



INFORME VALORACIÓN CRITERIOS
SOMETIDOS A LA APLICACIÓN DE
JUICIOS DE VALOR PARA LA
ELABORACIÓN DE UN "SERVICIO DE
EASM & BRAND PROTECTION Y
PROTECCIÓN DE IDENTIDAD
DIGITAL PARA EMPRESAS EN
NAVARRA" – FINANCIADO CON
FONDOS DE LA UNIÓN EUROPEA –
NEXT GENERATION EU

JULIO DE 2025



Navarra de Servicios y Tecnologías, S.A.

| C/ Orcoyen, s/n. 31011 Pamplona - Navarra |

| info@nasertic.es

| www.nasertic.es

| Tel: 848 420 500

| Fax: 848 426 751

Índice

1 OBJETO	2
2 CONCURRENCIA	2
3 VALORACIÓN DE LOS CRITERIOS SOMETIDOS A LA APLICACIÓN DE JUICIOS DE VALOR	2
3.1 THALES S21SEC	3
3.1.1 Herramienta de EASM & Brand Protection y Protección de Identidad Digital (hasta 30 puntos)....	3
3.1.2 Servicio de formación, soporte, supervisión y reporting, indicando la metodología, planificación, modelo de gobierno y equipo de trabajo (hasta 20 puntos).....	5
3.2 SEIN TIC.....	8
3.2.1 Herramienta de EASM & Brand Protection y Protección de Identidad Digital (hasta 30 puntos)....	8
3.2.2 Servicio de formación, soporte, supervisión y reporting, indicando la metodología, planificación, modelo de gobierno y equipo de trabajo (hasta 20 puntos).....	10
4 RESUMEN DE PUNTUACIÓN DE CRITERIOS SOMETIDOS A LA APLICACIÓN DE JUICIOS DE VALOR	13

1 OBJETO

Con objeto de contratar la elaboración de un “Servicio de EASM & Brand Protection y Protección de Identidad Digital para empresas en Navarra”, NASERTIC ha promovido una licitación mediante procedimiento abierto.

En el presente documento, se recoge la valoración de las ofertas presentadas, de acuerdo con los criterios sometidos a la aplicación de juicios de valor definidos en el Pliego de Cláusulas Administrativas.

2 CONCURRENCIA

Habiendo finalizado el plazo de presentación de ofertas, se ha recibido documentación de las siguientes empresas:

- Thales S21sec
- SEIN TIC

3 VALORACIÓN DE LOS CRITERIOS SOMETIDOS A LA APLICACIÓN DE JUICIOS DE VALOR

El pliego de cláusulas administrativas incluye una relación de los elementos a valorar en las diferentes ofertas presentadas, así como la puntuación máxima asignada a cada uno de ellos.

Se han revisado todas las propuestas recibidas y se han puntuado de acuerdo a dichos criterios, hasta un valor máximo de 50 puntos.

A continuación, se detalla la valoración técnica obtenida por cada una de las empresas en cada uno de los criterios especificados en el pliego.

3.1 THALES S21SEC

3.1.1 Herramienta de EASM & Brand Protection y Protección de Identidad Digital (hasta 30 puntos)

HERRAMIENTA DE EASM & Brand Protection y Protección de Identidad Digital

Thales S21sec (22 puntos)

<p>Alcance cubierto por el tipo de licencia (10 puntos)</p>	<p>La propuesta presenta una solución con funcionalidades que incluyen monitorización continua en tiempo real y un modelo de licenciamiento por dominio. La cobertura contempla subdominios e IPs ilimitados por licencia, gestión personalizada de activos digitales y detección de credenciales comprometidas incluso de fuentes indirectas. Incorpora automatización de alertas, evidencias detalladas por cada acción de cierre y soporte 24x7 a través de su herramienta propietaria de gestión de incidentes.</p> <p>Se incluye un paquete de 10 takedowns con múltiples escenarios que cuentan con una descripción detallada (phishing, cybersquatting, apps, redes sociales, repositorios y acortadores). La solución también incluye inteligencia contextual, categorización de amenazas y colaboración con CERTs e ISPs.</p> <p>Todas estas capacidades demuestran un dimensionamiento por tipo de licencia alineado con los requisitos del servicio de protección de marca e identidad digital, por lo que se asigna la puntuación máxima en este apartado: 10 puntos.</p>
<p>Look&Feel (3 puntos)</p>	<p>La propuesta incluye la posibilidad de personalización visual mediante la incorporación del logotipo institucional del Gobierno de Navarra en informes y paneles de resultados. Asimismo, se valoran positivamente las evidencias gráficas aportadas, que muestran ejemplos gráficos de presentación de informes.</p> <p>Adicionalmente, se contempla en el roadmap la evolución hacia una personalización completa de la interfaz gráfica, incluyendo adaptación de colores corporativos, tipografías y otros elementos visuales alineados con la identidad del Navarra Cybersecurity Center (NavCC), sin coste adicional.</p> <p>No obstante, estas capacidades de personalización aún no se encuentran desplegadas en la versión actual del producto, y su implementación depende del cumplimiento del roadmap, que carece de una planificación formal definida.</p> <p>Por tanto, aunque se reconocen los avances visuales mostrados y la intención de evolución, no existe una garantía de que esto se desarrolle en el plazo de ejecución del proyecto, lo que justifica una puntuación de 3 sobre 5 en este apartado.</p>



Referencias (3 puntos)	<p>La propuesta aporta referencias del sector público tanto en España como en LATAM. Las entidades que cita utilizan la herramienta objeto de la licitación para la monitorización tanto de su propio dominio como de terceros, aplicando funcionalidades como reputación de IP, gestión de parches, análisis web, filtración de credenciales, fugas de datos y squatting.</p> <p>Si bien las referencias son relevantes y se alinean con el objeto de la licitación, no se mencionan expresamente referencias en cuanto al servicio de monitorización de perfiles VIP, considerado fundamental para la ejecución del contrato. Es por ello por lo que se obtiene una puntuación de 3 sobre 5 en este apartado.</p>
RoadMap (1 punto)	<p>La propuesta incluye una descripción general de funcionalidades que podrían incorporarse en futuras actualizaciones de la plataforma, como el cumplimiento normativo (ISO 27001 y PCI), integración de un marketplace, mapas de amenazas globales y herramientas de scoring por sectores y regiones.</p> <p>No obstante, la información carece de una planificación formal. No se presenta un cronograma estructurado, ni fases de desarrollo, ni indicadores de progreso que permitan evaluar el grado de ejecución. Las mejoras se formulan como objetivos genéricos, sin fechas concretas ni compromisos asociados. La mención a una posible release en el cuarto trimestre del año no está vinculada a un esquema de evolución técnica definido.</p> <p>Por tanto, aunque se exponen intenciones alineadas con el objeto de la licitación, la falta de un roadmap en sentido estricto impide valorar adecuadamente la viabilidad y alcance temporal del desarrollo. Por este motivo y, al tratarse de una declaración de intenciones sin una delimitación temporal concreta, la puntuación otorgada en este apartado es de 1 punto sobre 5.</p>
Auditorías de Seguridad (5 puntos)	<p>La herramienta SaaS cuenta con certificaciones ISO 27001 y ENS, y se encuentra sujeta a los sistemas de gestión certificados del proveedor, aplicando de forma nativa las mejores prácticas de seguridad y calidad. Además, se indica que la solución está auditada y alineada con estándares industriales, lo que garantiza un control efectivo sobre su seguridad y evolución.</p> <p>Estas condiciones otorgan un nivel de confianza óptimo en términos de seguridad de la solución, motivo por el cual se le asigna la máxima puntuación en este subapartado: 5 puntos.</p>

Por todo ello, la puntuación obtenida por el licitador en este apartado es de 22 puntos.

3.1.2 Servicio de formación, soporte, supervisión y reporting, indicando la metodología, planificación, modelo de gobierno y equipo de trabajo (hasta 20 puntos)

3.1.2.1 Metodología, planificación y modelo de gobierno (hasta 10 puntos)

MEMORIA DESCRIPTIVA

Thales S21sec (10 puntos)

<p>Valoración global (10 puntos)</p>	<p>Destaca la incorporación en la propuesta de una metodología estructurada basada en un modelo propio alineado con estándares reconocidos como ITIL v4, ISO 20000 y VeriSM, cuyo eje es la mejora continua. La aplicación del enfoque está claramente descrita, con la definición detallada de las fases del servicio, indicadores de rendimiento (SLAs) y mecanismos de control para una adecuada gestión del servicio.</p> <p>En cuanto a la planificación, se presenta un cronograma visual, acompañado de una descripción narrativa clara y detallada de cada fase, actividades, hitos y entregables. Esto permite un seguimiento concreto de la ejecución temporal del servicio. Finalmente, el modelo de gobierno incluye un Comité de Control y Supervisión con funciones bien definidas, niveles de escalado y criterios de decisión en función de métricas propuestas. Esta estructuración y descripción desarrollada justifica la puntuación máxima de 10 puntos.</p>
<p>Metodología</p>	<p>Se define una metodología estructurada basada en un modelo interno Enterprise Service Management, alineada con estándares como ITIL v4, ISO 20000 y VeriSM. Este enfoque proporciona una base para la gestión de servicios, que articula el ciclo de vida del proyecto en 4 fases diferenciadas: determinación del alcance, transición de entrada, prestación del servicio y transición de salida.</p> <p>Se valora positivamente el uso de indicadores como SLAs para garantizar el seguimiento, control y mejora continua de la calidad del servicio. Es por ello, por lo que la propuesta obtiene la máxima puntuación en este apartado.</p>
<p>Planificación</p>	<p>La planificación presentada estructura adecuadamente el proyecto en fases, con la inclusión de un diagrama de Gantt que permite visualizar la distribución temporal de las tareas, hitos y entregables.</p> <p>Cada acción está descrita detalladamente en la sección indicada en el diagrama, permitiendo un control y comprensión de la ejecución del servicio. Esta presentación en formato gráfico refleja una secuencia lógica con una estimación temporal adecuada alineada con el ciclo de vida del servicio. Por estos motivos, esta propuesta obtiene la máxima puntuación en este apartado.</p>

<p>Modelo de gobierno</p>	<p>La propuesta presenta un modelo de gobierno claramente definido, sustentado en la existencia de un Comité de Control y Supervisión encargado de gestionar los cambios, hacer seguimiento del servicio y aprobar modificaciones relevantes.</p> <p>Se especifican las responsabilidades del comité, los mecanismos de control mediante informes de servicio y los criterios para escalar acciones en función de su impacto sobre el acuerdo de servicio.</p> <p>Por el nivel de concreción y detalle aportado, se otorga la puntuación máxima para este apartado.</p>
----------------------------------	---

3.1.2.2 Equipo de trabajo (hasta 10 puntos)

MEMORIA DESCRIPTIVA	Thales S21sec (10 puntos)
<p>Valoración global (10 puntos)</p>	<p>El equipo de trabajo propuesto presenta un dimensionamiento adecuado a los requisitos del pliego y una estructura definida por perfiles, cubriendo así las distintas áreas funcionales del servicio.</p> <p>La propuesta incluye una descripción detallada de los roles, funciones y competencias de cada integrante del equipo, con asignación clara de responsabilidades y tareas específicas en el marco del proyecto.</p> <p>Asimismo, se aporta experiencia contrastable en proyectos directamente relacionados con EASM & Brand Protection y Protección de Identidad Digital, lo que refuerza la idoneidad técnica del equipo para la correcta ejecución del servicio, aprovechando el conocimiento adquirido en experiencias previas similares. Por tanto, todo ello justifica la puntuación máxima de 10 puntos en este apartado.</p>
<p>Roles y funciones</p>	<p>La propuesta detalla roles, funciones y responsabilidades individuales de cada miembro del equipo. Se identifican concretamente los perfiles (gestor del servicio, consultor estratégico, consultor GRC y consultor de inteligencia), así como sus tareas específicas dentro del proyecto, incluyendo la interlocución con el cliente, coordinación operativa, elaboración de informes personalizados, ejecución de tareas por área de especialización y reporting continuo.</p> <p>Esta asignación de roles y responsabilidades está alineada con los objetivos del servicio y del alcance funcional requerido, lo que permite atribuir la puntuación máxima en este apartado.</p>
<p>Experiencia en proyectos similares</p>	<p>La propuesta presenta un equipo técnico con una relación detallada de experiencias en proyectos similares al alcance de la licitación. Se incluyen actuaciones previas en iniciativas como Rating as a Service, Gestión de plataforma EASM & Brand Protection y Huella Digital de VIPs, realizadas para organizaciones y entidades diversas.</p> <p>Esta experiencia concreta en proyectos directamente relacionados con protección de marca y exposición de la superficie de ataque permite valorar positivamente la adecuación del equipo para asumir el servicio licitado.</p>



	<p>Por el grado de especificidad y vinculación con el objeto del contrato, esta oferta obtiene la puntuación máxima en este apartado.</p>
Certificaciones profesionales	<p>La propuesta detalla los perfiles asociados al servicio junto con la formación específica y las certificaciones asociadas. Se incluyen dos perfiles con certificaciones CISA y CISM respectivamente, y otras como Lead Auditor ISO en diferentes normas (27001, 22301, 20000-1), además de certificaciones técnicas como ITIL Foundations y PMP.</p> <p>Este nivel de acreditación profesional garantiza la competencia técnica del equipo para abordar tanto la auditoría como la gestión del riesgo y la seguridad. La información está bien estructurada y alineada con los requisitos del proyecto en cuanto a certificaciones de los perfiles asignados, lo que justifica la máxima puntuación en este apartado.</p>

Por todo ello, la puntuación obtenida por el licitador en este apartado es de 20 puntos.

3.2 SEIN TIC

3.2.1 Herramienta de EASM & Brand Protection y Protección de Identidad Digital (hasta 30 puntos)

HERRAMIENTA DE EASM & Brand Protection y Protección de Identidad Digital

SEIN TIC (12 puntos)

<p>Alcance cubierto por el tipo de licencia (2 puntos)</p>	<p>La propuesta describe de forma muy general las capacidades de la herramienta EASM & Brand Protection y Protección de Identidad Digital a través del portal FortiRecon. No obstante, no se proporciona visibilidad concreta sobre el tipo de licencia ofertada, ni sobre el alcance específico que cubre, lo que impide valorar la dimensión real del servicio. Asimismo, no se detallan los módulos de FortiRecon que se incluyen por licencia para cada necesidad. Tampoco se aclara el modelo de suscripción aplicable ni la cobertura del licenciamiento en cuanto a dominios, subdominios y número de direcciones IP cubiertas; ni si existen restricciones técnicas o comerciales por licencia. Esta falta de concreción representa una limitación clave para evaluar la capacidad operativa del servicio ofertado.</p> <p>En cuanto a los takedowns, la oferta menciona únicamente la posibilidad de solicitar su ejecución frente a usos indebidos de la imagen de marca o actividades maliciosas, pero no se detallan los tipos de cierres, su frecuencia ni alcance operativo, dificultando la evaluación de su cobertura. Si bien se valora la existencia de este componente, su peso es accesorio respecto al núcleo del servicio y su cobertura es insuficientemente detallada.</p> <p>Dado que la propuesta no permite dimensionar adecuadamente el alcance del servicio ni verificar qué funcionalidades están realmente cubiertas por cada licencia ofertada, se considera que la descripción es muy general y limitada. Por tanto, se asigna una puntuación de 2 sobre 10 en este apartado.</p>
<p>Look&Feel (2 puntos)</p>	<p>La oferta incluye la posibilidad de personalización visual del entorno, permitiendo adaptar el portal a la identidad corporativa del NavCC mediante logotipos, colores, tipografías y selección de tema. También se destaca la posibilidad de representar datos en portales externos mediante integración vía API, lo que aporta flexibilidad.</p> <p>Sin embargo, la propuesta no aporta evidencia gráfica que demuestren la personalización ofrecida ni su implementación real. La ausencia de pruebas visuales limita la capacidad de validar esta funcionalidad.</p> <p>Por tanto, se reconoce la descripción funcional, pero se penaliza la falta de evidencia visual y concreción obteniendo una puntuación de 2 sobre 5 en este subapartado.</p>

<p>Referencias (3 puntos)</p>	<p>La propuesta incluye referencias contratables en el ámbito empresarial, con implantaciones de FortiRecon en distintos clientes. Estas organizaciones han desplegado servicios de EASM & Brand Protection con el soporte de TIGLOO, lo cual aporta valor al demostrar experiencia en distintos sectores industriales. Se adjuntan certificados de buena ejecución en dos casos, lo que refuerza la validez de las referencias.</p> <p>Sin embargo, la descripción es genérica y no se especifica el uso concreto de funcionalidades clave, como la monitorización de perfiles VIP. Dado que este último aspecto es un requerimiento relevante en la licitación, la ausencia de esta mención limita su valoración global, obteniendo una puntuación de 3 puntos sobre 5 en este apartado.</p>
<p>RoadMap (0 puntos)</p>	<p>La propuesta recoge un listado de versiones y mejoras ya implementadas hasta junio de 2025, incluyendo funcionalidades como filtros avanzados, soporte con FortiGate, monitorización de perfiles VIP y paneles de auditoría. Estas actualizaciones reflejan el estado actual del producto, pero no constituyen un roadmap futuro.</p> <p>Además, la oferta reconoce explícitamente que no se dispone de un roadmap público para FortiRecon, y la información futura está sujeta a confidencialidad. La mayoría de las acciones están formuladas como declaraciones de intención sin una delimitación temporal concreta, lo que limita totalmente la visibilidad sobre el desarrollo futuro de la solución.</p> <p>Por ello, no se asigna puntuación en este apartado, al no cumplir con los criterios requeridos para ser considerado un roadmap de evolución en sentido estricto.</p>
<p>Auditorías de Seguridad (5 puntos)</p>	<p>La propuesta incluye un conjunto específico de certificaciones de seguridad aplicadas al entorno SaaS propuesto, destacando ISO 27001, 27017, 27018 y 9001, que cubren tanto la gestión de la seguridad de la información como la protección de datos personales en la nube y la calidad del servicio.</p> <p>El nivel de cumplimiento y madurez normativa de la solución FortiRecon propuesta permite validar su idoneidad en términos de seguridad de esta, por lo que se asigna la puntuación máxima en este apartado: 5 puntos.</p>

Por todo ello, la puntuación obtenida por el licitador en este apartado es de 12 puntos.

3.2.2 Servicio de formación, soporte, supervisión y reporting, indicando la metodología, planificación, modelo de gobierno y equipo de trabajo (hasta 20 puntos)

3.2.2.1 Metodología, planificación y modelo de gobierno (hasta 10 puntos)

MEMORIA DESCRIPTIVA	SEIN TIC (3 puntos)
<p>Valoración global (3 puntos)</p>	<p>La propuesta presenta un enfoque metodológico apoyado en una lógica operativa de detectar, proteger y responder. Esta aproximación metodológica se limita únicamente al funcionamiento de la herramienta y no se identifica una metodología formal de gestión de servicios que permita evaluar las capacidades de Tigloo como proveedor de servicios de ciberseguridad.</p> <p>La planificación incluye una descripción general de fases y entregables, pero carece de un cronograma visual que facilite la estructura temporal concreta asociada a cada una de ellas. Asimismo, no se establece un modelo de gobierno claro, más allá de la figura de un coordinador del servicio ni se definen comités ni asignan responsabilidades diferenciadas, impidiendo evaluar los mecanismos de supervisión y decisión para la gestión adecuada del servicio. Debido a estas limitaciones, la puntuación en este apartado es de 3 puntos.</p>
<p>Metodología</p>	<p>La descripción carece de una metodología formal de gestión de servicios que permita evaluar la madurez del proveedor como gestor de servicios de ciberseguridad. La aproximación metodológica presentada se basa en una secuencia de acciones tipo "detección, protección y respuesta", alineadas con las capacidades técnicas de la herramienta, pero no con un modelo de gestión de servicios que evidencie la planificación y gestión operativa del servicio.</p> <p>Dado que la propuesta únicamente incluye metodología referente a la solución tecnológica y no a la metodología del servicio en su conjunto ofrecida por el proveedor, no se otorga puntuación en este criterio.</p>
<p>Planificación</p>	<p>Se incluye una planificación estructurada por fases, con la definición de actividades clave y entregables para cada una de ellas. Sin embargo, la ausencia de un diagrama visual dificulta la evaluación precisa de la secuencia temporal, la distribución de tareas y los plazos concretos de ejecución.</p> <p>Por lo tanto, esto limita la capacidad para valorar concretamente la viabilidad temporal del proyecto, lo que impacta negativamente en la puntuación de este apartado. Por ello, se otorgan 2 puntos en este apartado.</p>

<p>Modelo de gobierno</p>	<p>La propuesta incluye únicamente la mención de la figura de un coordinador del servicio, sin detallar la existencia de un comité ni una estructura clara de gobierno. No se proporciona una descripción del modelo de control ni se especifican los roles y responsabilidades asociados a la dirección y seguimiento del servicio más allá de la figura del coordinador.</p> <p>Esta falta de detalle limita la capacidad de evaluar el modelo de gobierno necesario para garantizar un adecuado desarrollo del servicio, obteniendo 1 punto en este apartado.</p>
----------------------------------	--

3.2.2.2 Equipo de trabajo (hasta 10 puntos)

MEMORIA DESCRIPTIVA	SEIN TIC (2 puntos)
<p>Valoración global (2 puntos)</p>	<p>La propuesta presentada incluye una descripción genérica del equipo necesario para garantizar la correcta ejecución y cobertura del servicio. Sin embargo, no se detallan funciones individualizadas ni se identifican responsables concretos dentro del proyecto, lo que limita la evaluación de su capacidad organizativa. La propuesta no incluye referencias específicas a proyectos de naturaleza similar, ni se aporta experiencia directamente vinculada con servicios de EASM & Brand Protection o Protección de Identidad Digital.</p> <p>Asimismo, no se presentan certificaciones técnicas de los perfiles asignados, elemento considerado fundamental en el marco de la licitación.</p> <p>Por tanto, la ausencia de estos elementos clave justifica la asignación de una puntuación de 2 puntos sobre 10 en este apartado.</p>
<p>Roles y funciones</p>	<p>Se describe una estructura funcional basada en perfiles técnicos (Red Team, Blue Team, Técnicos de Infraestructuras) y presenta tareas generales por grupo. Sin embargo, no se definen de forma individualizada los roles ni las funciones específicas de cada miembro del equipo y las descripciones resultan genéricas, sin vincular responsabilidades concretas.</p> <p>Esta falta de concreción impide valorar adecuadamente la organización del equipo y su idoneidad para asumir las funciones del servicio en el contexto de esta licitación. En consecuencia, se otorga la mitad de la puntuación para este apartado.</p>
<p>Experiencia en proyectos similares</p>	<p>La propuesta describe un equipo con experiencia general en proyectos de ciberseguridad, así como competencias en protección de marca y uso de herramientas como FortiRecon.</p> <p>Sin embargo, no se aporta información concreta ni ejemplos verificables de proyectos similares realizados previamente que permitan evaluar la experiencia específica en servicios de EASM & Brand Protection y protección de identidad por parte de los perfiles especificados para la ejecución del servicio.</p>



	<p>Aunque los perfiles cuentan con experiencia técnica relevante en infraestructuras y seguridad, la falta de referencias explícitas limita la capacidad de valorar la idoneidad del equipo en contextos comparables al objeto de la licitación.</p> <p>Por lo tanto, esta oferta no obtiene puntuación en este subapartado.</p>
Certificaciones profesionales	<p>La propuesta describe de forma genérica perfiles con experiencia en ciberseguridad y en el uso de la herramienta propuesta para la ejecución del servicio, pero no se detalla ningún tipo de certificación concreta del equipo de trabajo.</p> <p>Dado que estas certificaciones se consideran fundamentales en el marco de esta licitación y no se aporta detalle de estas, esta propuesta no obtiene puntuación en este apartado.</p>

Por todo ello, la puntuación obtenida por el licitador en este apartado es de 5 puntos.

4 RESUMEN DE PUNTUACIÓN DE CRITERIOS SOMETIDOS A LA APLICACIÓN DE JUICIOS DE VALOR

De las valoraciones de los criterios sometidos a la aplicación de juicios de valor definidos

	Puntuación máxima	Puntuación Thales S21sec	Puntuación SEIN TIC
Herramienta de EASM & Brand Protection y Protección de Identidad Digital	30	22	12
Servicio de formación, soporte, supervisión y reporting, indicando la metodología, planificación, modelo de gobierno y equipo de trabajo	20	20	5
TOTAL	50	42	17

en el Pliego de Cláusulas Administrativas, se obtiene el siguiente resultado:

En Pamplona, a 24 de julio de 2025

Juan Ramón Aramendia Muneta
Coordinador del Navarra Cybersecurity Center

Haritz Elizetxe Berenguer
Especialista en Ciberseguridad en Navarra Cybersecurity Center

Teresa Carrasco Pérez
Técnico en Ciberseguridad en Navarra Cybersecurity Center