser capaz de comprender y aplicar las especialidades presentes en el sector y que servirá para que el alumno tome consciencia y aptitud de las disciplinas más demandadas en el sector.

### CONTENIDOS

1. Concepto y objetivos de un SOC
2. Concepto y objetivos de la auditoría de seguridad informática
3. Concepto y objetivos del análisis forense
4. Concepto y objetivos de los NGFW
5. Normativa
  - a. LOPD
  - b. ISO 27002

- **BLOQUE-3 CERTIFICACIONES DE UN TECNICO EN CIBERSEGURIDAD**

**OBJETIVOS**

- Ser capaz de profundizar en cada una de las materias y especialidades propuestas en el bloque-2 para que puedan prepararse y superar con éxito algunas de las certificaciones más demandadas en el sector.

**CONTENIDOS**

**Certificaciones oficiales**

- o CCNA 200/301 Associate
- o CiberOps 200/201
- o Fortinet (Nivel 1, Nivel 2 y Nivel 3) básico
- o Fortinet. FCP (NSE4+Fortianalyzer)

- **BLOQUE-4 EXÁMENES PARA LAS CERTIFICACIONES OFICIALES**