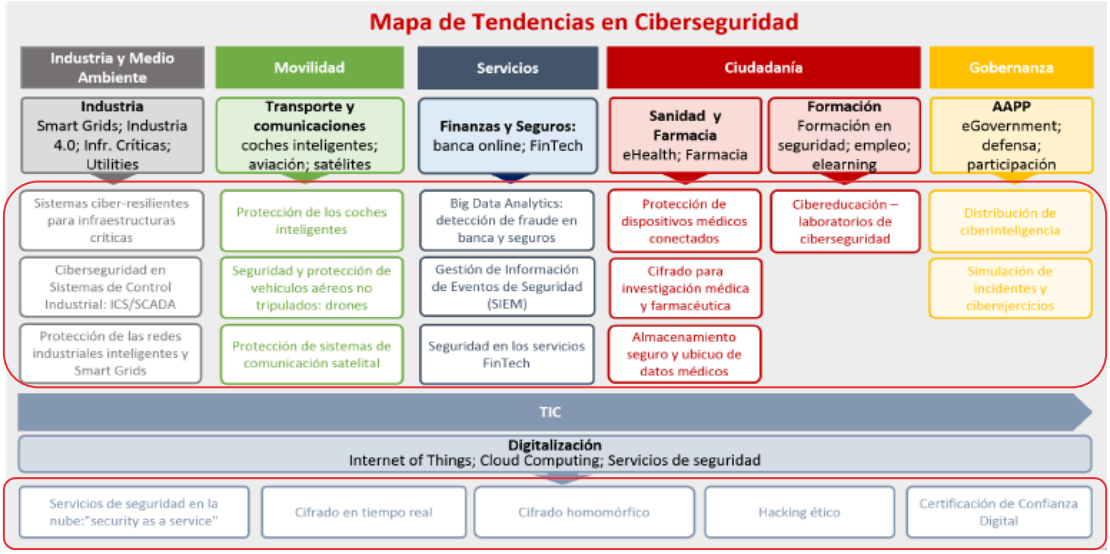
Retos estratégicos del programa de aceleración

La figura presenta los retos estratégicos en Ciberseguridad correspondiéndose con las tendencias identificadas en el documento de "Tendencias en el Mercado de la Ciberseguridad". Se puede consultar una explicación más detallada de cada uno de los retos en el Anexo 1 directamente accediendo al citado documento a través de la web de INCIBE (www.incibe.es)



Teniendo en cuenta la cadena de valor de la Ciberseguridad y su impacto en ciudadanos, empresas y Administraciones Públicas, se ha diseñado un mapa de tendencias de demanda en el que se identifican 22 tendencias globales en Ciberseguridad catalogadas en torno a 6 sectores de actividad.

Sector Industrial y Medio Ambiente.

- **Sistemas ciber-resilientes para Infraestructuras Críticas:** La destrucción o perturbación de infraestructuras estratégicas cuyo funcionamiento es indispensable tendría graves consecuencias sobre servicios esenciales, por lo que requieren de sistemas diseñados para hacer frente a una crisis de seguridad sin que su actividad se vea afectada, incluyendo nuevos estándares, mecanismos, frameworks y tool suites que provean dicha seguridad automatizada.
- **Ciberseguridad en Sistemas de Control Industrial:** ICS/SCADA. La complejidad de los sistemas ICS/SCADA radica principalmente en su naturaleza multidisciplinar y aplicable a multitud de sectores. Ello justifica la necesidad de implantar altos niveles de ciberseguridad en los sistemas SCADA, lo que incluye tanto la securización de sistemas legados ya desplegados como la creación de una nueva generación de redes y ecosistemas ciberseguros.

Protección de las redes industriales inteligentes y Smart Grids. La necesidad de protección de las redes de sensores industriales radica en medidas de seguridad que sin impactar en el nivel y calidad del servicio requerido por las normativas y estándares de cada dominio de aplicación ofrezcan protocolos de autenticación, cifrado de conexiones M2M y eliminación de redundancias.

Sector Transporte y Comunicaciones

- **Protección de vehículos inteligentes**. La protección de vehículos inteligentes hace referencia a la seguridad de los **sistemas de control** de vehículos interconectados y de vehículos terrestres autónomos, así como de los **sistemas inteligentes de transporte** que interaccionan con ellos por medio de redes de comunicaciones específicas. Estas redes deben estar protegidas contra **bloqueos de la señal**, ataques de denegación de servicio, privacidad del usuario y su localización precisa, así como la transmisión de datos falsos a los vehículos terrestres conectados y a sus conductores.
- **Seguridad y protección de vehículos aéreos no tripulados: drones**. El desarrollo y uso de drones supone un gran reto para la seguridad. Desde el punto de vista de la ciberseguridad, estos dispositivos están expuestos a riesgos de **pérdida de confidencialidad, integridad y disponibilidad** de los datos.
- **Protección de sistemas de comunicación vía satélite**. Las Comunicaciones por Satélite juegan un papel vital en el sistema de telecomunicaciones global. Estos sistemas presentan distintas vulnerabilidades que podrían permitir a **atacantes remotos** inutilizar por completo los dispositivos. Entre los sistemas afectados se podrían encontrar múltiples **sistemas y servicios críticos**, como: servicios de emergencia, militares, aviones, barcos, sistemas industriales, etc.

Sector Finanzas y Seguros

- **Big Data Analytics: detección de fraude en banca y seguros**. El uso de Big Data Analytics en el sector bancario y de seguros, permite entre otras la detección y prevención del fraude en tiempo real, reduciendo los costes de monitorización e investigación de incidentes y por tanto reduciendo las pérdidas derivadas de actividades fraudulentas.
- **Seguridad en los servicios Fintech**. La seguridad en servicios Fintech se basa en el desarrollo de nuevas soluciones de protección de sistemas o aplicaciones de pago online, sistemas de m-commerce o comercio móvil, email/browser sandboxing, dispositivos de tecnología NFC, lectores de tarjetas para móviles, etc., basadas en la **autenticación de usuario, confidencialidad** y soluciones de prevención de fraude.

Sector Salud

- **Protección de dispositivos médicos conectados**. Estos dispositivos pueden exponer a los pacientes y a las organizaciones de atención de la salud, a los riesgos de la seguridad y la protección. Todos estos dispositivos interconectados en una red necesitan asegurar la **confidencialidad, integridad y control** de los mismos, especialmente, en aquellos cuyo software no está personalizado para su uso.
- **Cifrado para investigación médica y farmacéutica**. La tendencia de seguridad de datos médicos avanza hacia un **cifrado apto** para hacer coincidir las fuentes de información de múltiples centros médicos, que están **cifrados con claves diferentes**, sin descifrado de la información, salvaguardando la **confidencialidad** en la información de los pacientes.
- **Almacenamiento seguro y ubicuo de datos médicos**. La sensibilidad de la información de los pacientes requiere no sólo de un sistema de almacenamiento cifrado, sino de un mecanismo de transferencia seguro, garantizando que la **ubicuidad de los datos personales y clínicos** de los pacientes no pone en peligro su confidencialidad.

Sector Formación e Investigación

- **Cibereducación – Laboratorios de seguridad**. La integración de la educación con la tecnología y la ciberseguridad converge en lo que se reconoce como cibereducación. Se trata de una **modalidad educativa** que formula la enseñanza a partir de diferentes competencias y disciplinas, tales como: interactuación, retroalimentación, gamificación, simulación, etc. aplicadas a la formación en ciberseguridad. La cibereducación **podrá estar orientada tanto a profesionales como a empresas**, incluyendo además de la capacitación en ciberseguridad otros aspectos como la simulación de incidentes y ciberejercicios de seguridad, cyber security challenges, etc.

Sector Gobierno y Defensa

- **Distribución de ciberinteligencia**. Se trata de un modelo cooperativo basado en el intercambio de información entre organismos, públicos y privados, proveniente del **análisis de ciberamenazas** con el objetivo de mejorar y agilizar la detección y actuación ante las amenazas en ciberseguridad.
- **Simulación de incidentes y ciberejercicios**. Los sistemas de simulación de escenarios e incidentes se basan en la utilización de **entornos de entrenamiento**, que ponen a prueba la capacidad tecnológica y de reacción de las herramientas y recursos de una organización. Los **ciberejercicios**, por su parte, permiten evaluar el estado de preparación de los participantes frente a **crisis de origen cibernético**.
- **Gobierno abierto y participación ciudadana**. La participación ciudadana e incluso los modelos de gobernanza abierta requieren de nuevas tecnologías que permitan **garantizar y combinar anonimización y auditabilidad** de la participación o voto electrónico para garantizar la confidencialidad y confianza de la ciudadanía en sus resultados.

Sector TIC

- **Servicios de seguridad en la nube: "*security as a service*"**. Estos servicios son generalmente **modelos de outsourcing** de la administración de la seguridad, que se aprovechan de la escalabilidad del modelo de Cloud Computing permitiendo a las organizaciones dimensionar los esfuerzos a su capacidad actual.
- **Cifrado en tiempo real**. Se trata de un mecanismo de **protección de la seguridad de los datos** en las transacciones electrónicas en el que los datos se cifran antes de ser almacenados y se descifran al descargarse, previamente a su utilización. Este tipo de cifrado permanece en segundo plano ante el usuario.
- **Cifrado homomórfico**. Esta tendencia de cifrado permite que la información que se codifique pueda ser compartida con **terceras partes** y ser utilizada en cálculos y procesos computacionales, sin que los sistemas implicados puedan interpretar dicha información pero sí ofrecer un resultado no cifrado a esos cálculos y procesos.
- **Criptografía cuántica**. La utilización de **principios de la mecánica cuántica** para el desarrollo de nuevos sistemas y protocolos criptográficos permitirá elevar exponencialmente la confidencialidad de la información y comunicaciones del futuro.
- **Nuevas tecnologías innovadoras de Hacking ético**. Se basa en innovadores sistemas para la búsqueda de vulnerabilidades mediante la utilización de **pruebas de penetración o "pentest"** en las redes de una organización con el objetivo de prevenir posibles fallos de seguridad, mitigar el impacto provocado por cualquier incidente de seguridad, priorizar riesgos y verificar el cumplimiento normativo.

- **Modelos innovadores de confianza digital**. Consiste en comprobar, materializar y dar visibilidad el **nivel de ciberseguridad** que implementa un proveedor en un servicio determinado, es decir, la emisión de **sellos de confianza digital** que valoran objetivamente las medidas de seguridad integradas por el proveedor de servicios.
- **Plataformas avanzadas de detección de anomalías, gestión de Información de Eventos de Seguridad (SIEM) y detección/prevención de intrusiones (IDS/IPS)**. Se basa en la detección de amenazas y respuesta a incidentes de seguridad a través de la obtención en **tiempo real** de eventos de seguridad y su **análisis histórico**, a partir de una amplia variedad de fuentes de eventos y datos contextuales.