AGENCIA DE CIBERSEGURIDAD

PLAN ESTRATÉGICO

AGENCIA DE CIBERSEGURIDAD

de la Comunidad de Madrid

Comunidad de Madrid

ÍNDICE

PLAN ESTRATÉGICO
AGENCIA DE CIBERSEGURIDAD
de la Comunidad de Madrid

1.
Presentación del Plan Estratégico

AGENCIA DE CIBERSEGURIDAD

La digitalización forma parte de nuestra vida y nos lleva a proteger nuestras infraestructuras físicamente y también en el ciberespacio: el agua, los transportes, hospitales, colegios, datos personales...

Por eso, desde el Gobierno de la Comunidad de Madrid pusimos en marcha —por ley—, la Agencia de Ciberseguridad. Una iniciativa estratégica con la que damos un paso decidido en la defensa de nuestros derechos digitales y en la confianza en las instituciones. Con este Plan Estratégico consolidamos nuestro compromiso hacia el futuro.

La agencia no solo refuerza nuestra capacidad operativa, sino que nos permite actuar con visión a largo plazo, anticiparnos a los nuevos riesgos y establecer prioridades claras. El plan que presentamos es fruto de una planificación rigurosa, basada en el conocimiento técnico y en la voluntad de proteger lo esencial.

No se trata solo de tecnología. Es una apuesta política por una región más fuerte, libre y segura. Un Madrid que impulsa herramientas como el Escudo Digital, refuerza la capacidad de respuesta ante ciberataques y acompaña a todos los municipios, sin excepción, en su digitalización segura.

La Comunidad de Madrid ha demostrado que es posible innovar sin renunciar a los principios que nos definen: libertad, responsabilidad, eficiencia y vocación de servicio. Este plan evita exceso de burocracia y tecnicismos, y ofrece soluciones útiles para proteger lo que realmente importa de forma ágil, realista y eficaz.

Confío plenamente en que, con la implicación de nuestras administraciones, empresas, profesionales y ciudadanos, la Comunidad de Madrid también seguirá liderando el ámbito digital como un ejemplo de seguridad y vanguardia.

ISABEL DÍAZ AYUSO
Presidenta de la Comunidad de Madrid

La ciberseguridad se ha convertido en una condición indispensable para el progreso. En un entorno donde lo digital atraviesa todos los ámbitos de nuestra vida —la educación, la sanidad, la movilidad, la administración—, no hay transformación tecnológica sostenible si no es también segura. Sin ciberseguridad, los datos no están protegidos, los servicios pierden confianza y la innovación se vuelve frágil.

Consciente de esta realidad, la Comunidad de Madrid dio un paso pionero al crear su propia Agencia de Ciberseguridad. Desde la Consejería de Digitalización, hemos impulsado el desarrollo de este Plan Estratégico como una herramienta que hace realidad una visión política ambiciosa. En él confluyen iniciativas tecnológicas de vanguardia —como el Escudo Digital o la consolidación del Computer Security Incident Response Team (CSIRT) regional— con medidas más estructurales: gobernanza del riesgo, cultura organizativa, formación, cumplimiento normativo y colaboración público-privada.

Este plan no parte de cero. Se apoya en el trabajo realizado en los últimos años con administraciones locales y entidades públicas, y proyecta ese esfuerzo hacia una nueva etapa con mayor capacidad operativa, coordinación regional y evaluación continua. Su enfoque es práctico, adaptable y dirigido a acompañar a todas las entidades —grandes o pequeñas— en su proceso de madurez digital.

Desde esta Consejería, respaldamos plenamente los objetivos y las líneas de actuación del plan. Reforzaremos sus medios, facilitaremos su despliegue institucional y promoveremos una digitalización segura como principio rector de toda política pública en el ámbito tecnológico.

Nuestro compromiso es claro: que Madrid siga siendo sinónimo de innovación, confianza y liderazgo tecnológico, pero también de protección, responsabilidad y garantía para todos sus ciudadanos.

MIGUEL LÓPEZ-VALVERDE ARGÜESO
Consejero de Digitalización de la Comunidad de Madrid

Este Plan Estratégico nace con la voluntad de dotar a la Comunidad de Madrid de un modelo sólido, integral y sostenible de seguridad digital. Se trata de una arquitectura común que vincula tecnología, organización y cultura de seguridad, alineada con los principios del buen gobierno digital y con una visión territorial e institucional compartida.

A lo largo de sus siete líneas estratégicas, el plan establece objetivos concretos que abarcan desde el diseño de un sistema de gestión de la seguridad aplicable al ecosistema público, hasta la implantación de indicadores que permitan medir el grado de madurez de cada entidad y el clima de amenaza regional. Este enfoque facilitará la detección de brechas, la respuesta eficaz y la mejora continua.

El Escudo Digital y el CSIRT de la Comunidad de Madrid son los pilares tecnológicos de este modelo: el primero, como infraestructura de protección activa basada en análisis de tráfico, correlación de eventos y respuestas automatizadas; el segundo, como centro regional para la detección, gestión y aprendizaje técnico ante incidentes. Ambos estarán integrados y operarán con capacidades de vigilancia digital, inteligencia de amenazas y coordinación con organismos nacionales e internacionales.

Pero la ciberseguridad no se basa únicamente en capacidades tecnológicas. Por eso, el plan incorpora una estrategia de refuerzo del cumplimiento normativo —Esquema Nacional de Seguridad (ENS) y Directiva NIS2—, programas de concienciación y formación especializada, iniciativas de desarrollo de talento, y un impulso claro a la colaboración público-privada. Esta combinación de medidas nos permitirá afrontar los retos con enfoque transversal, anticipación y respuesta eficaz.

Desde la Agencia asumimos el liderazgo de esta estrategia con el firme compromiso de desplegarla con rigor, transparencia y acompañamiento continuo. Nuestro propósito es claro: elevar la ciberresiliencia de la Comunidad de Madrid y consolidar un entorno digital fiable, robusto y preparado para los desafíos del presente y del futuro.

ALEJANDRO LAS HERAS VÁZQUEZ
Consejero Delegado de la Agencia de Ciberseguridad de la Comunidad de Madrid

PLAN ESTRATÉGICO
AGENCIA DE CIBERSEGURIDAD
de la Comunidad de Madrid

2.
Contexto y Resumen Ejecutivo

AGENCIA DE CIBERSEGURIDAD

Contexto

En la Administración de la Comunidad de Madrid se detectaron en el año 2023 un total de 50.089 ataques informáticos correspondientes a amenazas e intentos de hackeo externos. Esta cifra no incluye aquellos ataques detectados por aquellas organizaciones públicas que cuentan con servicios propios fuera de las competencias de la Agencia autonómica para la Administración Digital (Madrid Digital), como son el Servicio de Emergencias 112, la Asamblea de Madrid, la Cámara de Cuentas, Metro de Madrid o Canal de Isabel II.

Otro de los grandes retos a los que se enfrenta la Administración pública en la región es el de proporcionar una cobertura de ciberseguridad o lo que es lo mismo, la implementación de un Escudo Digital, para todas aquellas localidades de la Comunidad de Madrid, ya que cuentan con menos capacidades y donde cada una parte de un nivel de madurez distinto tanto a nivel de protección como en cumplimiento regulatorio.

Por este motivo, es necesario tener una visión más granular sobre aquellas entidades regionales, conociendo su realidad particular para ofrecerles el apoyo necesario en el asesoramiento y suministro de servicios y soluciones de ciberseguridad, no solamente desde la prevención y detección de ciberamenazas, sino también mejorando la coordinación en la gestión de ciberincidentes junto con las autoridades del ámbito nacional y otros órganos de cooperación relevantes.

En la Administración de la Comunidad de Madrid se detectaron en el año 2023 un total de 50.089 ataques informáticos correspondientes a amenazas e intentos de hackeo externos.

Principales regulaciones de referencia en materia de ciberseguridad a nivel nacional:

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

Principales regulaciones de referencia en materia de ciberseguridad en el ámbito de la Unión Europea:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por lo que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («Reglamento sobre la Ciberseguridad»).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
- Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo de 23 de octubre de 2024 sobre requisitos horizontales de ciberseguridad para productos con elementos digitales.

Resumen Ejecutivo

La Comunidad de Madrid concentra aproximadamente el **28% de la actividad vinculada a la economía digital** en toda España, representando esta actividad el 21% del PIB español. Adicionalmente, dentro de la región, prácticamente un tercio de su actividad económica se debe a la digitalización. Por lo tanto, es necesario desarrollar las capacidades necesarias para abordar un futuro digital seguro para la administración regional, los **ciudadanos y empresas**.

En este contexto nace la **Agencia de Ciberseguridad de la Comunidad de Madrid**. Es necesario crear un ecosistema de confianza digital en la región, incrementar la colaboración público-privada para ofrecer los mejores servicios de ciberseguridad a los ciudadanos, favorecer la creación de nuevas empresas en esta materia y captar el mejor talento en capacidades digitales.

La Agencia pretende convertirse no solo en un líder regional, sino también en el **ámbito nacional e internacional**, estando presente en foros internacionales y ser un actor de primera línea en la coordinación con organismos y autoridades.

En este Plan Estratégico de la Agencia se abordan **siete líneas** con la finalidad de llevar a cabo la misión encomendada, tal y como se recoge en la ley 14/2023 del 20 de diciembre. Éstas abordan aspectos como el gobierno de la ciberseguridad en la región, potenciar las capacidades de gestión y respuesta a ciberincidentes, garantizar el cumplimiento efectivo de la legislación aplicable e impulsar el ecosistema de ciberseguridad, entre otros. En el Plan se plantean en detalle las actividades que están contenidas en cada una de estas líneas, así como su planificación hasta el año 2028.

Finalmente, se aborda cuales van a ser los mecanismos para realizar una **evaluación y seguimiento** del Plan Estratégico.

La Agencia de Ciberseguridad de la Comunidad de Madrid nace para abordar un futuro digital seguro para ciudadanos y empresas.

3.
Entendimiento y Posicionamiento de la Agencia

AGENCIA DE CIBERSEGURIDAD

La Agencia nace con el objetivo de posicionar a la Comunidad de Madrid como un referente en Ciberseguridad.

2024

01 REFERENTE REGIONAL

Creación de la Agencia de Ciberseguridad de la Comunidad de Madrid

- Crear la **Agencia** de acuerdo con la ley 14/2023.
- Definición y puesta en marcha del **Plan Estratégico**.
- Establecer un **modelo de gobernanza y control de ciberseguridad**.
- Iniciar la **prestación de servicios** de ciberseguridad en la región.

2025 - 2026

02 REFERENTE NACIONAL

La Agencia referente en el panorama nacional

- Fortalecer las capacidades mediante el despliegue del Escudo Digital.
- Establecer el **Computer Security Incident Response Team (CSIRT)** de referencia de la Comunidad de Madrid.
- Garantizar el **cumplimiento efectivo** de los organismos y entidades.
- Apoyar al **emprendimiento del ecosistema** empresarial de ciberseguridad como pilar de crecimiento industrial y económico.

2027

03 REFERENTE EUROPEO

Posicionar a la Agencia como un referente europeo

- Extender el cumplimiento de **estándares internacionales**.
- Fomentar Madrid como **Hub de talento y empresas** de ciberseguridad.
- **Evento internacional** de ciberseguridad de la Agencia de la Comunidad de Madrid.

2028

04 REFERENTE INTERNACIONAL

La Agencia de Ciberseguridad adquiere estatus de referente internacional

- Presencia en los **grandes foros internacionales**.
- Colaborar en el **desarrollo de estándares, productos y servicios** innovadores de ciberseguridad.
- **Alianzas estratégicas** a nivel internacional.

Análisis DAFO

FORTALEZAS

Desde 2022, ha asumido el desafío de convertirse en el **motor digital de Europa**, con la previsión de que la digitalización represente el **40% del PIB** en los próximos años. Este compromiso se traduce en el desarrollo de modernas **infraestructuras digitalizadas** que fortalecen la base tecnológica de la región. Además, la presencia de **Centros de Excelencia y universidades** con formación especializada en ciberseguridad, junto con la reciente creación de la **Agencia de Ciberseguridad**, refuerzan la capacidad de la región para liderar la seguridad digital.

OPORTUNIDADES

El impulso a la implementación de un proceso de compras centralizadas permitirá **optimizar costes** en ciberseguridad, además de **dinamizar** el sector y fomentar el **crecimiento y fortalecimiento** de las **PYMES** (Pequeñas y Medianas empresas) en el ámbito digital. La **garantía** de cumplimiento con nuevas regulaciones, como el **Esquema Nacional de Seguridad** (ENS), **Critical Entities Resilience** (CER), **Directiva NIS2** y su transposición a través del **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**, será un factor clave para garantizar la protección. El uso de las **tecnologías innovadoras**, como la Inteligencia Artificial, es un motor clave de la transformación digital, y la promoción de la **colaboración público-privada** facilitará el intercambio de información y recursos en el ámbito de la ciberseguridad.

AMENAZAS

En la Administración del Ejecutivo autonómico se detectaron en 2024 un total de 50.089 ataques informáticos, lo que refleja el panorama actual de amenazas en el entorno digital. La **coordinación** entre los actores clave debe evolucionar para mejorar la gestión de incidentes. Las **tecnologías emergentes** como la inteligencia artificial, el 5G, la computación en la nube y la biometría presentan **riesgos significativos sin controlar**. Además, en la región se encuentra un **gran número de infraestructuras críticas**, lo que aumenta su vulnerabilidad frente a ataques. El **contexto geopolítico actual** también representa una amenaza para las infraestructuras críticas y la Administración Pública madrileña.

DEBILIDADES

Uno de los principales retos en el ámbito de la ciberseguridad es la **escasez de talento especializado**, lo que limita la capacidad de respuesta ante los crecientes ciberataques. Además, tanto la **Administración Pública** como las **empresas privadas** disponen de **recursos limitados** en ciberseguridad, lo que dificulta el fortalecimiento de las defensas digitales. Existe una **diversidad en los niveles de madurez** en ciberseguridad entre los diferentes entes y organismos del Gobierno regional, lo que genera desigualdad en la protección y gestión de la seguridad digital. También persiste una **baja concienciación y formación en seguridad digital**, especialmente entre los **ciudadanos y las pequeñas empresas**, lo que las hace más vulnerables a incidentes. La **obsolescencia tecnológica** y la falta de **medidas adecuadas de protección** aumentan los riesgos. Además, la **ausencia de certificación en el Esquema Nacional de Seguridad (ENS)** en muchas **localidades** impide una evaluación adecuada de los estándares de seguridad implementados.

Misión, Visión y Valores

La **VISIÓN** de la Agencia consiste en garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguras y fiables.

La **MISIÓN** es la de dirigir y coordinar la ciberseguridad, así como impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la región.

Por último, los **VALORES** de la Agencia son los siguientes:

- **Compromiso y Rigor:** Con la rigurosidad, colaboración, proactividad, entusiasmo y trabajo en equipo.
- **Ética y Transparencia:** Conducta ética, transparencia e independencia del mercado.
- **Eficiencia y Simplificación:** Búsqueda permanente de la eficiencia y calidad en la prestación de todos nuestros servicios, facilitándolos y simplificándolos.
- **Innovación:** Inquietud y constante innovación.

4.
Líneas del Plan Estratégico

AGENCIA DE CIBERSEGURIDAD

Líneas del Plan Estratégico

Establecer un modelo de gobernanza y control de ciberseguridad

Supervisión y coordinación de la seguridad de sistemas y redes que soportan los servicios esenciales de la Administración Pública regional y local, garantizando el cumplimiento de los marcos normativos nacionales e internacionales aplicables.

Fortalecer las capacidades de prevención y detección

Desplegar un **Escudo Digital (CiberEscudo)** integral **enmarcado dentro del Escudo Europeo de Ciberseguridad** que fortalezca la protección, optimice la detección y garantice una respuesta efectiva frente a amenazas, abarcando todas las entidades de la Comunidad de Madrid.

Fomentar el talento y cultura de ciberseguridad

Impulsar la concienciación y la formación en seguridad digital con el objetivo de proteger a los ciudadanos y organizaciones frente a las ciberamenazas, promoviendo prácticas seguras y responsables en el entorno digital.

Impulsar la realización de eventos y alianzas estratégicas

Posicionar a la Agencia como líder de ciberseguridad mediante iniciativas innovadoras, el fomento de alianzas estratégicas y la evaluación del impacto de las nuevas tecnologías en ciberseguridad, promoviendo la innovación y estándares de excelencia.

Garantizar el cumplimiento efectivo de la legislación aplicable

Auditorías exhaustivas para evaluar la conformidad de las organizaciones de la Administración Autonómica madrileña con los marcos normativos como el ENS y el anteproyecto de Ley de la NIS2, garantizando la implementación efectiva de medidas de seguridad.

Potenciar las capacidades de gestión y respuesta ante a ciberincidentes

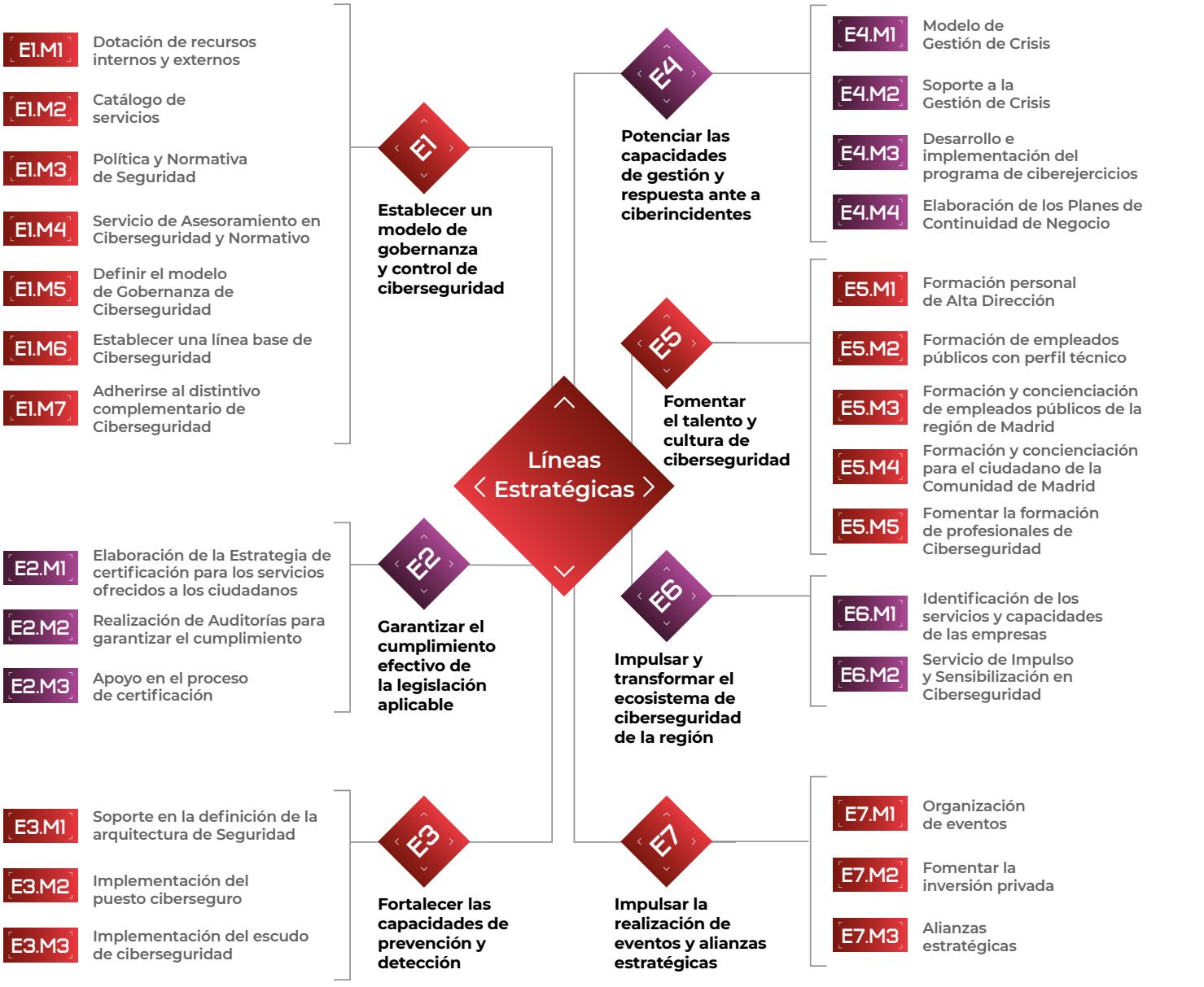
Supervisión continua de redes y fuentes de información para detectar y dar respuesta rápida y efectiva a ciberamenazas, garantizando una protección tanto proactiva como reactiva según la naturaleza de cada incidente.

Impulsar y transformar el ecosistema de ciberseguridad de la región

Promover un entorno empresarial en ciberseguridad a través de la identificación de servicios y capacidades de las empresas, junto con el impulso de inversiones estratégicas en innovación y captación de capital privado.

El Plan Estratégico lo conforman una serie de líneas o ejes estratégicos que a su vez contiene una serie de medidas que lo completan. Este plan contiene un total de siete líneas estratégicas que cubren diferentes dominios de la ciberseguridad, como la creación de un modelo de gobernanza de la ciberseguridad, el cumplimiento regulatorio, el refuerzo de las capacidades de respuesta frente a ciberincidentes o el impulso de la industria de ciberseguridad en la región.

Dichos ejes y medidas buscan elevar el nivel de madurez de ciberseguridad de la región, aumentar el grado de concienciación de los ciudadanos y empresas, así como reforzar las capacidades de ciberseguridad de las entidades locales y organismos de la Comunidad de Madrid mediante la provisión de servicios y soluciones de ciberseguridad que estén dirigidas y personalizadas acorde a las necesidades específicas.



01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

Resumen

El establecimiento de un **modelo de gobernanza y control de ciberseguridad** permitirá definir un marco estructurado para la supervisión y coordinación de la seguridad de los sistemas y redes que soportan los servicios esenciales de la Administración Pública regional y local garantizando el cumplimiento de los marcos normativos nacionales e internacionales aplicables y la resiliencia digital en el sector público.

Para ello, se abordarán diversas áreas estratégicas, como la **dotación de recursos internos y externos**, asegurando que la Administración cuente con el talento y las herramientas necesarias para gestionar la ciberseguridad de manera efectiva. Además, se desarrollará un **catálogo de servicios** que permitirá estructurar las capacidades y soluciones disponibles para las entidades gubernamentales. En el ámbito normativo, se establecerá una **política y normativa de seguridad** que garantice la alineación con regulaciones nacionales e internacionales. Además, se creará un **servicio de asesoramiento en ciberseguridad y legal**, para dar apoyo y reforzar el cumplimiento legal. Finalmente, con el objetivo de fomentar una cultura de ciberseguridad y reconocer las mejores prácticas en ciberseguridad, se impulsará la adhesión al **programa Madrid Excelente**, desarrollando un **distintivo de ciberseguridad.**

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E1.M1 Dotación de recursos internos y externos

Para proporcionar servicios de seguridad a los organismos de la Administración regional y entidades locales, y asegurar una gestión eficiente de los mismos, es imprescindible dotar a la agencia de los recursos necesarios, tanto internos como externos, que le permitan cumplir con su misión encomendada.

La creación de la **Agencia de Ciberseguridad** será clave para coordinar y supervisar todas las iniciativas relacionadas con la protección digital en el ámbito regional y local. Esta agencia tendrá la responsabilidad de implementar el Plan Estratégico de Ciberseguridad, cuyo contenido será aprobado y difundido en los medios para asegurar su visibilidad y alineación con las normativas y mejores prácticas nacionales e internacionales.

Para asegurar una **gestión eficaz** el objetivo es destinar de forma progresiva recursos internos altamente cualificados. Asimismo, se crearán diferentes **Subdirecciones y diversas oficinas** especializadas en cumplimiento normativo, riesgos, operaciones de ciberseguridad, sensibilización... de forma que toda la gestión se encuentre estructurada y optimizada.

Objetivos

1. **Incremento de los recursos internos.** Se van a ampliar de forma progresiva los recursos internos para fortalecer la capacidad operativa y estratégica de la Agencia. A medida que las amenazas cibernéticas evolucionan y los servicios digitales de la Administración Pública se expanden, es crucial contar con un equipo de profesionales altamente capacitados que puedan gestionar, operar y responder de manera eficiente a los retos de la ciberseguridad.

2. **Estructura Organizativa.** Se prevé un incremento de la estructura organizativa de forma paulatina mediante la creación de Subdirecciones Generales y Oficinas para tener una estructura organizativa adecuada a los retos y objetivos enmarcados en el Plan Estratégico.

Beneficios

- Refuerzo y aumento de las **capacidades de los recursos**, disponiendo así de un equipo altamente capacitado con las herramientas y conocimientos necesarios.
- **Incremento de la eficiencia**: La **optimización de los recursos** y la mejora de la organización interna permitirán una **gestión más eficiente** de las operaciones de ciberseguridad.
- **Centralizar la gestión de la ciberseguridad** en la Administración Pública a partir de la creación de la Agencia de Ciberseguridad.
- **Cumplimiento normativo:** garantizar que la Administración Pública cumple con las normativas de seguridad, evitando sanciones y aumentando la confianza de la ciudadanía en los servicios públicos.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M1

Planificación

2025 - 2026

- **Creación de la Agencia de Ciberseguridad**. Se constituirá formalmente la Agencia como entidad pública autonómica especializada en ciberseguridad. Actuará como órgano de referencia para coordinar políticas, capacidades y servicios de protección digital en la Comunidad de Madrid.
- **Aprobación y difusión del Plan Estratégico en los medios**. El Plan Estratégico será aprobado por el órgano competente y difundido públicamente para asegurar su conocimiento, legitimidad y compromiso institucional. La comunicación se apoyará en medios digitales, institucionales y prensa especializada.
- **Dotación de recursos internos**. Se prevé la incorporación inicial de **15 profesionales** con perfiles técnicos, jurídicos y de gestión. Esta dotación permitirá cubrir funciones clave en cumplimiento normativo, operaciones de ciberseguridad y comunicación estratégica.
- Inicialmente se crearán dos Subdirecciones Generales**: Gobierno, Riesgo y Cumplimiento (GRC)** y **Operaciones de Ciberseguridad**. De acuerdo a las necesidades de la Agencia, irá creciendo su estructura, aumentando el número de Subdirecciones Generales.
- Creación de oficinas:
  - Oficina GRC (Cumplimiento Normativo y Riesgos).
  - Oficina de Operaciones de ciberseguridad.
  - Oficina Vigilancia y CSIRT.
  - Oficina de Impulso y Sensibilización.
  - Oficina de Auditoría.

2027

- Aumento de los recursos internos.
- Creación de una nueva Subdirección General (4 SGs en total).
- Incorporación de nuevos perfiles más especializados:
  - Especialista automatización de procesos.
  - Coordinador de Servicios.
  - Analista de Vulnerabilidades.
  - Arquitecto de Seguridad.

2028

- Aumento de los recursos internos.
- Creación una nueva Subdirección (5 SGs en total) especializada en auditoría externa e interna.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M2 Catálogo de servicios

Para garantizar una **oferta integral y coherente de servicios de ciberseguridad**, es fundamental elaborar un catálogo detallado que incluya todas las soluciones y servicios disponibles. Este catálogo será accesible tanto para los organismos de la Administración regional como para las entidades locales, y estará alineado con las mejores prácticas y estándares nacionales e internacionales. Además, el catálogo permitirá reforzar las capacidades de ciberseguridad de cada entidad, adaptándose siempre a la realidad de cada una para brindar una protección eficaz y personalizada.

Al desarrollar un catálogo organizado y accesible, se logrará una mejor gestión operativa, facilitando tanto la toma de decisiones estratégicas como el control y la supervisión de los servicios que forman parte del ecosistema digital de la Administración autonómica madrileña. Además, este catálogo servirá como un referente para la implementación de medidas de mejora continua, contribuyendo a la actualización constante de los servicios, de acuerdo con las necesidades de seguridad y los cambios normativos en el ámbito de la ciberseguridad.

Planificación

2025-2026	→ Establecer un **catálogo de servicios**, en diferentes bloques, para ofrecer la mayor variedad de servicios posible a la ciudadanía, desde asesoramiento en cumplimiento normativo, respuesta a incidentes, monitorización y gestión de amenazas, capacitación y concienciación.
2027	→ **Evolucionar y mejorar** el catálogo de servicios, con el objetivo de promover de forma continua el desarrollo y crecimiento de las capacidades y el alcance de la Agencia.
2028	→ Además de seguir **ampliando el catálogo**, se automatizarán y orquestarán los servicios ofrecidos, integrando todas las capacidades.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

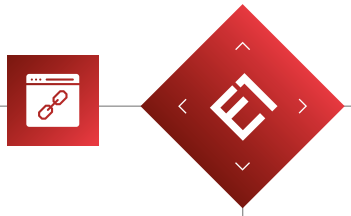
E1.M3 Política y Normativa de Seguridad

Establecer una **política de seguridad** es esencial para proteger la información y los recursos de amenazas internas y externas, garantizando la **confidencialidad, integridad y disponibilidad** de los datos, que son imprescindibles para mantener la confianza de los ciudadanos, entidades locales y organismos de la región.

La implementación de una normativa de seguridad clara y comprensible facilita la **coherencia en la gestión de la ciberseguridad**, proporciona una base sólida para la **evaluación de riesgos** y asegura que las **mejores prácticas** sean seguidas. También permitirá mantener una comunicación clara y constante entre las distintas áreas de la Agencia y otras entidades gubernamentales, contribuyendo a un enfoque integrado y coordinado frente a los desafíos de la ciberseguridad.

En conclusión, la política garantiza que se construya un entorno seguro, y un correcto cumplimiento de normativas y estándares.

01



ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M3

Objetivos

1. **Credibilidad y formación** mediante la certificación de la Agencia en el en el Esquema Nacional de Seguridad (ENS) y la ISO 27001. Estas certificaciones son garantías de que la Agencia implementa las mejores prácticas en la **gestión de la seguridad de la información**, asegurando que los sistemas y servicios digitales cumplen con los más altos estándares de **protección y confianza**.

2. **Cumplimiento normativo**: Garantizar un correcto cumplimiento de las normativas y políticas vigentes en el ámbito de ciberseguridad en la región. El cumplimiento no solo evita sanciones, sino que también establece una **base sólida de confianza** para la ciudadanía y las entidades públicas, demostrando el compromiso de la Agencia con la **seguridad y protección de los datos**.

3. Definición de **políticas y directrices claras**. Estas políticas abarcarán aspectos técnicos, operativos, de gestión y ayudarán a establecer procedimientos estandarizados para la **gestión de riesgos**, la **gestión de incidentes de seguridad** y la **evaluación de vulnerabilidades.**

Beneficios

- **Adaptabilidad y Resiliencia:** Tener normativas y políticas actualizadas permite a la Agencia adaptarse de forma eficaz a nuevas amenazas y vulnerabilidades, aumentando su resiliencia frente a ciberataques.

- **Buena gestión de la seguridad:** Alinear la política con los estándares nacionales e internacionales como el **Esquema Nacional de Seguridad (ENS)** y la **ISO 27001**, mejora significativamente la **gestión de la seguridad** dentro de la organización.

- **Reducción de riesgos:** Políticas actualizadas permiten anticiparse a posibles amenazas y reducir el impacto de los incidentes de ciberseguridad. Al contar con procedimientos preventivos bien definidos, la Agencia puede identificar, evaluar y mitigar riesgos de forma **proactiva**, reduciendo significativamente el impacto de posibles **incidentes de ciberseguridad**. Este enfoque no solo mejora la **capacidad de respuesta**, sino que también contribuye a **disminuir la exposición a riesgos** de seguridad.

- **Concienciación y formación** en ciberseguridad para los empleados públicos de la Comunidad de Madrid. Un beneficio clave de contar con **políticas y normativas claras es la concienciación y formación** continua.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M3

Planificación

2025 - 2026

- Aprobación de la **Política Global de Seguridad de la Información por el Consejo de Gobierno**.
- Establecer las **normas y directrices** de la Agencia de Ciberseguridad de la Comunidad de Madrid que regirán su actuación. Estas normas incluirán procedimientos específicos de seguridad, roles y responsabilidades del personal, mecanismos de control y auditoría, y protocolos a seguir en situaciones de crisis o ciberincidentes.
- Aprobación y presentación del informe anual de la **estrategia global de Seguridad de la Información de la Comunidad de Madrid**.
- Elaborar el **Libro Blanco** de la ciberseguridad que ofrezca buenas propuestas de acción y buenas prácticas sobre su gestión y ofrezca confianza a todos los actores políticos, económicos y sociales del ecosistema digital madrileño en sus relaciones con la Comunidad de Madrid.
- Certificación de la Agencia en el año 2026 en el **ENS** (Esquema Nacional de Seguridad), con **nivel MEDIO**, asegurando así que cumple con las normas de seguridad nacionales en la protección de los sistemas de información y en la **ISO/IEC 27001,** normativa internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI).

2027

- **Revisión periódica** de las normas y procedimientos definidos, con el objetivo de asegurar un cumplimiento correcto de las normativas vigentes y una adaptación a cualquier cambio en el ámbito de la ciberseguridad.

2028

- Certificación de la Agencia en **ENS nivel ALTO**.
- **Revisión periódica** de las normas y procedimientos definidos, con el objetivo de asegurar un cumplimiento correcto de las normativas vigentes y una adaptación a cualquier cambio en el ámbito de la ciberseguridad.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M4 Servicio de Asesoramiento en Ciberseguridad y Normativo

Establecer un **Servicio de Asesoramiento en Ciberseguridad y Normativo** para garantizar que las entidades locales y los organismos de la región puedan desarrollar un plan de acción efectivo. Este servicio permitirá reforzar la ciberseguridad, establecer un gobierno adecuado de la misma y asegurar el cumplimiento de las normativas vigentes.

El **servicio** estará estrechamente relacionado con varios planes clave de la Agencia, los cuales permitirán que las entidades locales, organismos públicos, ciudadanos y PYMES puedan recibir apoyo integral en aspectos tanto técnicos como normativos.

De esta forma, el asesoramiento ofrecido será clave para contribuir a la resolución de problemas técnicos, así como a la integración del cumplimiento normativo en todas las actividades relacionadas con la ciberseguridad.

Objetivos

1. Respaldar el **cumplimiento normativo y legal:** El asesoramiento ayuda a un correcto cumplimiento de normativas y políticas.
2. Ofrecer **información y soporte técnico** sobre la arquitectura y soluciones de ciberseguridad dependiendo de las necesidades.
3. Prevenir las **sanciones y gestionar los riesgos legales**.

Beneficios

- **Aumento de la seguridad** y protección en los sistemas y datos.
- **Cumplimiento normativo:** A través del asesoramiento sobre diferentes aspectos en ciberseguridad, esto facilitará que se cumpla con la normativa vigente.
- **Diseños robustos y eficientes:** Conocer la arquitectura de seguridad, ayuda a desarrollar diseños robustos y eficientes que cumplan con los principios de ciberseguridad.
- **Reducción de riesgos, vulnerabilidades y sanciones.** El asesoramiento permitirá a las entidades y organismos gestionar el cumplimiento normativo de manera adecuada previniendo la posibilidad de incurrir en incumplimiento y por lo tanto en una sanción. Adicionalmente, el asesoramiento permitirá establecer un mejor gobierno de la seguridad y por lo tanto una mejor gestión de riesgos.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M4

Planificación

2025 - 2026

- Asesoría técnica de **arquitectura de seguridad, infraestructura y desarrollo.** Este aspecto se centrará en ofrecer orientación experta sobre cómo diseñar, implementar y gestionar infraestructuras tecnológicas seguras.
- Asesoría sobre **cumplimiento legal de las normativas** como el Reglamento General de Protección de Datos (GDPR), el anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, el Esquema Nacional de Seguridad (ENS), y otros marcos normativos nacionales e internacionales.

2027 - 2028

- Continuar **prestando el servicio** para todas las Entidades, garantizando que tengan acceso a una asistencia y orientación eficaz sobre normativa, arquitectura de ciberseguridad y asesoramiento legal.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M5 Definir el modelo de Gobernanza de Ciberseguridad

La **Gobernanza de ciberseguridad** es esencial para garantizar que las estrategias, políticas y prácticas relacionadas con la protección de los sistemas y datos sean efectivas y estén alineadas con los objetivos organizacionales.

La creación de un modelo adecuado garantiza la alineación de estos objetivos de ciberseguridad con los objetivos estratégicos de la Agencia, estableciendo un marco que permite operar de forma transparente y coordinada.

La gobernanza de la ciberseguridad en la región se articulará a través del **Comité de Seguridad de la Información** de la Comunidad de Madrid, dependiente de la Agencia de Ciberseguridad, que actúa como órgano colegiado de referencia para la coordinación y supervisión de la ciberseguridad en el sector público madrileño.

El modelo planteado por la Agencia estará basado en principios de **transparencia**, **responsabilidad, eficacia y coordinación** y se apoyará en el enfoque de **tres líneas de defensa**, un marco probado que permite una gestión y un control claros de los riesgos cibernéticos. Dentro de este modelo, será fundamental **diseñar un mapa relacional de *stakeholders*** que identifique a todos los actores clave involucrados en la ciberseguridad.

Además, otro punto clave del modelo será el establecimiento de un **foro de expertos** con responsables de seguridad del sector privado. Esta acción estratégica fomentará la colaboración público - privada.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M5

Objetivos

1. Establecer una **estructura sólida** de gobernanza, basada en tres líneas de defensa que distribuirán las funciones según el nivel de supervisión y control.

2. Gobernar la ciberseguridad en el sector público de la región a través del **Comité de Seguridad de la Información**

3. Fomentar la **colaboración estratégica con el sector privado.** Estas colaboraciones permitirán el intercambio de mejores prácticas, recursos y soluciones innovadoras, además de facilitar el acceso a conocimientos técnicos avanzados.

4. Impulsar la **cooperación interregional** en ciberseguridad para enfrentar los desafíos de ciberseguridad a gran escala.

5. Fortalecer la **gestión de riesgos** en ciberseguridad, con el fin de reducir la vulnerabilidad de los sistemas críticos.

6. **Integrar competencias** en ciberseguridad, con el fin de optimizar la utilización de los recursos y mejorar la eficiencia operativa.

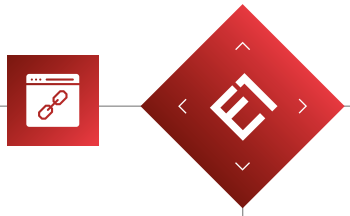
Beneficios

- Mejora de la **coordinación y la comunicación** entre los diferentes actores involucrados (empresas, organismos gubernamentales, Comunidades Autónomas...), facilitando una comunicación más fluida y eficaz entre ellos.

- Fortalecimiento de la **seguridad empresarial:** La cooperación con las empresas representa una oportunidad única para fortalecer la seguridad empresarial.

- **Aumento de la resiliencia** de la Agencia tras implementar un modelo basado en tres líneas de defensa, fortaleciendo la capacidad de la Agencia para identificar, gestionar y mitigar los riesgos cibernéticos de manera más eficiente.

01



ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M5

Planificación

2025 - 2026

- Crear el **Comité de Seguridad de la Información** y celebrar su primer pleno, dando cumplimiento a las obligaciones establecidas por el ENS y NIS2 para abordar los retos de ciberseguridad de la región.
- Implementar un **modelo de gobernanza** basado en **tres líneas de defensa**. La primera la componen las funciones que poseen y gestionan los riesgos (como medidas básicas de seguridad); la segunda corresponde a las funciones de control independientes que supervisan y monitorean la gestión de riesgos de la primera y la tercera se centra en la auditoría interna.
- Diseñar un **mapa relacional de *stakeholders***. Este mapa incluirá una clasificación de los *stakeholders* según su nivel de influencia y responsabilidad en la ciberseguridad, así como sus interacciones y dependencias. Además, se definirán los roles y responsabilidades de cada *stakeholder*, estableciendo mecanismos de comunicación y colaboración para asegurar una coordinación efectiva.
- Establecer un **modelo eficiente de relación y coordinación** entre los organismos que conforman el ecosistema.
- Iniciar el proceso de **integración de las competencias en Ciberseguridad** entre la Consejería de Digitalización, otros organismos y la Agencia de Ciberseguridad.

2027

- Establecer **un Comité de Expertos** con empresas de la Comunidad de Madrid para fomentar la colaboración público-privada.
- Crear una ***Red de Trabajo*** con las Comunidades Autónomas para fortalecer la cooperación interregional.
- Continuar con el proceso **proceso de integración** de las competencias acorde a la planificación.
- Celebrar el pleno del **Comité de Seguridad de la Información** para abordar los retos de ciberseguridad de la región.

2028

- Colaborar de forma activa con **organismos de supervisión** europeos.
- Continuar con el **proceso de integración** de las competencias acorde a la planificación.
- Celebrar el pleno del **Comité de Seguridad de la Información** para abordar los retos de ciberseguridad de la región.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M6 Establecer una línea base de Ciberseguridad

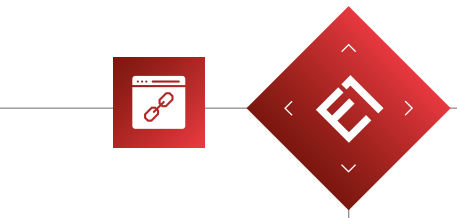
La **línea base de Ciberseguridad** es una referencia donde se define un conjunto mínimo de requisitos, controles y procedimientos para evaluar el nivel de madurez en ciberseguridad.

Esta línea base proporcionará un marco común para medir el nivel de seguridad de las entidades y permitir la implementación de controles adecuados en función de su **nivel de criticidad.** Para ello, primero se clasificará a las entidades en tres niveles: crítico, importante y esencial, asegurando que aquellas de mayor criticidad reciban una mayor protección, acorde con los riesgos y el impacto que supondría un ciberataque. Tras su clasificación, se establecerá una **línea base de ciberseguridad** adaptada a cada nivel de criticidad, lo que permitirá crear políticas y medidas de protección personalizadas y más efectivas.

La implementación de un **sistema de métricas** será clave para evaluar el nivel de madurez de las entidades en cuanto a ciberseguridad, permitiendo un seguimiento constante del cumplimiento de las medidas de protección establecidas.

Además, se desarrollará un **Cuadro de Mando** que centralice la información de todos los sistemas de seguridad, proporcionando una visión consolidada de la situación de ciberseguridad en la región.

01



ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M6

Objetivos

1. Implementar un **sistema de métricas** para evaluar niveles de madurez en ciberseguridad de forma continua y precisa.

2. Generar **reportes periódicos** para adaptarse a posibles nuevas amenazas y realizar un seguimiento de los requisitos normativos, empleándolos como herramientas esenciales para garantizar que las entidades locales y organismos estén preparados frente a nuevas amenazas, vulnerabilidades y riesgos, así como a los cambios en la normativa.

3. Garantizar que cada entidad tenga los **controles mínimos** necesarios para su protección para asegurar la seguridad de los sistemas y servicios.

Beneficios

- **Protección:** Al establecerse requisitos mínimos de seguridad, disminuyen los riesgos de incidentes de ciberseguridad, así como posibles vulnerabilidades y la exposición a nuevas amenazas.

- **Estandarización** de prácticas y controles de seguridad. Al definir y aplicar una línea base de ciberseguridad adaptada a la clasificación de las entidades, se establece un conjunto claro de prácticas y controles de seguridad que deben seguir todas las entidades.

- **Facilitación de auditorías:** Simplificación en la realización de evaluaciones y auditorías al estar definido un sistema de métricas y un conjunto de controles establecidos.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M6

Planificación

2025 - 2026

- **Clasificar** las entidades por **nivel de criticidad**: crítico, importante y esencial. El **crítico** incluye a aquellas entidades cuya operatividad es fundamental para la estabilidad económica y social, así como la prestación de servicios básicos a la ciudadanía. El **esencial** implica aquellas entidades que desempeñan funciones clave y que, aunque no son críticos, son importantes para el funcionamiento de la sociedad. El **importante** incluye aquellas entidades cuyo funcionamiento es relevante, y que tienen un impacto significativo en la sociedad.
- Establecer **una línea base de ciberseguridad** adaptada a la clasificación de las entidades.
- Implementar un **sistema de métricas** para evaluar el nivel de madurez.
- Establecer un Cuadro de Mando que proporcione una **visión consolidada** de todas las métricas.
- Generar **reportes periódicos** sobre el estado de la ciberseguridad.
- Implementar en la Agencia para el año 2026 un **Sistema de Gestión de Seguridad de la Información (SGSI)**.

2027

- Actualizar la **línea base de ciberseguridad** y del **sistema de métricas**.
- Solicitar información periódica sobre los **indicadores de ciberseguridad.**
- **Integrar y consolidar** la información que facilite tener una visión completa y coherente del estado de la ciberseguridad.
- Elaborar **reportes detallados** sobre el estado de la ciberseguridad, proporcionando una visión clara y actualizada de los niveles de protección, vulnerabilidades detectadas y medidas implementadas.

2028

- Realizar una **automatización de los reportes** para informar a las partes interesadas.
- **Evolucionar** los indicadores acorde al análisis de situación del año 2028
- **Publicar informes** del estado de Ciberseguridad de la Comunidad de Madrid.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M7 Adherirse al distintivo complementario de Ciberseguridad

La Agencia ha definido, en colaboración con **Madrid Excelente**, un **distintivo complementario de Ciberseguridad** que servirá como un sello de calidad para reconocer a aquellas empresas en la región que cumplan con altos estándares de seguridad en la protección de la información y los sistemas digitales.

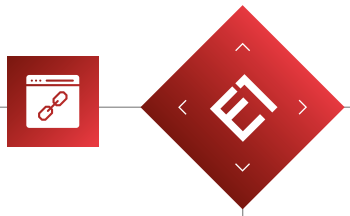
Este distintivo fomentará la mejora continua en la gestión de la ciberseguridad, incentivando la adopción de buenas prácticas, normativas y certificaciones reconocidas.

Otorgar dicho reconocimiento mediante un distintivo de ciberseguridad contribuirá a generar confianza entre la ciudadanía, posicionando a la Comunidad de Madrid como un referente en la protección digital.

Este distintivo de calidad se denominará ***Lugar Ciberseguro*** y forma parte de una iniciativa que no solo promueve buenas prácticas en ciberseguridad para las empresas, sino que también se extiende a los municipios. Además, se desarrollará un **esquema de certificación** que permitirá tanto a empresas como a entidades locales demostrar su compromiso con la ciberseguridad, garantizando el cumplimiento de los estándares establecidos.

Este distintivo es un reconocimiento adicional, anexo al sello de Madrid Excelente, pero en ningun caso sustituirá las certificaciones oficiales como el ENS, la ISO 27001 o la Directiva NIS2.

01



ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M7

Objetivos

1. Impulsar una **transformación digital segura.** El distintivo de *Lugar Ciberseguro* busca garantizar que la adopción de tecnologías digitales se realice bajo estándares adecuados de seguridad, minimizando vulnerabilidades y protegiendo la integridad de la información.

2. Establecer un **control** en el ámbito de la ciberseguridad, a través de auditorías, revisiones periódicas y un marco de certificación basado en estándares reconocidos.

3. Desarrollar un **distintivo de Ciberseguridad** que reconozca el compromiso de las empresas en la ciberseguridad.

4. Promover la **confianza digital y la competitividad** en el ecosistema empresarial de Madrid. Las empresas que cuenten con el distintivo podrán aprovechar este reconocimiento como un valor diferencial.

Beneficios

- **Ventaja competitiva:** Diferenciación de las empresas en el mercado al tener un sello de calidad reconocido en el ámbito de la ciberseguridad.

- **Reconocimiento y prestigio:** Las empresas con este sello demostrarán compromiso con la ciberseguridad. Este reconocimiento fortalecerá la reputación corporativa y favorecerá su imagen ante organismos públicos, entidades privadas y clientes, impulsando la captación de nuevos negocios y alianzas estratégicas.

- **Confianza de la ciudadanía:** Un distintivo que aumenta la confianza de la ciudadanía en las organizaciones y empresas certificadas.

- **Fomento de la cultura de ciberseguridad en el tejido empresarial.** La creación y adopción del sello ***Lugar Ciberseguro*** incentivará a las empresas a mejorar continuamente sus estrategias de ciberseguridad.

01

ESTABLECER UN MODELO DE GOBERNANZA Y CONTROL DE CIBERSEGURIDAD

E1.M7

Planificación

2025 - 2026

- Definir los requisitos de ciberseguridad para el distintivo ***Lugar Ciberseguro***.
- Diseñar un **esquema de certificación** para obtener el distintivo de ***Lugar Ciberseguro*** y que esté diferenciado por niveles para empresas, PYMES (Pequeñas y Medianas empresas), instituciones que cumplan con los estándares de ciberseguridad. Se desarrollará un **modelo de certificación estructurado** con criterios técnicos y normativos alineados con estándares nacionales e internacionales de ciberseguridad. Este esquema incluirá requisitos, niveles de certificación y procedimientos de auditoría que las empresas deberán cumplir para obtener y mantener el sello.
- Conseguir que las empresas de la región se certifiquen con el distintivo.
- **Publicación de la guía oficial *Lugar Ciberseguro*** para entidades privadas de la Comunidad de Madrid y creación de un registro público de entidades certificadas.
- Promocionar el distintivo de *Lugar Ciberseguro* en la Comunidad de Madrid.

2027

- Alcanzar la certificación de un conjunto de **empresas** para que cumpla con los criterios establecidos.
- Garantizar la mejora continua con el **mantenimiento de los distintivos** previamente otorgados. Se establecerán **mecanismos de seguimiento y renovación** para asegurar que las empresas mantengan los estándares exigidos.

2028

- Alcanzar los criterios establecidos para un volumen significativo de **empresas**.
- Garantizar la mejora continua con el **mantenimiento de las certificaciones** previamente otorgadas. Se establecerán **mecanismos de seguimiento y renovación** para asegurar que las empresas certificadas mantengan los estándares exigidos.
- Incluir nuevos requerimientos de ciberseguridad para cada uno de los niveles del distintivo ***Lugar Ciberseguro***.

02

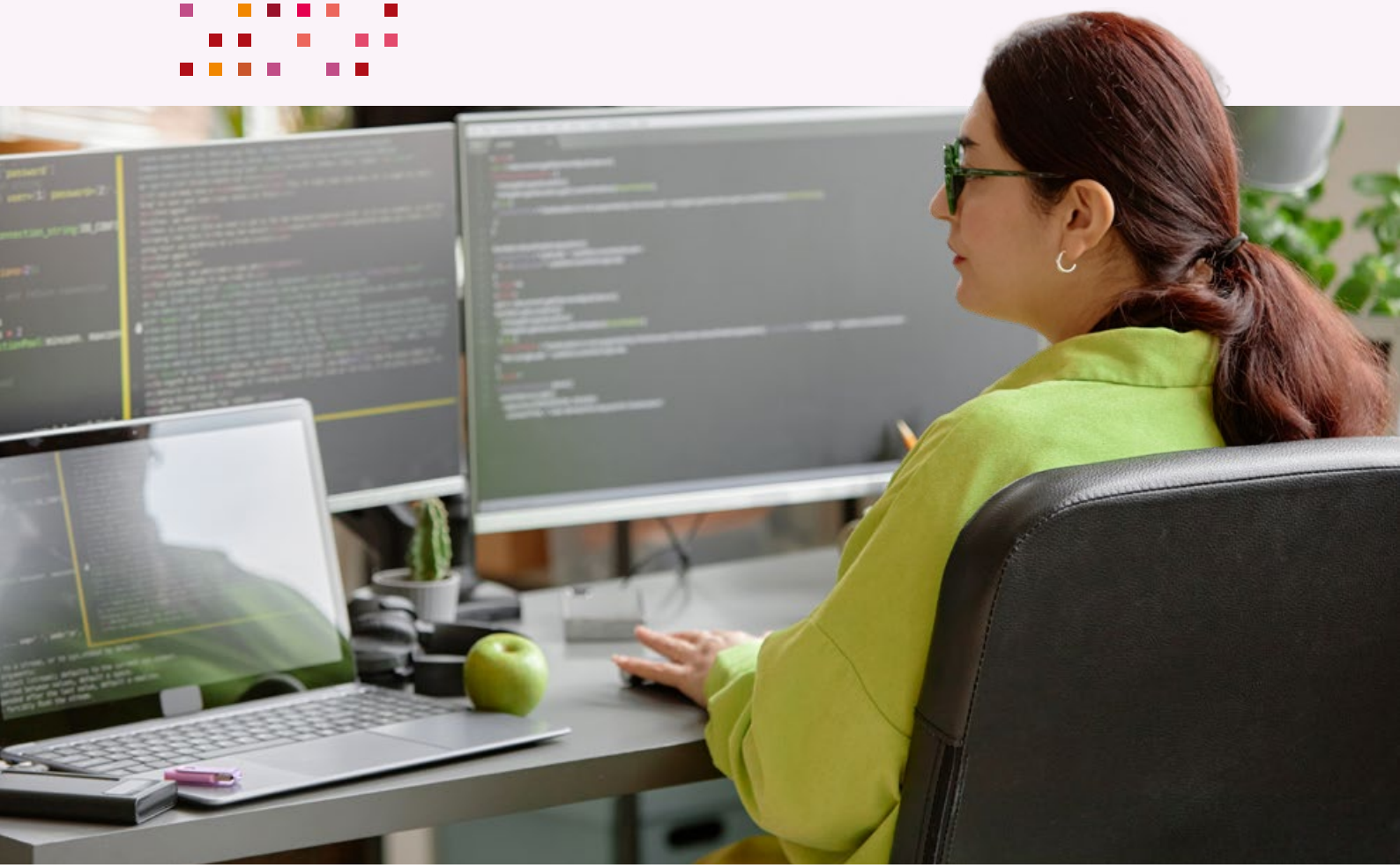
E2

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

Resumen

El **cumplimiento normativo** en ciberseguridad es un pilar fundamental para la protección de los sistemas y redes que soportan los servicios digitales. Por este motivo, es importante que los equipos responsables de la seguridad de las distintas entidades y organismos cuenten con el conocimiento y herramientas necesarias para adaptar sus estrategias a los requisitos y exigencias de la legislación.

En el presente eje estratégico se establecerán las medidas, procedimientos y mecanismos necesarios para que todas las organizaciones de la Administración autonómica madrileña cumplan con los marcos normativos como el **ENS o el anteproyecto de Ley de la NIS2,** garantizando la implementación efectiva de medidas de seguridad. Para ello, se definirán procesos de auditorías exhaustivas, en los que se llevarán a cabo revisiones técnicas, análisis de riesgos, evaluación de políticas y procedimientos y verificación de la adopción de las medidas de seguridad adecuadas.



02

E2

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E2.M1 Elaboración de la Estrategia de certificación para los servicios ofrecidos a los ciudadanos

A través de una **Estrategia de certificación** para los servicios ofrecidos a los ciudadanos, se garantizará un cumplimiento de los estándares de ciberseguridad establecidos, proporcionando un aumento en la protección y confianza en el uso de servicios de este ámbito.

Esta estrategia asegurará que las plataformas y sistemas que prestan servicios esenciales a la ciudadanía cuenten con los niveles adecuados de seguridad, minimizando riesgos y fortaleciendo la protección de la información.

Para ello, se definirán requisitos específicos de certificación basados en marcos normativos y prácticas nacionales e internacionales, asegurando que las soluciones tecnológicas cumplan con criterios de seguridad, disponibilidad e integridad.

Objetivos

1. Diseñar un **sistema de certificación** que garantice seguridad y calidad de los servicios digitales dirigidos a la ciudadanía, identificando y definiendo las normativas aplicables. Se definirá un marco de certificación basado en los estándares nacionales e internacionales más importantes, eficiente a los retos de la ciberseguridad.

2. Asegurar **transparencia y confianza** en los servicios digitales.

3. Incrementar de forma progresiva los **niveles de certificación** de diferentes tipos de entidades.

Beneficios

- **Cumplimiento normativo y alineación con estándares de ciberseguridad**: a través de las certificaciones se asegura el cumplimiento de normativas y estándares, como el Cyber Resilience Act (CRA), la Directiva NIS2 y el Esquema Nacional de Seguridad (ENS).

- Más **protección** en los datos de los ciudadanos. Se fomentará el uso de mecanismos de protección como cifrado, autenticación robusta y otras medidas enfocadas a garantizar la integridad y confidencialidad de los datos.

- **Mejora y fortalecimiento en la confianza digital**: los ciudadanos tendrán acceso a servicios confiables y protegidos.

02

E2

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

E2.M1

Planificación

2025 - 2026

- Identificar las **normativas de aplicación y estrategia de certificación**.
- **Publicar guías de la Agencia** para ayudar a las Entidades Locales **(EELL)** a certificarse en el Esquema Nacional de Seguridad **(ENS)**. Estas guías se diseñarán para proporcionar directrices claras y prácticas a las entidades, con el objetivo de que cumplan con los requisitos de ciberseguridad establecidos.
- Elaborar el **Plan Anual de Certificaciones** de los servicios ofrecidos al ciudadano. El Esquema Nacional de Seguridad define tres niveles de seguridad: **bajo**, cuando las consecuencias de un incidente de seguridad suponen un perjuicio limitado, **medio** cuando las consecuencias del incidente suponen un perjuicio grave y **alto** cuando las consecuencias ocasionen un perjuicio muy grave.
  En el **Plan Anual de Certificaciones**, como mínimo, se deberán adscribir a los siguientes niveles:
  - **Agencia:** Certificación ENS nivel medio e ISO 27001 para el año 2026.
  - **Entidades Críticas:** Certificación ENS nivel medio.
  - **Entidades esenciales (Ayto.>20k)**: Certificación ENS nivel bajo.
  - **Entidades importantes (Ayto.<20k)**: μCeENS bajo.

2027

- Elaborar el **Plan Anual de Certificaciones** de los servicios ofrecidos al ciudadano, como **mínimo**:
  - **Entidades esenciales (Ayto. >20k)**: Certificación ENS nivel medio.
  - **Entidades importantes (Ayto. <20k)**: Certificación ENS nivel bajo.

2028

- Elaborar el **Plan Anual de Certificaciones** de los servicios ofrecidos al ciudadano, como **mínimo**:
  - **Agencia:** Certificación ENS nivel alto.
  - **Entidades Críticas**: Certificación ENS nivel alto.
  - **Entidades esenciales (Ayto. >20k)**: Certificación ENS nivel medio.
  - **Entidades importantes (Ayto. <20k)**: Certificación ENS nivel medio.

02

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

E2.M2 Realización de Auditorías para garantizar el cumplimiento

Para garantizar la protección y seguridad de los servicios digitales, así como la confianza de la ciudadanía, es imprescindible realizar **auditorías periódicas que evalúen el grado de cumplimiento de la legislación.**

Estas auditorías permitirán identificar brechas de seguridad, posibles amenazas y vulnerabilidades, evaluar el nivel de madurez en la implementación de controles y garantizar el cumplimiento de los requisitos legislativos, tanto nacionales como internacionales.

El proceso de auditoría consistirá en evaluaciones técnicas, análisis de riesgos, evaluación de procedimientos y políticas, comprobación de las medidas implementadas, así como evaluaciones periódicas que permitan asegurar un control y mejora continua.

Objetivos

1. Revisión del **cumplimiento** de la legislación mediante auditorías para asegurar que las entidades cumplen con las normativas de ciberseguridad vigentes, incluyendo el **Esquema Nacional de Seguridad**, la **ISO 27001**, la **Directiva NIS2,** la **Directiva CER** y otros marcos regulatorios aplicables.

2. Identificar **vulnerabilidades y riesgos** en la implementación de medidas de seguridad. A través de los procesos de auditoría, se analizarán las infraestructuras tecnológicas, los procedimientos de seguridad y las prácticas operativas para detectar **posibles vulnerabilidades y riesgos**.

3. Garantizar la **mejora continua** de la ciberseguridad mediante la implementación de un sistema integral de monitoreo y evaluación donde se revisarán y actualizarán regularmente las políticas y procedimientos de ciberseguridad para asegurarse de que estén alineados con las mejores prácticas y las normativas vigentes.

Beneficios

- Refuerzo del **cumplimiento normativo.**
- **DIsminución de incidentes de ciberseguridad:** detección temprana de vulnerabilidades o riesgos en las auditorías.
- **Fortalecimiento de la confianza** en los servicios.

02

E2

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

E2.M2

Planificación

2025 - 2026

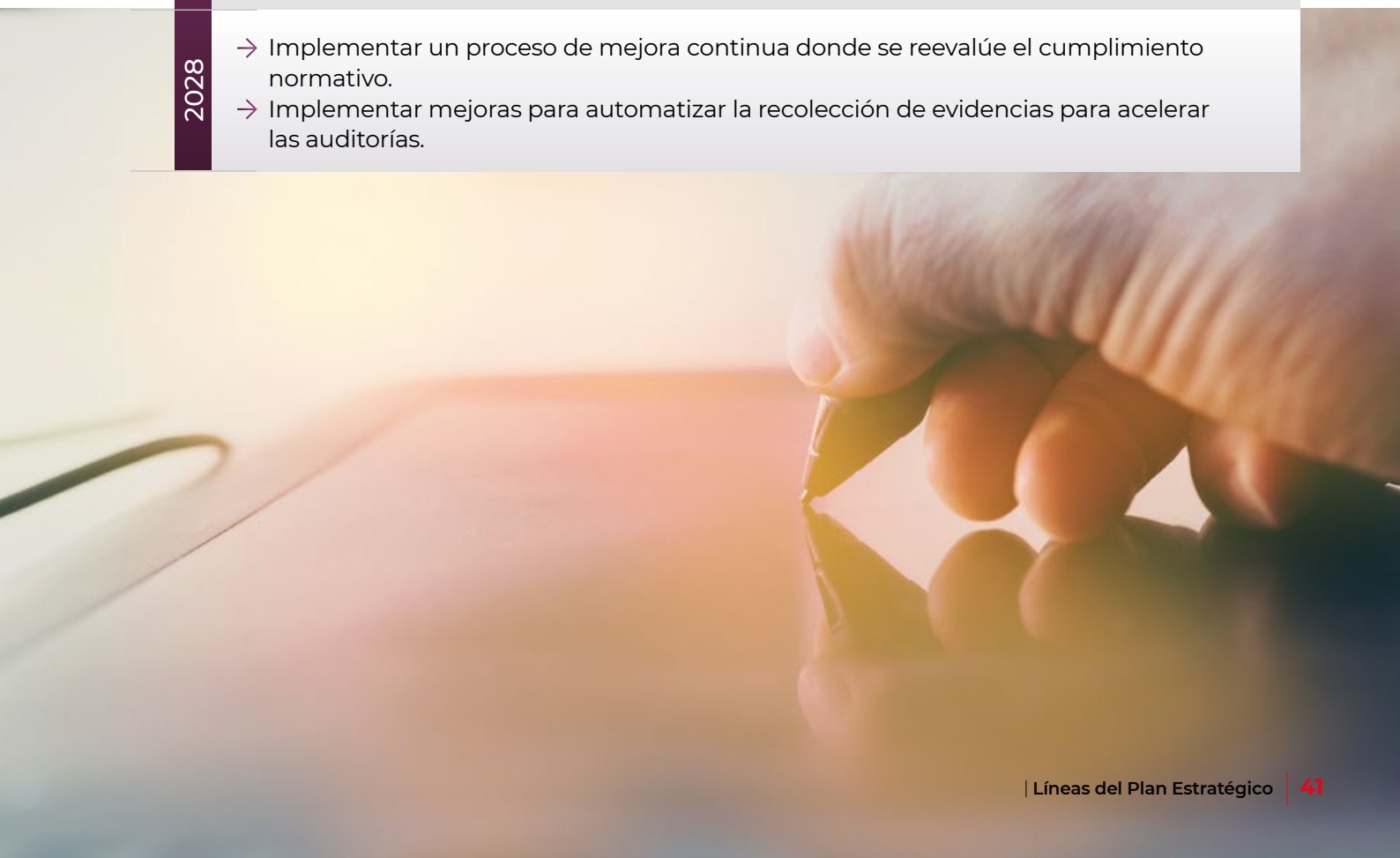
- Realizar un análisis del **nivel de madurez** y los servicios operativos. El análisis se centrará en estudiar cómo evolucionan los procesos, tecnologías y recursos, para identificar posibles áreas a mejorar, así como oportunidades para aumentar la eficiencia y efectividad.
- Realizar **auditorías periódicas** para garantizar el nivel de cumplimiento de los controles y de la legislación aplicable, como el **Esquema Nacional de Seguridad**, la **ISO 27001**, la **Directiva NIS2** y la **CER**. Estas auditorías permiten evaluar de forma continua que se implementan las medidas correctivas y de seguridad convenientes.

2027

- Realizar un análisis del **nivel de madurez** y los servicios operativos.
- Realizar **auditorías periódicas** el nivel de cumplimiento de los controles y de la legislación aplicable (ENS, ISO 27001, NIS2, etc.).

2028

- Implementar un proceso de mejora continua donde se reevalúe el cumplimiento normativo.
- Implementar mejoras para automatizar la recolección de evidencias para acelerar las auditorías.



02

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

E2.M3 Apoyo en el proceso de certificación

La Agencia de Ciberseguridad de la Comunidad de Madrid proporcionará soporte especializado a las entidades durante las auditorías de certificación, asegurándose así de que cumplen con los estándares y criterios de ciberseguridad establecidos. Además, se encargará de **proporcionar herramientas durante las auditorías** para facilitar el proceso y mejorar la eficiencia. Con el objetivo de **aumentar la tasa de certificación en la región**, la agencia implementará estrategias específicas y ofrecerá recursos adicionales a las entidades. Finalmente, se realizará un **seguimiento periódico para garantizar un nivel continuo de calidad y cumplimiento normativo**, asegurando que las entidades mantengan los estándares requeridos a lo largo del tiempo.

Objetivos

1. **Asistir y ayudar** a las entidades en la preparación y cumplimiento de los requisitos necesarios para superar los procesos de certificación.
2. Proporcionar **herramientas y asesoramiento** durante las auditorías.
3. Identificar cuáles son los **problemas** más comunes que surgen durante las certificaciones.

Beneficios

- **Aumento en la tasa de certificación:** El apoyo en el proceso de certificación implica que más entidades puedan cumplir con los requisitos de la normativa y obtengan la certificación.
- **Cumplimiento normativo asegurado:** Ayuda a las entidades a operar dentro del marco regulador vigente.
- **Optimización constante:** Implementación continua de mejoras basadas en observaciones identificadas.

02

E2

GARANTIZAR EL CUMPLIMIENTO EFECTIVO DE LA LEGISLACIÓN APLICABLE

E2.M3

Planificación

2025 - 2026

- Elaborar un **plan de auditorías** priorizado en función de la criticidad de cada organismo, así como de otros criterios relevantes que permitan identificar el nivel de madurez en ciberseguridad.
- Crear una metodología que genere un impacto mínimo en la operativa de la entidad durante las auditorías.
- Crear un repositorio de evidencias común con todas las entidades para las auditorías.

2027

- Realizar un **seguimiento periódico** de las recomendaciones y hallazgos detectados, con el que se garantiza un nivel continuo de calidad y cumplimiento normativo.
- Preparar los **temas más recurrentes detectados** en el proceso de certificación para poder identificarlos, estudiarlos y desarrollar estrategias para poder actuar ante ellos y resolverlos de forma eficaz.
- Proporcionar **soporte especializado** durante las auditorías de certificación que consista en ofrecer asesoramiento técnico y operativo a lo largo del proceso de evaluación, asegurando que la entidad cumple con los requisitos establecidos.

2028

- Mejorar el proceso de auditoría automatizando, en la medida de lo posible, la recolección de evidencias para todas las normativas en alcance.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

Resumen

Desplegar un **Escudo Digital** integral que fortalezca la protección, optimice la detección y garantice una respuesta efectiva frente a amenazas, abarcando todas las entidades de la Comunidad de Madrid.

Este eje estratégico tiene como objetivo fortalecer las capacidades de prevención y detección. Para ello se enfoca principalmente en el despliegue de un Escudo Digital integral que abarca a todas las entidades públicas de la Comunidad de Madrid.

03

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E3.M1 Soporte en la definición de la arquitectura de Seguridad

La creación de una **arquitectura de seguridad sólida y coherente,** que sirva para detectar en segundos y remediar en minutos, con el objetivo de proteger es esencial para proteger las infraestructuras digitales de la Comunidad de Madrid frente a las crecientes amenazas cibernéticas.

Además, se brindará **asesoramiento experto** a las entidades en aspectos clave, como la selección de fabricantes, la instalación y configuración de los componentes de hardware y software necesarios, asegurando una implementación eficaz y alineada con los objetivos de seguridad establecidos. Con este enfoque, se busca optimizar los recursos y garantizar la protección continua de los servicios esenciales de la Comunidad de Madrid.

Objetivos

1. Establecer un **modelo de arquitectura de seguridad** alineado con normativas y estándares nacionales e internacionales (ISO 27001, NIST, ENS, etc.).

2. Desarrollar una **hoja de ruta** para la implementación del modelo de arquitectura de seguridad en los organismos de la administración de la región.

3. Dar soporte en el Diseño de un modelo de seguridad perimetral y de acceso basado en el principio de **Zero Trust**.

4. **Integrar soluciones de seguridad** como Security Information and Event Management (SIEM), Security Operations Center (SOC) y plataformas de respuesta ante incidentes.

5. Definir un **modelo de interoperabilidad** y compatibilidad entre herramientas de seguridad.

6. Promover que se apliquen **metodologías DevSecOps** para garantizar la seguridad en entornos de desarrollo.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M1

Planificación

2025 - 2026

- Definición de los requerimientos de **arquitectura de seguridad** en las entidades de la Comunidad de Madrid para establecer unas mínimas medidas de seguridad. Los requerimientos de arquitectura de seguridad incluyen, entre otros aspectos, la protección de datos sensibles, la autenticación y control de acceso, la monitorización de redes, la gestión de incidentes de seguridad, y la resiliencia ante ataques.
- **Aprobación de la arquitectura de seguridad** integrada en el Escudo Digital.

2027

- **Asesoramiento** a las entidades en la selección de la solución que mejor se adapte a sus requerimientos, asegurando que cumpla con los estándares de seguridad requeridos. Además, se ofrece asesoramiento para una correcta **instalación y configuración** de los distintos elementos de hardware y software en la arquitectura.

2028

- **Acompañamiento** en el desarrollo de la **arquitectura de seguridad** de las entidades locales para la evolución y mejora de sus sistemas.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M2

Implementación del puesto ciberseguro

La implementación de un **puesto ciberseguro** es una estrategia fundamental para garantizar que los entornos de trabajo sean resistentes a las amenazas cibernéticas.

El puesto ciberseguro se refiere a la integración de medidas de seguridad en el espacio de trabajo digital, asegurando que cada dispositivo, red y aplicación utilizados por los empleados estén adecuadamente protegidos contra posibles vulnerabilidades. Este enfoque abarca diversas áreas, desde la **configuración segura de equipos de trabajo**, hasta la **gestión de accesos** y la **protección de datos personales**.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M2

Objetivos

1. Fortalecer la **seguridad de los puestos de trabajo**. Implementar medidas de seguridad en los dispositivos de los empleados para reducir el riesgo de accesos no autorizados, malware y otras amenazas cibernéticas.

2. **Establecer políticas de acceso y autenticación robustas**. Implementar sistemas de autenticación multifactor (MFA) y políticas de acceso restringido para evitar el acceso no autorizado.

3. **Implementar herramientas de detección y prevención de amenazas**. Desplegar soluciones de ciberseguridad avanzadas, como antivirus, firewalls y sistemas de detección de intrusiones (IDS), para monitorear y proteger de manera proactiva los dispositivos de trabajo.

4. **Garantizar la actualización constante de los sistemas operativos y aplicaciones**. Establecer procesos automáticos o manuales para asegurar que todos los dispositivos de los empleados se mantengan actualizados con los últimos parches de seguridad.

5. **Fomentar el uso de herramientas seguras para la colaboración y comunicación**. Asegurar que las plataformas y aplicaciones de colaboración utilizadas por los empleados sean seguras, incluyendo la implementación de medidas de cifrado y autenticación.

Beneficios

- **Reducción de riesgos.** Minimiza las vulnerabilidades de los dispositivos al tener implementadas medidas de seguridad.

- **Mayor protección de la información sensible.** Asegura la integridad, confidencialidad y disponibilidad de los datos.

- **Mejora de la productividad.** Al contar con un entorno de trabajo seguro, los empleados pueden concentrarse en sus tareas sin preocuparse por posibles amenazas cibernéticas, lo que aumenta su eficiencia y rendimiento.

- **Aumento de la confianza de los clientes y socios.** Las empresas que implementan medidas de seguridad avanzadas en sus puestos de trabajo generan confianza entre los clientes y socios, demostrando un compromiso con la protección de los datos y la seguridad digital.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M2

Planificación

2025 - 2026

- Implementar el **puesto ciberseguro**, que integra soluciones como:
  - Protección avanzada de **puestos de trabajo** (EDR) mediante la monitorización continua y la respuesta a amenazas de manera inmediata.
  - Automatización del **análisis de vulnerabilidades** que **integre** herramientas avanzadas de escaneo, evaluación de riesgos y generación de informes, con capacidad para realizar análisis continuos y programados, priorizar vulnerabilidades según su impacto y proporcionar recomendaciones de mitigación en tiempo real.
  - Simulación de **pentesting automático** (pruebas de penetración automáticas), con el objetivo de evaluar la resistencia de los sistemas y redes frente a ciberataques, mediante la simulación de dichos ataques.
  - Realización de ejercicios de **Red team/Blue Team** que simulen ataques cibernéticos avanzados y evalúen la efectividad de las defensas de la organización, con el objetivo de identificar vulnerabilidades, mejorar la respuesta ante incidentes y fortalecer la postura de seguridad general.
  - Monitorización y análisis de **eventos relevantes** definiendo previamente **casos de uso** donde se identifiquen las diferentes fuentes de inteligencia (SIEM, EDR, DLP, etc) necesarias para monitorizar y por lo tanto detectar en base al catálogo de amenazas MITTRE ACK&CK.
  - Desplegar **filtros avanzados** de correo para proteger de amenazas como el phishing, el **spam**, y otros tipos de **malware** que a menudo se propagan a través del correo electrónico.
  - Soluciones de inteligencia artificial para detectar y mitigar vulnerabilidades en tiempo real.
  - Ejecución de actividades de **Threat Hunting** en respuesta a amenazas internas y externas. Estas actividades sobre caza de amenazas se basan en la investigación activa por parte de analistas y expertos en ciberseguridad para identificar actividades maliciosas que pueden haber pasado desapercibidas por las herramientas automatizadas.
  - Implementar un **proxy de navegación** para asegurar la navegación por Internet, de forma que actúe como como un intermediario entre los usuarios y los sitios web o servicios en línea a los que acceden. Mediante la implementación de un proxy se puede mejorar tanto la **seguridad** como el **rendimiento** de la red.
- Implementar **servicios de vigilancia digital** para identificar amenazas emergentes. Mediante la monitorización de diferentes fuentes como son la dark web, foros clandestinos y redes sociales se pueden identificar posibles brechas de seguridad. Adicionalmente, gracias al análisis de los Indicadores de Compromiso (IOCs) se refuerzan las defensas.
- Implementación de las medidas para la certificación de ***Lugar Ciberseguro*** para las entidades locales.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M2

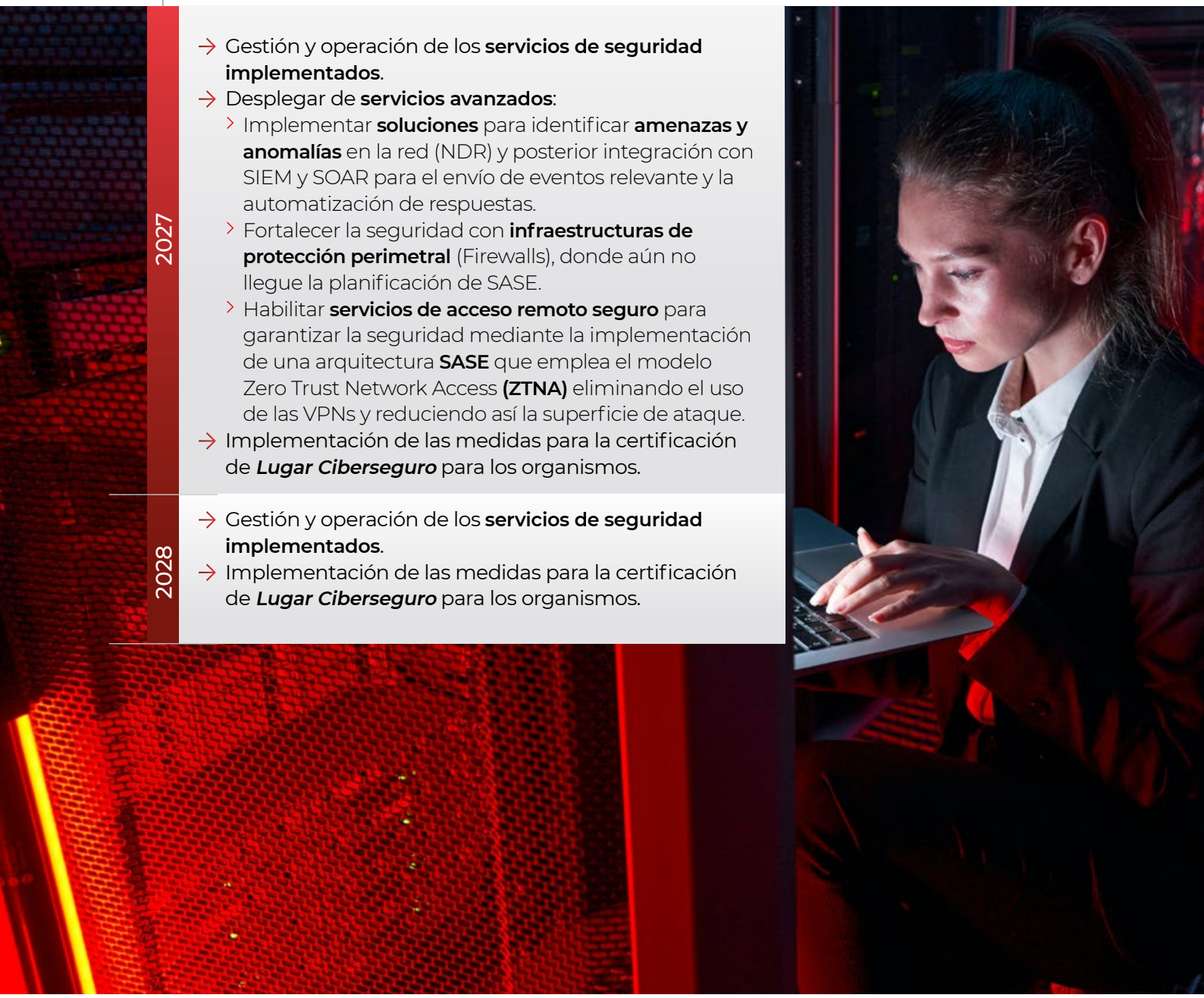
Planificación

2027

- Gestión y operación de los **servicios de seguridad implementados**.
- Desplegar de **servicios avanzados**:
  - Implementar **soluciones** para identificar **amenazas y anomalías** en la red (NDR) y posterior integración con SIEM y SOAR para el envío de eventos relevante y la automatización de respuestas.
  - Fortalecer la seguridad con **infraestructuras de protección perimetral** (Firewalls), donde aún no llegue la planificación de SASE.
  - Habilitar **servicios de acceso remoto seguro** para garantizar la seguridad mediante la implementación de una arquitectura **SASE** que emplea el modelo Zero Trust Network Access **(ZTNA)** eliminando el uso de las VPNs y reduciendo así la superficie de ataque.
- Implementación de las medidas para la certificación de ***Lugar Ciberseguro*** para los organismos.

2028

- Gestión y operación de los **servicios de seguridad implementados**.
- Implementación de las medidas para la certificación de ***Lugar Ciberseguro*** para los organismos.



03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M3

Implementación del escudo de ciberseguridad

La implementación de un **escudo de ciberseguridad** tiene como principal objetivo establecer un conjunto robusto de medidas, herramientas y procesos para proteger los sistemas y servicios críticos frente a amenazas cibernéticas.

El **escudo de ciberseguridad** propuesto por la Agencia consiste en un sistema centralizado de ciberseguridad en la Comunidad de Madrid integrando los SOC de las entidades clave y mejorando la colaboración con los organismos nacionales. Además, se busca realizar ciberejercicios con tecnología SOAR, intercambiar información de manera fluida entre los diferentes SOC y automatizar los servicios de seguridad para mejorar la eficiencia operativa y la respuesta ante incidentes.

Objetivos

1. Fortalecer la **ciberseguridad regional** mediante la creación de un sistema centralizado y coordinado de protección.
2. **Optimizar la respuesta ante incidentes**, a través de la automatización y los ciberejercicios.
3. **Mejorar la colaboración interinstitucional.** Fomentar el intercambio de información bidireccional entre los SOC de la Comunidad de Madrid y los nacionales, permitiendo una colaboración más estrecha y eficiente en la gestión de amenazas y vulnerabilidades.
4. Mayor **interoperabilidad** en los sistemas de seguridad, garantizando que los SOC operen de manera integrada.
5. **Automatizar y evolucionar los servicios de seguridad.** Desarrollar procesos automatizados que mejoren la eficiencia operativa.

Beneficios

- **Mejora en la coordinación y comunicación** entre los SOC de las entidades clave de la Comunidad de Madrid y los organismos nacionales.
- **Optimización en la respuesta ante incidentes** mediante la automatización de los procesos de seguridad.
- **Mayor capacidad de adaptación** ante nuevas amenazas.
- **Optimización de recursos.** Al integrar y homogenizar los diferentes SOC de las entidades clave, se logra una mejor asignación de recursos.

03

E3

FORTALECER LAS CAPACIDADES DE PREVENCIÓN Y DETECCIÓN

E3.M3

Planificación

2025 - 2026

- Crear un **escudo de ciberseguridad** con tecnología SOAR, integrando la información de los diferentes SOC (Centro de Operaciones de Seguridad). Esta tecnología permite a las organizaciones gestionar la seguridad de forma más rápida, eficiente y escalable al integrar y automatizar procesos de respuesta ante incidentes.
- Actuar como **punto central** para el intercambio de **información bidireccional** entre los SOC de la Comunidad de Madrid y el resto de los organismos nacionales (CSIRT).
- **Integración y homogeneización** entre los diferentes SOC de las entidades clave de la Comunidad de Madrid.

2027

- **Integración y homogeneización** entre los diferentes SOC de las entidades clave de la Comunidad de Madrid.
- **Evolución y automatización** de los servicios de seguridad implementados.

2028

- Implementar capacidades de **ciberinteligencia predictiva** a escala regional empleando modelos de IA entrenados con datos agregados del punto central.
- Desplegar **simulaciones regionales de cibercrisis** y ejercicios de respuesta coordinada con participación de los SOC regionales.

04

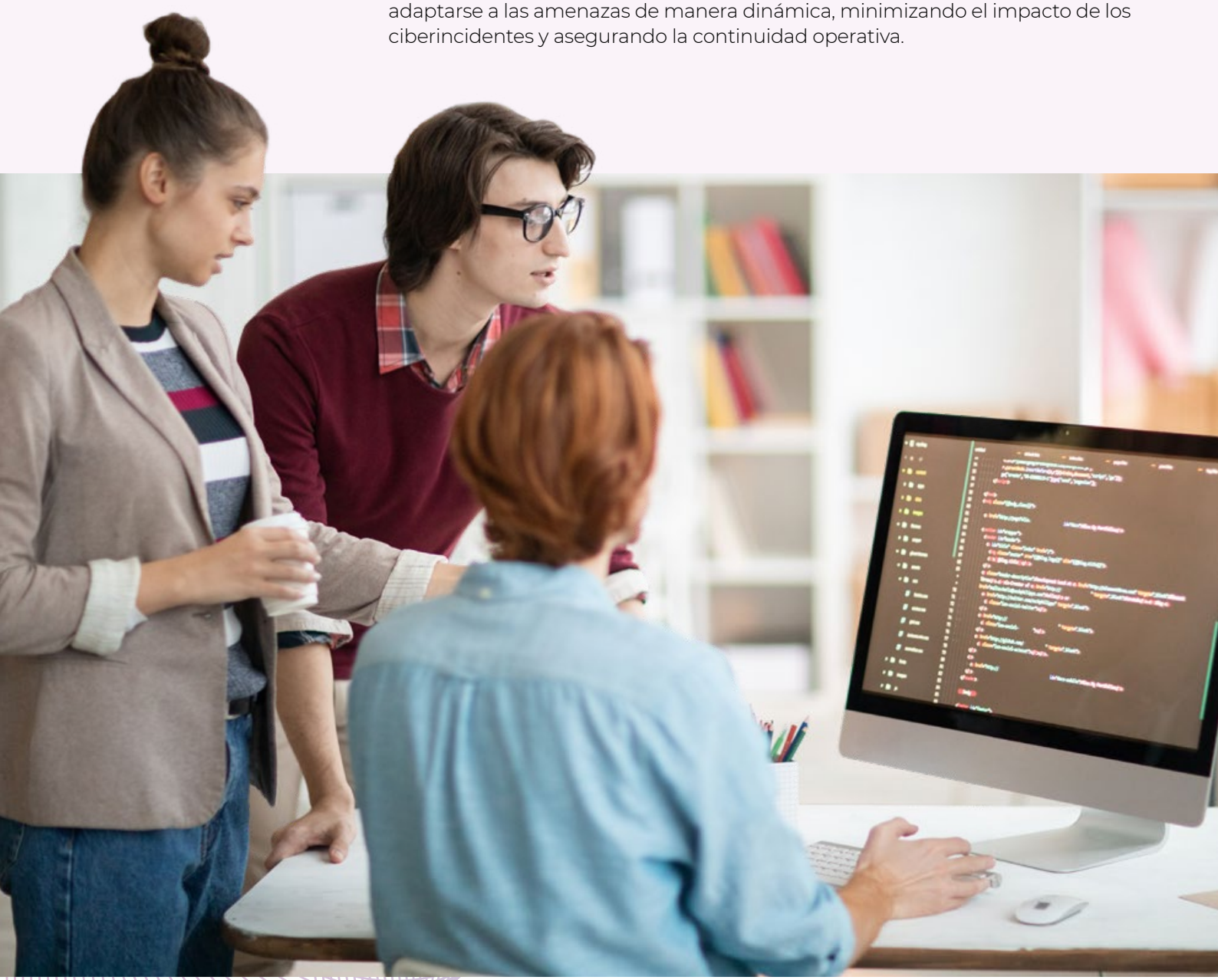
E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE CIBERINCIDENTES

Resumen

El cuarto eje sobre **potenciar las capacidades de gestión y respuesta ante ciberincidentes** se enfoca en reforzar la capacidad de las organizaciones para supervisar de manera continua las redes y fuentes de información para detectar con una respuesta rápida y efectiva las ciberamenazas, garantizando una protección tanto proactiva como reactiva según la naturaleza de cada incidente.

Esto implica no solo la detección temprana de amenazas, sino también una capacidad de respuesta organizada y eficiente que permita a las entidades adaptarse a las amenazas de manera dinámica, minimizando el impacto de los ciberincidentes y asegurando la continuidad operativa.



04

E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E4.M1 Modelo de Gestión de Crisis

Un **modelo de gestión de crisis** es un plan para manejar situaciones de emergencia, en este caso, incidentes cibernéticos. Este modelo establece procedimientos, roles y responsabilidades claras para responder de manera efectiva a las crisis y minimizar su impacto.

En este pilar, se establece un **modelo de gestión y coordinación de crisis único**, que servirá como guía para la respuesta organizada y eficiente a incidentes de seguridad. Un aspecto clave es la **integración del CSIRT en los CSIRT nacionales**, lo que permitirá a la organización colaborar con otros equipos de respuesta ante incidentes a nivel nacional. Además, para fortalecer la colaboración, **se contempla la incorporación del equipo en los CSIRT europeos e internacionales**, lo cual facilitará el intercambio de información sobre amenazas y vulnerabilidades a nivel global. Además, se busca capacitar a los equipos de gestión de crisis en función del impacto de los incidentes, de forma que estén preparados para actuar ante situaciones de cualquier magnitud.

Objetivos

1. Garantizar una **capacidad de respuesta continua** ante incidentes de ciberseguridad, disponiendo de un equipo especializado que se encuentre disponible en todo momento.
2. **Alinear los procedimientos** de gestión de crisis con los protocolos nacionales.
3. **Impartir formaciones** a los equipos de respuesta para mejorar su capacitación.
4. Tener un **alcance de colaboración internacional**, participando en redes internacionales de CSIRT.

Beneficios

- **Mejorar y aumentar la capacidad de respuesta ante incidentes.** Tener un equipo disponible las 24 horas del día, todos los días de la semana, supone una mejora en la detección, análisis y mitigación de los ciberincidentes.
- **Coordinación efectiva.** Disponer de un modelo único de gestión, permite que todas las entidades puedan actuar de manera alineada y sincronizada.
- **Mayor integración con CSIRT nacionales e internacionales.** Formar parte de redes nacionales y europeas de CSIRT facilita el intercambio de inteligencia de amenazas y buenas prácticas, mejorando la anticipación y mitigación de riesgos.
- **Mayor preparación.** Capacitar a los equipos de gestión de crisis según el impacto, permite que tengan una mayor preparación para poder enfrentar cualquier tipo de amenaza, independientemente de su magnitud.

04

E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M1

Planificación

2025 - 2026

- Establecer y definir un **Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT)** que operará de manera continua, las 24 horas del día, los 7 días de la semana. Este centro contará con **recursos externos y personal altamente especializado** en la detección, análisis y mitigación de incidentes de ciberseguridad.
- Definir un **modelo de gestión y coordinación de crisis único**, estableciendo un marco normativo y operativo unificado para la gestión de crisis en el ámbito de la ciberseguridad.
- Integrar el **equipo en los CSIRT** nacionales. El CSIRT regional se integrará dentro de la red nacional **de centros de respuesta a incidentes**, permitiendo el acceso a información crítica sobre amenazas y vulnerabilidades en tiempo real. Esto facilitará la cooperación con organismos nacionales como el **INCIBE-CERT** o el **CCN-CERT**.
- Capacitar a los **equipos de gestión de crisis** según el impacto, mediante programas de formación y simulacros de cibercrisis.

2027

- Incorporar el **equipo en los CSIRT** a nivel europeo e internacional.

04

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M2 Soporte a la Gestión de Crisis

El eje de **Soporte a la Gestión de Crisis** busca fortalecer la capacidad de respuesta ante ciberataques y amenazas mediante una **coordinación eficaz, un soporte técnico especializado y una comunicación eficiente** entre los diferentes actores involucrados.

Para ello, se establecerá un **punto único de reporte y gestión** de incidentes críticos, además de fomentar la **coordinación global** en aquellas situaciones que afecten a diversas entidades.

Asimismo, se implementará un **canal de mensajería instantánea** para la comunicación en tiempo real con los CSIRTs, permitiendo un intercambio ágil de información.

Objetivos

1. **Coordinación global.** Garantizar una respuesta estructurada y eficiente en incidentes que afecten a múltiples entidades siguiendo las mejores prácticas y estándares internacionales como ISO/IEC 27035 y NIST 800-61.
2. Ofrecer **asistencia especializada** en la investigación, identificación y gestión de ciberincidentes.
3. **Centralizar la recepción y comunicación** de todos los incidentes.
4. **Mejorar la comunicación** mediante un sistema de mensajería instantánea.

Beneficios

- **Actuación más rápida y efectiva.** Tener una buena coordinación afecta directamente en una mejora en la capacidad de actuar ante ciberincidentes de forma más rápida y efectiva.
- **Mayor capacidad de respuesta y disminución del impacto de incidentes** gracias a ofrecer soporte técnico y análisis forense.
- **Agilización en la comunicación.** Tener un canal de mensajería instantánea permite agilizar y facilitar la comunicación entre las entidades y el CSIRT.

04

E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M2

Planificación

2025 - 2026

- **Coordinación global** en casos de afectación de múltiples entidades, en busca de una respuesta ágil, coordinada y con acceso a la información en tiempo real para mitigar el impacto de la amenaza.
- Apoyar en la **gestión y coordinación** de incidentes críticos.
- Ofrecer **soporte técnico y análisis forense** en la resolución de incidentes críticos, que permitan determinar el origen del ataque, identificar las vulnerabilidades explotadas, recuperar datos afectados, así como recopilar evidencias para poder tomar acciones legales en casos concretos.
- **Punto único** de reporte e información de gestión de todas las crisis e incidentes.
- Implantar un **canal de mensajería instantánea** de CSIRT para para entidades locales, PYMES y organismos públicos de la región.

2027

- **Coordinación global** en casos de afectación de múltiples entidades.
- Apoyar en la **gestión y coordinación** de incidentes críticos.
- Ofrecer **soporte técnico y análisis forense** en la resolución de incidentes críticos.
- **Punto único** de reporte e información de gestión de todas las crisis e incidentes.

2028

- **Asesoramiento** en la definición de la arquitectura para obtener redundancia de sistemas, copias de seguridad, etc.
- Dar apoyo en la **realización de ejercicios** para poner en práctica los **procedimientos de crisis** para optimizar los tiempos de respuesta y la mejora de los procedimientos.
- Asesorar en la mejora de los reportes y su automatización.

04

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M3 Desarrollo e implementación del programa de ciberejercicios

Los **ciberejercicios** constituyen una herramienta fundamental para evaluar y fortalecer las capacidades de prevención, detección, defensa y recuperación frente a ciberataques.

El objetivo de este pilar es desarrollar un **Programa de Ciberejercicios** que ayude a los organismos y entidades a mejorar su preparación, coordinación y capacidad operativa. A lo largo de la planificación del pilar, se definirán las pruebas y ejercicios que lo comprenderán, las metodologías de ejecución y las métricas de evaluación.

Objetivos

1. **Mejorar las capacidades de respuesta** mediante simulaciones prácticas.
2. **Incluir diferentes escenarios de ataque.** Determinar los tipos de ejercicios más adecuados para cada entidad y objetivo específico.
3. Realizar ejercicios diseñados específicamente para **entidades críticas**, así como evaluar sus resultados para identificar áreas de mejora.

Beneficios

- **Fortalecimiento de la resiliencia de infraestructuras críticas.** Al diseñar ejercicios enfocados en ellas, se asegura una mejora en su seguridad.
- **Detección temprana de debilidades.** Durante los ejercicios, se identifican puntos débiles en las políticas, procesos y sistemas de ciberseguridad.
- **Simulaciones realistas de escenarios complejos.** Los ciberejercicios como ataques dirigidos o simulaciones crean escenarios de ciberataques realistas que permiten a las organizaciones probar sus defensas en situaciones controladas, pero similares a amenazas de la vida real.

04

E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M3

Planificación

2025 - 2026

- Diseñar un **Programa de Ciberejercicios** para evaluar la preparación, coordinación y capacidad operativa de los organismos y entidades.
- Definir el **tipo de pruebas y ciberejercicios** (TableTop, ataque dirigido y/o simulación).
- **Diseñar y ejecutar los ciberejercicios** enfocados en entidades críticas.
- **Realizar ciberjercicios con Entidades Locales** en Digitaliza Madrid y en un Centro de Capacitación Digital.
- **Evaluar** los resultados de los ciberejercicios para las entidades críticas.

2027

- Definir el **plan de trabajo anual** de ciberejercicios.
- **Diseñar y ejecutar los ciberejercicios** para las entidades **críticas y de nivel medio**.
- **Evaluar** los resultados de los ciberejercicios para las **entidades críticas** y para un número de **nivel medio**.

2028

- Definir el **plan de trabajo anual** de ciberejercicios.
- **Diseñar y ejecutar los ciberejercicios** para las entidades **críticas y de nivel bajo**.
- **Evaluar** los resultados de los ciberejercicios para las entidades **críticas** y para un número de **nivel bajo**.

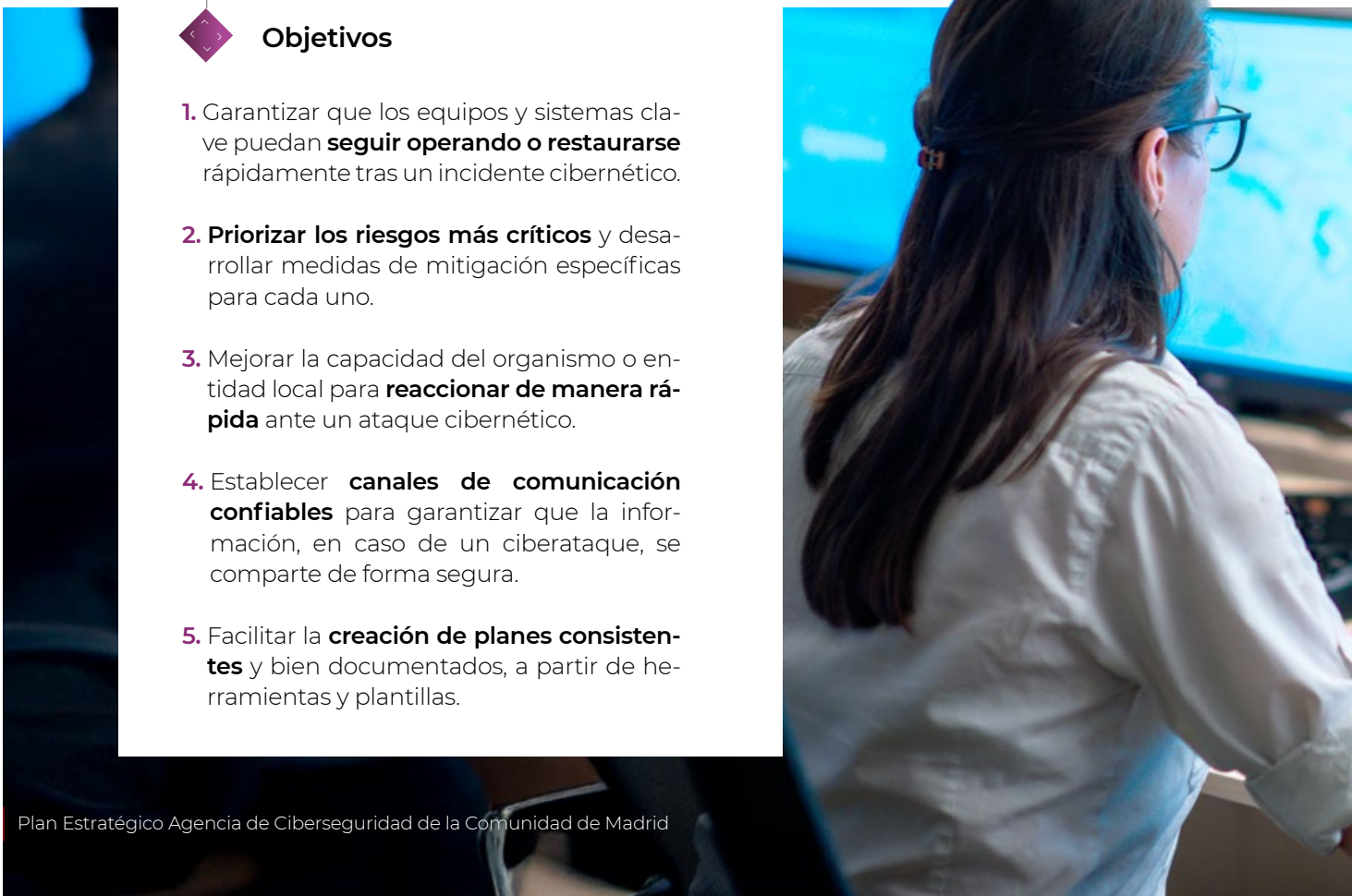
04

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M4 Elaboración de los Planes de Continuidad de Negocio

Un ciberataque, una vulnerabilidad explotada o un fallo en la infraestructura tecnológica puede poner en riesgo la operatividad de una entidad local u organismo, afectando no solo a su reputación, sino también a su capacidad operativa para seguir ofreciendo servicios públicos al ciudadano y mantener la confianza del ciudadano en la administración pública de la región. Por este motivo, es crucial tener definido un **Plan de Continuidad de Negocio** que permita seguir funcionando de manera efectiva tras el suceso.

Este pilar tiene como objetivo la elaboración y optimización de **Planes de Continuidad de Negocio**, diseñados para asegurar que, ante cualquier incidente cibernético, **las operaciones críticas de la organización puedan mantenerse o recuperarse rápidamente con el mínimo impacto.**



Objetivos

1. Garantizar que los equipos y sistemas clave puedan **seguir operando o restaurarse** rápidamente tras un incidente cibernético.
2. **Priorizar los riesgos más críticos** y desarrollar medidas de mitigación específicas para cada uno.
3. Mejorar la capacidad del organismo o entidad local para **reaccionar de manera rápida** ante un ataque cibernético.
4. Establecer **canales de comunicación confiables** para garantizar que la información, en caso de un ciberataque, se comparte de forma segura.
5. Facilitar la **creación de planes consistentes** y bien documentados, a partir de herramientas y plantillas.

04

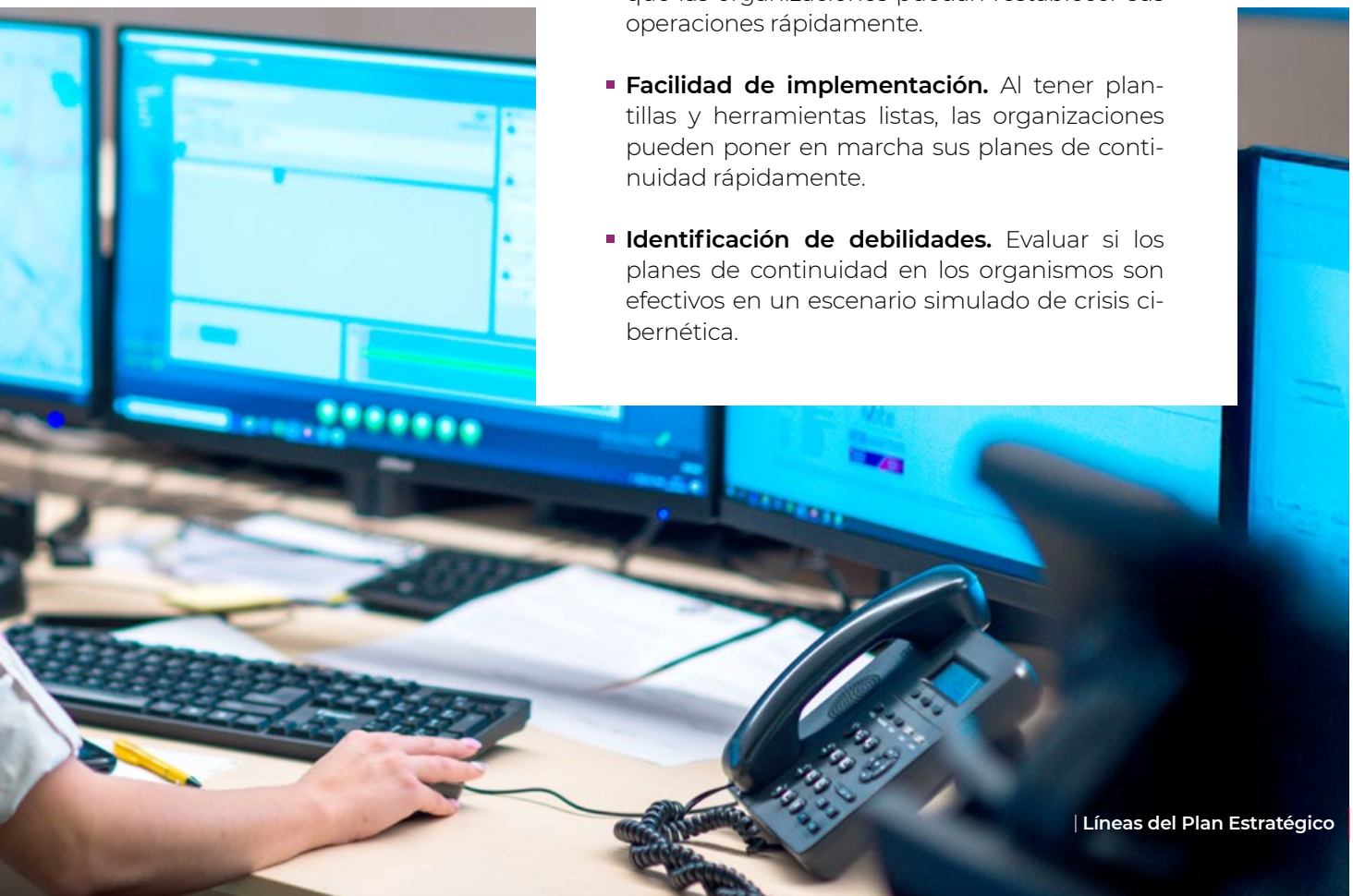
E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M4

Beneficios

- **Reducción de riesgos.** Un Plan de Continuidad de Negocio ayuda a que las organizaciones estén más preparadas para actuar ante un ciberataque, lo que disminuye el riesgo e impacto de las amenazas.
- **Comunicación eficiente y segura.** Establecer canales de comunicación fiables asegura la integridad y seguridad de la información.
- **Mejora de la resiliencia organizacional.** Tener un Plan de Continuidad de Negocio bien estructurado y probado aumenta la capacidad de recuperación ante ciberataques, asegurando que las organizaciones puedan restablecer sus operaciones rápidamente.
- **Facilidad de implementación.** Al tener plantillas y herramientas listas, las organizaciones pueden poner en marcha sus planes de continuidad rápidamente.
- **Identificación de debilidades.** Evaluar si los planes de continuidad en los organismos son efectivos en un escenario simulado de crisis cibernética.



04

E4

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E4.M4

Planificación

2025 - 2026

- Definir y establecer los **canales de comunicación seguros** para asegurar que, en caso de incidente cibernético, las organizaciones puedan comunicarse sin comprometer la integridad o confidencialidad de la información.
- Proporcionar **herramientas y plantillas** para desarrollar los Planes de Continuidad de Negocio.
- Definir el **plan de trabajo anual** de elaboración de los **Planes de Continuidad de Negocio**, incluyendo un calendario de actividades definiendo un cronograma detallado con fechas clave.
- **Supervisión** y seguimiento de la elaboración de los Planes de Continuidad de Negocio para las entidades críticas.
- Pruebas de **Continuidad Avanzada en organismos** de la Comunidad de Madrid, que verifiquen la efectividad de los Planes de Continuidad de Negocio en condiciones controladas.
- Ciberjercicio en **infraestructuras críticas** con escenario de cibercrísis combinado con varias entidades críticas de la Comunidad de Madrid en Digitaliza Madrid.

2027

- Definir el **plan de trabajo anual** de elaboración de los **Planes de Continuidad de Negocio.**
- Elaboración de los Planes de Continuidad de Negocio para las **entidades de nivel medio**.
- Realización de **pruebas de contingencia tecnológica** para las **entidades críticas,** estas pruebas son simulaciones y evaluaciones que permiten verificar que las entidades críticas puedan continuar funcionando en caso de un ciberincidente.
- Supervisión y seguimiento de pruebas de contingencia tecnológica.
- **Asesoramiento** en Continuidad de Negocio para **PYMES** (Pequeñas y Medianas Empresas).

2028

- Definir el **plan de trabajo anual** de elaboración de los **Planes de Continuidad de Negocio**.
- Elaboración de los Planes de Continuidad de Negocio para las **entidades de nivel bajo**. De acuerdo con el Esquema Nacional de Seguridad, estas entidades son aquellas cuyas consecuencias de un incidente de seguridad supongan un **perjuicio limitado** sobre las funciones de la organización, sus activos o individuos afectados.
- Realización y supervisión de **pruebas de contingencia** tecnológica para las **entidades críticas y de nivel medio**. De acuerdo con el Esquema Nacional de Seguridad, las entidades de nivel medio son aquellas cuyas consecuencias de un incidente de seguridad supongan un **perjuicio grave** sobre las funciones de la organización, sus activos o individuos afectados.
- Supervisión y seguimiento de **pruebas de contingencia tecnológica**.
- **Asesoramiento** en Continuidad de Negocio para **PYMES** (Pequeñas y Medianas Empresas).

05

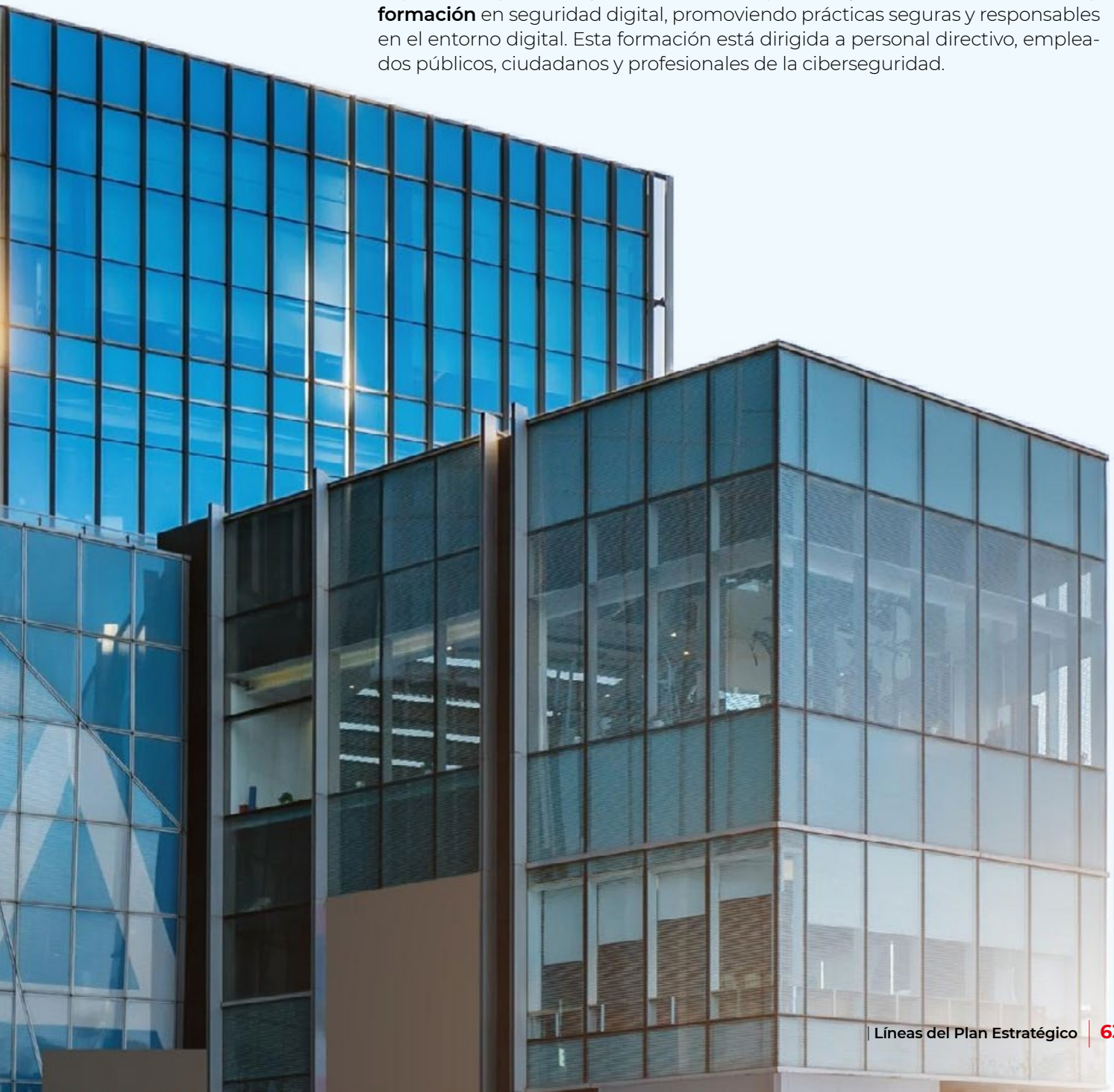
E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

Resumen

Las **amenazas cibernéticas** son una realidad constante, y su evolución pone en riesgo tanto a ciudadanos como a organizaciones en todos los sectores. Para mitigar estos riesgos, es esencial no solo contar con tecnologías avanzadas, sino también con una **cultura sólida de ciberseguridad** y un talento capacitado que sepa identificar, prevenir y responder adecuadamente a estos desafíos.

El presente eje estratégico tiene como objetivo **impulsar la concienciación y formación** en seguridad digital, promoviendo prácticas seguras y responsables en el entorno digital. Esta formación está dirigida a personal directivo, empleados públicos, ciudadanos y profesionales de la ciberseguridad.



05

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E5.M1 Formación personal de Alta Dirección

La **Alta Dirección** juega un papel esencial en la protección de las organizaciones frente a las amenazas cibernéticas. Las **decisiones estratégicas** tomadas por los líderes de una organización pueden determinar su capacidad para gestionar y mitigar riesgos cibernéticos, así como para garantizar la continuidad operativa y la integridad de los datos.

Por este motivo, el presente pilar está enfocado a la **formación de personal de Alta Dirección** en ciberseguridad, con el objetivo de proporcionarle al **personal directivo** de la Administración General e Institucional de la Comunidad de Madrid las **herramientas y campañas de sensibilización** necesarias para que obtengan el conocimiento esencial para tomar decisiones informadas en relación con la protección de los activos digitales y la gestión de incidentes cibernéticos.

Objetivos

1. **Sensibilizar** a la **Alta Dirección** sobre la importancia de la ciberseguridad, mediante campañas e iniciativas de concienciación.
2. Asegurar que el personal directivo pueda **establecer prioridades en ciberseguridad** y asignar recursos de manera eficaz, en línea con los objetivos de negocio y los riesgos emergentes.
3. **Capacitar a la Alta Dirección** para que pueda gestionar los riesgos cibernéticos de manera adecuada dentro de la estrategia organizacional.

Beneficios

- **Mejora en la toma de decisiones estratégicas.** Al tener un personal directivo bien formado en el ámbito de la ciberseguridad, la toma de decisiones será más acertada y teniendo en cuenta los riesgos cibernéticos.
- **Cumplimiento normativo.** La formación en ciberseguridad asegura que la alta dirección esté al tanto de las normativas y estándares de seguridad requeridos, facilitando el cumplimiento de leyes y regulaciones.
- **Cultura organizacional.** Transmisión de una cultura de ciberseguridad desde los puestos más importantes, al resto de la organización.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M1

Planificación

2025 - 2026

→ Realizar **iniciativas de sensibilización** de alto impacto y formación sobre normativa actual de ciberseguridad dirigidas al personal directivo de la Administración general e institucional de la Comunidad de Madrid.

2027

→ Realizar **iniciativas de sensibilización** de alto impacto dirigidas al personal directivo de la Administración general e institucional del Gobierno regional. Como, por ejemplo, charlas con expertos de prestigio, invitados internacionales, análisis de casos reales, mesa redonda con CEO, etc.

2028

→ Realizar **iniciativas de sensibilización** de alto impacto dirigidas al personal directivo de la Administración general e institucional del Ejecutivo autonómico. Como, por ejemplo, simulaciones de crisis, cambios de rol, aprendizaje mediante gamificación, etc.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E5.M2 Formación de empleados públicos con perfil técnico

Las amenazas cibernéticas son cada vez más sofisticadas y están en constante evolución, lo que exige que las organizaciones, tanto públicas como privadas, cuenten con **profesionales altamente capacitados** para proteger sus sistemas y datos. Los **funcionarios con perfil técnico** desempeñan un papel clave en la defensa frente a estos riesgos, siendo responsables de la implementación y gestión de las medidas de seguridad cibernética en diversas entidades.

Este pilar estratégico tiene como objetivo proporcionar una **formación especializada en ciberseguridad** a los funcionarios con perfil técnico, quienes son los encargados de ejecutar, mantener y supervisar las políticas y herramientas de seguridad en las instituciones públicas.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M2

Objetivos

1. Desarrollo de **competencias técnicas especializadas en ciberseguridad y protección de datos.**

2. **Fortalecer la capacidad de respuesta y gestión de incidentes cibernéticos** mediante programas de formación especializados, que incluyan simulacros prácticos y capacitación continua para el personal, asegurando una preparación integral frente a cualquier tipo de amenaza cibernética.

3. Favorecer que los funcionarios sean **conocedores de los requisitos normativas y regulatorios de Ciberseguridad** para su cumplimiento.

4. **Manejo Seguro de Información:** Los empleados públicos aprenden a manejar datos sensibles de manera segura, previniendo fugas de información y protegiendo la privacidad de los ciudadanos.

Beneficios

- **Reducción de vulnerabilidades en la Administración Pública de la región** mediante una mejor gestión de los riesgos asegurando una protección efectiva de los sistemas y datos que manejan datos de los ciudadanos.

- **Mejora en la Protección de Datos y Privacidad.** La formación asegura que los empleados públicos apliquen los principios de seguridad para proteger datos sensibles y garantizar la privacidad de los ciudadanos y usuarios del sistema público.

- **Fortalecimiento de la Confianza Ciudadana.** Al garantizar la seguridad de los sistemas públicos y los datos de los ciudadanos, se mejora la confianza en las instituciones gubernamentales.

Planificación

2025 - 2026

→ Desarrollar un **Programa de Formación** especializado en Ciberseguridad, diseñado con diferentes itinerarios en función de los diversos perfiles técnicos de los funcionarios (desarrollo, IA, especialista de datos, etc).

→ Impartir las sesiones enfocadas en la mejora de los **conocimientos técnicos y el uso de herramientas de ciberseguridad**.

2027

→ Impartir las sesiones basadas en la **especialización técnica**, incluyendo **laboratorios prácticos y sesiones específicas avanzadas**.

2028

→ Impartir las sesiones orientadas a la obtención de **certificaciones de reconocido prestigio internacional**.

05

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M3 Formación y concienciación empleados públicos de la región de Madrid

La **formación y concienciación en ciberseguridad** de los empleados públicos de la **Comunidad de Madrid** es crucial para garantizar la seguridad y la protección de los datos sensibles y las infraestructuras críticas del gobierno regional.

El personal que gestiona y opera sistemas informáticos, bases de datos, aplicaciones y redes es el **primer eslabón de defensa** ante ataques cibernéticos. Por ello, es necesario asegurar que todos los empleados públicos tengan un conocimiento adecuado de los riesgos y las mejores prácticas de seguridad digital.

Objetivos

1. **Sensibilizar sobre la Importancia de la Ciberseguridad.** Concienciar a todos los empleados públicos de la Comunidad de Madrid sobre los riesgos cibernéticos y la importancia de adoptar buenas prácticas de seguridad digital.

2. **Proporcionar Formación Continua en Ciberseguridad.** Ofrecer una formación adecuada y continua para que los empleados públicos estén al tanto de las últimas amenazas cibernéticas y las mejores herramientas para defenderse de ellas.

3. **Fomentar Prácticas Seguras y Responsables.** Capacitar a los empleados en el uso seguro de contraseñas, el manejo de datos sensibles, y la protección de dispositivos y sistemas informáticos contra accesos no autorizados.

4. **Aumentar la Confianza Pública en la Gestión de Datos.** Demostrar el compromiso de la Administración Pública de la región con la seguridad de los datos de los ciudadanos

Beneficios

- **Reducción de Errores Humanos.** Muchos ciberataques y brechas de seguridad se deben a errores humanos, como el uso de contraseñas débiles o la apertura de correos electrónicos maliciosos. La formación reduce estos errores, protegiendo mejor los recursos digitales.

- **Mejora en la Resiliencia ante Ciberataques.** La formación y concienciación mejoran la capacidad de los empleados para detectar, prevenir y mitigar ciberataques.

- **Optimización de los Recursos Digitales.** Tener empleados públicos formados en ciberseguridad supone que puedan gestionar de una forma más eficiente los recursos tecnológicos, implementando medidas de seguridad adecuadas y optimizando el uso de herramientas y plataformas digitales dentro de la Administración Pública.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M3

Planificación

2025 - 2026

- Desarrollar un **Programa de Sensibilización** en formato online, con el principal objetivo de concienciar sobre la importancia de la ciberseguridad y sensibilizar a los empleados respecto a las amenazas cibernéticas más comunes, como el phishing, los ataques de Ransomware y las vulnerabilidades derivadas del uso inapropiado de la tecnología.
- Crear una **plataforma digital** para la impartición de la formación y evaluación de los conocimientos adquiridos.
- Diseñar y elaborar los **contenidos formativos** que aborden los principales riesgos cibernéticos, técnicas de protección y buenas prácticas de seguridad digital.
- Definir un **plan anual de capacitación**.

2027

- Impartir las sesiones de **formación y concienciación** por distintas temáticas.

2028

- Actualizar los temarios del plan de formación y concienciación de acuerdo a las amenazas actuales.
- Medir el grado de satisfacción de los asistentes a las formaciones para obtener retrospectiva y tener una mejora continua.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M4

Formación y concienciación para el ciudadano de la Comunidad de Madrid

La formación y concienciación en ciberseguridad para los ciudadanos de la Comunidad de Madrid es un pilar fundamental para garantizar una **sociedad digital segura y protegida.**

Es de vital importancia que la ciudadanía tenga los conocimientos necesarios para proteger su información personal y su privacidad. Este pilar tiene como objetivo proporcionar a los ciudadanos las **herramientas** para reconocer los riesgos, prevenir ataques y saber cómo actuar ante incidentes de ciberseguridad.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M4

Objetivos

1. **Aumentar la concienciación sobre los riesgos en ciberseguridad.** Informar y sensibilizar a la población sobre las principales amenazas cibernéticas.
2. **Formación en la Identificación de amenazas comunes.** Proporcionar formación práctica sobre cómo reconocer correos electrónicos fraudulentos, sitios web maliciosos y otras formas de manipulación en línea.
3. **Fomentar el Uso Responsable de las Tecnologías Digitales.** Promover el uso ético y responsable de la tecnología.
4. **Ayudar a la ciudadanía a evitar caer en trampas y fraudes digitales maliciosos.**

Beneficios

- **Reducción de Riesgos y Vulnerabilidades Personales.** Si la ciudadanía está formada y sensibilizada con la ciberseguridad, podrá protegerse mejor contra amenazas cibernéticas y evitar ser víctima de ellas.
- **Fortalecimiento de la Resiliencia Comunitaria.** Conforme más informada esté la ciudadanía sobre los riesgos cibernéticos, más resiliente será en su conjunto frente a posibles ataques y amenazas.
- **Mejora en la Protección de la Privacidad y Datos Personales.** Los ciudadanos serán más conscientes de los riesgos asociados con la divulgación de información personal y estarán mejor equipados para proteger su privacidad en plataformas digitales.

Planificación

2025 - 26	→ Realizar **acciones de sensibilización** en Redes Sociales para el ciudadano. → Creación de un **canal de mensajería instantánea** para dar respuesta a las consultas del ciudadano.
2027	→ Reforzar las **acciones de sensibilización** en Redes Sociales para el ciudadano.
2028	→ Establecer un **programa de gamificación** para los ciudadanos. → Establecer un **servicio de atención al ciudadano y PYMES** (Pequeñas y Medianas Empresas) sobre fraudes e incidentes.

05

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M5 Fomentar la formación de profesionales de Ciberseguridad

Para poder enfrentar las amenazas cibernéticas emergentes y proteger los sistemas, datos e infraestructuras, es necesario contar con **profesionales capacitados y formados** en el ámbito de la ciberseguridad.

El **fomento de la formación de profesionales de ciberseguridad** es esencial no solo para mejorar la capacidad de las organizaciones de responder ante incidentes, sino también para fortalecer la infraestructura cibernética de la región y el país.

Objetivos

1. Ofrecer **talleres de formación** en Centros Educativos y Universidades.
2. **Colaborar con empresas** para promover y facilitar la contratación de alumnos en puestos de trabajo relacionados con ciberseguridad.
3. Impulsar y fomentar **el interés de la ciudadanía** mediante la realización de competiciones.
4. Reducir la brecha de talento en ciberseguridad. Abordar la **escasez de profesionales en ciberseguridad** mediante la formación de nuevos expertos.

Beneficios

- **Fomento de la innovación y la investigación en ciberseguridad.** La formación de profesionales en ciberseguridad aumenta la capacidad de innovación e investigación en el sector.
- **Impulso de la vocación e interés en ciberseguridad.** A través de la impartición de talleres en centros educativos, se fomenta el interés de los estudiantes, creando una cantera de profesionales desde una temprana edad.
- **Inserción laboral.** Establecer convenios con empresas ayuda a los estudiantes a tener una vía directa para acceder al mercado laboral.

05

E5

FOMENTAR EL TALENTO Y CULTURA DE CIBERSEGURIDAD

E5.M5

Planificación

2025 - 26

- Fomentar **talleres formativos** en los **Centros de Educación de Secundaria** para fomentar el interés en la ciberseguridad.

2027

- Continuar con la oferta de **talleres formativos** en los **Centros de Educación de Secundaria**.
- Establecer alianzas con **Universidades y Centros de Formación** para desarrollar programas especializados en ciberseguridad.
- Promover **convenios con empresas privadas** para facilitar la contratación de alumnos.
- Organizar competiciones tipo **Hackaton o CTF** (Capture the Flag).
- Constituir y participación del equipo **MIB (Men In Black) Team** (selección oficial de Ciberseguridad de la Comunidad de Madrid).

2028

- Continuar con la oferta de **talleres formativos** en los **Centros de Formación de la región**.
- Continuar con el desarrollo de **alianzas y convenios** con las empresas privadas.
- Organizar competiciones tipo **Hackaton o CTF** (Capture the Flag).
- Profesionalizar el equipo **MIB (Men In Black) Team** (selección oficial de Ciberseguridad de la Comunidad de Madrid).

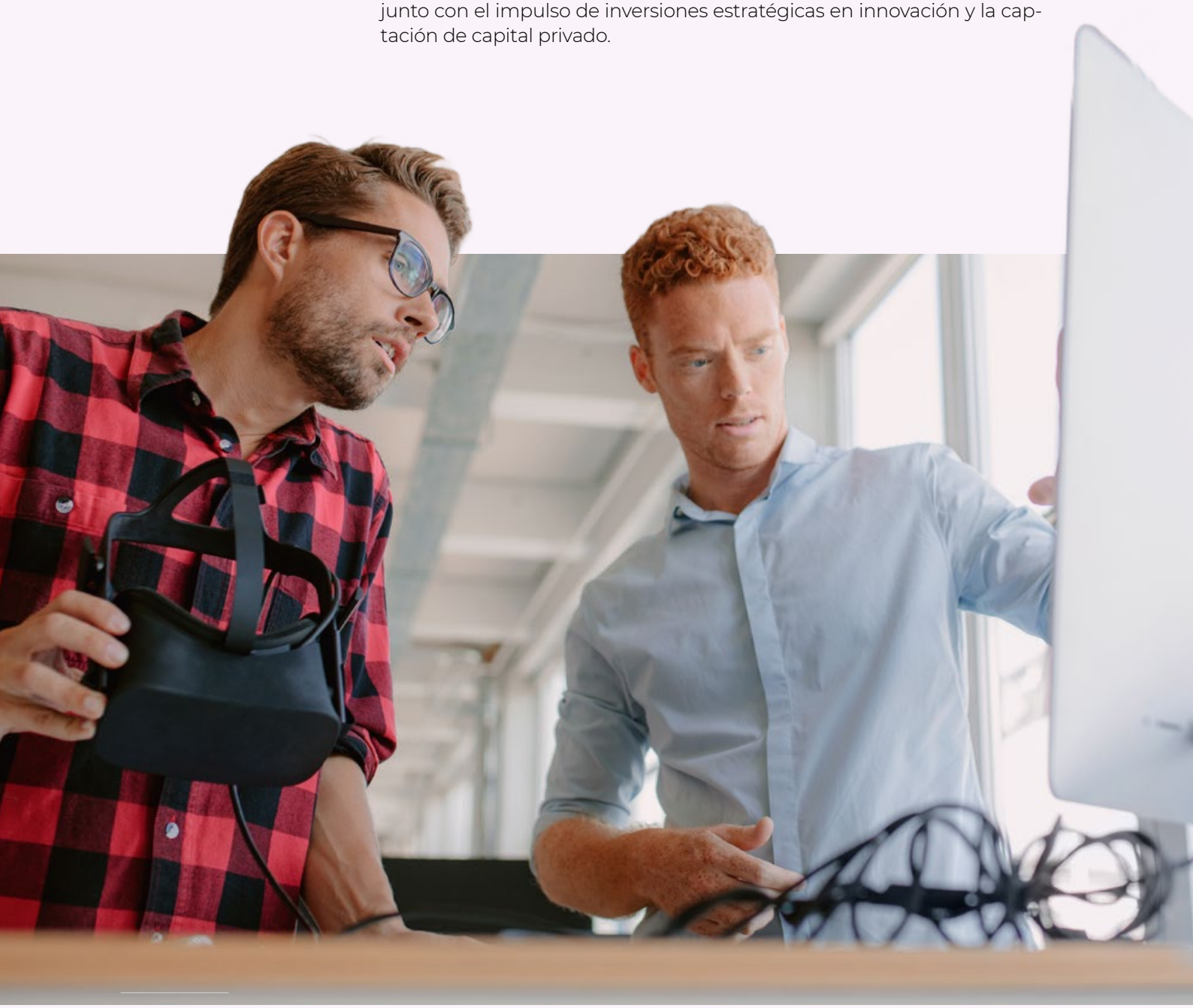
06

E6

IMPULSAR Y TRANSFORMAR EL ECOSISTEMA DE CIBERSEGURIDAD DE LA REGIÓN.

Resumen

Al **impulsar y transformar el ecosistema de ciberseguridad,** la Comunidad de Madrid busca crear un entorno favorable para la innovación, el crecimiento empresarial y la colaboración en el ámbito de la ciberseguridad. Este eje se centra en fortalecer la infraestructura digital y la capacidad de respuesta ante ciberamenazas, favoreciendo la creación y expansión de **empresas de ciberseguridad** de alto impacto en la región, junto con el impulso de inversiones estratégicas en innovación y la captación de capital privado.



06

E6

IMPULSAR Y TRANSFORMAR EL ECOSISTEMA DE CIBERSEGURIDAD DE LA REGIÓN.

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E6.M1 Identificación de los servicios y capacidades de las empresas

El objetivo principal de la **identificación de los servicios y capacidades de las empresas** es proporcionar un mapa detallado del ecosistema de ciberseguridad de la Comunidad de Madrid. A través de la elaboración de un **Libro Blanco** y la realización de un estudio sobre las **empresas y startups,** este eje busca fortalecer la **competitividad** y **visibilidad** de las empresas madrileñas, además de facilitar la creación de **nuevas oportunidades de colaboración** tanto a nivel regional como global.

Objetivos

1. **Mapear el ecosistema** de ciberseguridad de la Comunidad de Madrid, identificando y visibilizando diferentes empresas y startups.
2. **Promover un entorno empresarial** en ciberseguridad mediante la identificación de servicios y capacidades de las empresas.
3. **Impulsar inversiones estratégicas,** proporcionando datos relevantes sobre el estado y evolución del sector.

Beneficios

- **Mayor conocimiento del sector.** Se obtendrá una visión clara del entorno empresarial y de las capacidades en ciberseguridad dentro de la Comunidad de Madrid.
- **Impulso a la innovación y el emprendimiento.** Identificar startups permitirá detectar oportunidades de crecimiento.
- **Oportunidades de colaboración y expansión.** Facilita la conexión con empresas fuera de Madrid, promoviendo asociaciones estratégicas.

Planificación

2025 - 26
- → Elaborar un **Libro Blanco** de las empresas de ciberseguridad de la región pertenecientes al **Cluster Cyber Madrid**.
- → Realizar un **estudio para identificar las empresas y startups** presentes en otros territorios.

2027
- → Publicitar el **Libro Blanco** y ampliar el detalle de las soluciones y servicios.

2028
- → **Actualizar** el contenido del **Libro Blanco** con información del estado del ecosistema de la **ciberseguridad actual** y las **tendencias** del sector.

06

E6

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E6.M2

Servicio de Impulso y sensibilización en Ciberseguridad

El nivel de **conocimiento y sensibilización** en ciberseguridad por parte de la ciudadanía, organismos y entidades es un factor importante de cara a mantener un entorno digital seguro.

Por este motivo, el objetivo del presente pilar es **fortalecer la cultura de ciberseguridad en la Comunidad de Madrid** a través de la formación, la concienciación y la colaboración estratégica.

Para ello, se promoverá la firma de convenios con actores clave, como el **Cluster Cyber-Madrid**, foros de ciberseguridad y organismos públicos nacionales e internacionales, fomentando el intercambio de conocimientos. Además, se presentará un **Plan de Difusión, Formación y Concienciación en Ciberseguridad**, con el objetivo de mejorar la preparación frente a amenazas cibernéticas. También se impulsará la creación de un **centro estratégico de ciberseguridad,** que atraiga empresas especializadas en el sector. Paralelamente, se desarrollarán estrategias para **captar inversión privada y fomentar la inversión en I+D+i** en tecnologías clave, garantizando el crecimiento y la competitividad del ecosistema de ciberseguridad en la región.

Objetivos

1. **Diseñar y ejecutar un Plan de Difusión, Formación y Concienciación en Ciberseguridad,** enfocado a mejorar la preparación frente a ciberamenazas de la ciudadanía y su conocimiento en materia de ciberseguridad.
2. **Fortalecer la industria de la ciberseguridad** mediante el aumento de las inversiones en I+D+i.
3. **Realizar y firmar convenios con actores clave** del sector para fortalecer la cooperación institucional.
4. Desarrollar estrategias para **atraer la inversión privada en ciberseguridad.**

Beneficios

- **Mayor concienciación y sensibilización** en el ámbito de la ciberseguridad entre ciudadanos y empresas.
- **Atracción de empresas y talento especializado,** gracias a la creación de un centro estratégico.
- **Impulso a la innovación y el desarrollo de nuevas soluciones tecnológicas,** gracias al fomento de la inversión en I+D+i.
- **Facilitar el crecimiento y desarrollo de empresas de ciberseguridad,** mediante la creación de estrategias para atraer capital privado.

06

E6

POTENCIAR LAS CAPACIDADES DE GESTIÓN Y RESPUESTA ANTE A CIBERINCIDENTES

E6.M2

Planificación

2025 - 2026

- Firmar el convenio con el **Cluster CyberMadrid,** una asociación sin ánimo de lucro que reúne a empresas, asociaciones e instituciones, tanto públicas como privadas, que desarrollan actividades en el área de Madrid, y que se asocian libremente para impulsar el desarrollo del sector de la ciberseguridad.
- Firmar los convenios con **Foros de Ciberseguridad,** permitiendo la participación activa de la Comunidad de Madrid en estos espacios de intercambio de conocimiento y experiencias entre profesionales del sector.
- Firmar convenios con **organismos públicos de ciberseguridad** tanto del ámbito nacional como internacional.
- Presentación del **Plan de difusión, formación y concienciación** en materia de ciberseguridad.

2027

- Crear un **centro estratégico** para atraer empresas especializadas en ciberseguridad a la Comunidad de Madrid.
- Promover **estrategias para atraer capital privado** a empresas de ciberseguridad de la región.
- Fomentar la **inversión en I+D+i** en tecnologías clave para la industria de ciberseguridad.

2028

- Extender las actividades del **centro estratégico** para que la Comunidad de Madrid sea el principal foco de atración de empresas especializadas en ciberseguridad.
- Promover **estrategias para atraer capital privado**, y otros fondos, como los de la Unión Europea, a empresas de ciberseguridad de la Comunidad de Madrid.
- Fomentar la **inversión en I+D+i** en tecnologías clave para la industria de ciberseguridad.

07

E7

IMPULSAR LA REALIZACIÓN DE EVENTOS Y ALIANZAS ESTRATÉGICAS

Resumen

Con el propósito de posicionar a la Agencia como líder en ciberseguridad, se divide el eje estratégico en tres pilares basados en la **organización de eventos** especializados en ciberseguridad, permitiendo un intercambio de conocimiento y tendencias del sector. Además, se busca el **fomento de la inversión privada** para garantizar el crecimiento y la sostenibilidad del sector de ciberseguridad, mediante la creación de Centros de Excelencia y, por último, el eje se enfoca en la consolidación de **alianzas estratégicas,** lo que permitirá fortalecer la cooperación con organismos nacionales e internacionales, asociaciones empresariales y centros de investigación

07

E7

IMPULSAR LA REALIZACIÓN DE EVENTOS Y ALIANZAS ESTRATÉGICAS

Los pilares sobre los que se sustentan las actividades de esta línea estratégica son:

E7.M1 Organización de eventos

La **organización de eventos** relacionados con la ciberseguridad es una estrategia clave para fortalecer el ecosistema, fomentar la cooperación entre actores del sector y posicionar a la Comunidad de Madrid como un referente en seguridad digital. A través de la organización y participación en eventos y asociaciones, se busca generar espacios de **intercambio de conocimiento e información** entre profesionales y empresas del sector.

Objetivos

1. **Fortalecer la presencia de la Agencia y la Comunidad de Madrid** en el ecosistema de ciberseguridad, a través de la participación en eventos y asociaciones.
2. **Reunir a expertos y profesionales de ciberseguridad** para debatir sobre las últimas tendencias, desafíos y oportunidades del sector.
3. **Impulsar la difusión de conocimientos y mejores prácticas en materia de ciberseguridad.**

Beneficios

- **Mayor visibilidad y reconocimiento del liderazgo en ciberseguridad.** La participación en eventos nacionales e internacionales permite que la Comunidad de Madrid sea reconocida como actor clave y relevante en el sector de la ciberseguridad.
- **Fortalecimiento de la cooperación público-privada.** La firma de convenios y la cooperación con asociaciones del sector facilitan la coordinación entre administraciones públicas y empresas.
- **Generación de oportunidades de colaboración.** La organización y participación en eventos facilita el contacto entre actores clave del sector.
- **Impulso al desarrollo de talento y formación especializada.** La organización de eventos genera oportunidades para la formación de futuros profesionales.

07

IMPULSAR LA REALIZACIÓN DE EVENTOS Y ALIANZAS ESTRATÉGICAS

E7.M1

Planificación

2025 - 2026

- Participar en **asociaciones y eventos de ciberseguridad** de alcance regional y nacional.
- Fomentar la **organización de eventos de ciberseguridad** en el centro de Innovación Digitaliza Madrid.

2027 - 2028

- Participar en **asociaciones y eventos de ciberseguridad** de alcance nacional e internacional.
- Organizar **un evento de ciberseguridad** de alcance **nacional**.
- Colaborar en eventos para difundir los **objetivos y logros conseguidos por la Agencia** y la Comunidad de Madrid en materia de ciberseguridad.
- **Fomentar la organización de eventos** de ciberseguridad en el centro de Innovación Digitaliza Madrid.

07

IMPULSAR LA REALIZACIÓN DE EVENTOS Y ALIANZAS ESTRATÉGICAS

E7.M2 Fomentar la inversión privada

El desarrollo de un **ecosistema sólido** en ciberseguridad requiere de una estrategia que **impulse la inversión privada** en el sector, facilitando el crecimiento de nuevas empresas, el desarrollo de nuevas tecnologías y la creación de empleo especializado.

En este contexto, el eje estratégico **Fomentar la Inversión Privada** tiene como objetivo principal atraer capital privado hacia empresas y startups de ciberseguridad en la Comunidad de Madrid. Para ello, se implementarán diversas acciones como la creación de Centros de Excelencia con universidades y el fomento de nuevas startups de ciberseguridad.

Objetivos

1. **Atraer inversión privada hacia el sector de la ciberseguridad,** facilitando el acceso de empresas y startups a fuentes de financiación.
2. **Facilitar y fomentar la creación de nuevas startups** dedicadas al ámbito de la ciberseguridad.
3. **Impulsar el desarrollo e investigación en diversas capacidades de ciberseguridad,** a partir de la creación de Centros de Excelencia.

Beneficios

- **Mayor acceso a financiación y recursos para startups,** asegurando su crecimiento y sostenibilidad.
- **Incremento del empleo** y profesionales especializados en ciberseguridad.
- **Aceleración del desarrollo tecnológico y la competitividad** en el sector de la ciberseguridad, gracias a la existencia de Centros de Excelencia, donde se desarrollan soluciones avanzadas y se promueve una innovación constante.

07

IMPULSAR LA REALIZACIÓN DE EVENTOS Y ALIANZAS ESTRATÉGICAS

E7M2

Planificación

2025 - 2026

- Fomentar la creación de **Centros de Excelencia** con universidades para impulsar **capacidades en ciberseguridad** (Inteligencia Artificial, Blockchain, 5G, RPA, cuántica).
- Fomentar la **creación de startups de Ciberseguridad** a través del Cluster CyberMadrid.

2027

- Mantener los centros creados e impulsar acuerdos.
- Fomentar la creación de **Centros de Especialistas** con universidades para impulsar **capacidades en ciberseguridad**.

2028

- Mantener la colaboración con estos **centros de excelencia** y fomentar el incremento de sus capacidades de ciberseguridad.

E7.M3 Alianzas estratégicas

El pilar que aborda las **'Alianzas Estratégicas'** tiene como objetivo fortalecer y expandir la presencia de la Comunidad de Madrid en el sector de la ciberseguridad mediante la colaboración estrecha con **actores clave**. Este eje busca establecer **alianzas duraderas y estratégicas con multinacionales tecnológicas de Cloud y Ciberseguridad,** así como con otras organizaciones y empresas relevantes, tanto nacionales como internacionales. Estas alianzas permitirán el **acceso a tecnologías avanzadas**, el **intercambio de conocimientos y mejores prácticas y la innovación** en ciberseguridad.

07

E7

IMPULSAR LA REALIZACIÓN DE EVENTOS Y ALIANZAS ESTRATÉGICAS

E7.M3

Alianzas estratégicas

Objetivos

1. **Establecer alianzas estratégicas** con empresas líderes internacionalmente tanto en servicios de computación en la nube como en especialistas de ciberseguridad.

2. **Fortalecer relaciones y promover el intercambio de conocimientos** y mejores prácticas entre actores claves del sector.

Planificación

2025 - 2026

- Firmar convenios con **multinacionales tecnológicas de Ciberseguridad**.
- Firmar convenios con **multinacionales tecnológicas especializadas en servicios de computación en la nube (Cloud).**

2027

- Actualizar **alianzas estratégicas** con empresas, organizaciones y actores relevantes nacionales e internacionales.

2028

- Actualizar y ampliar **alianzas estratégicas** con empresas, organizaciones y actores relevantes nacionales e internacionales.

Beneficios

- **Acceso a las tecnologías e infraestructuras más avanzadas y novedosas.** Los convenios con multinacionales suponen la posibilidad de tener acceso a los últimos recursos tecnológicos.

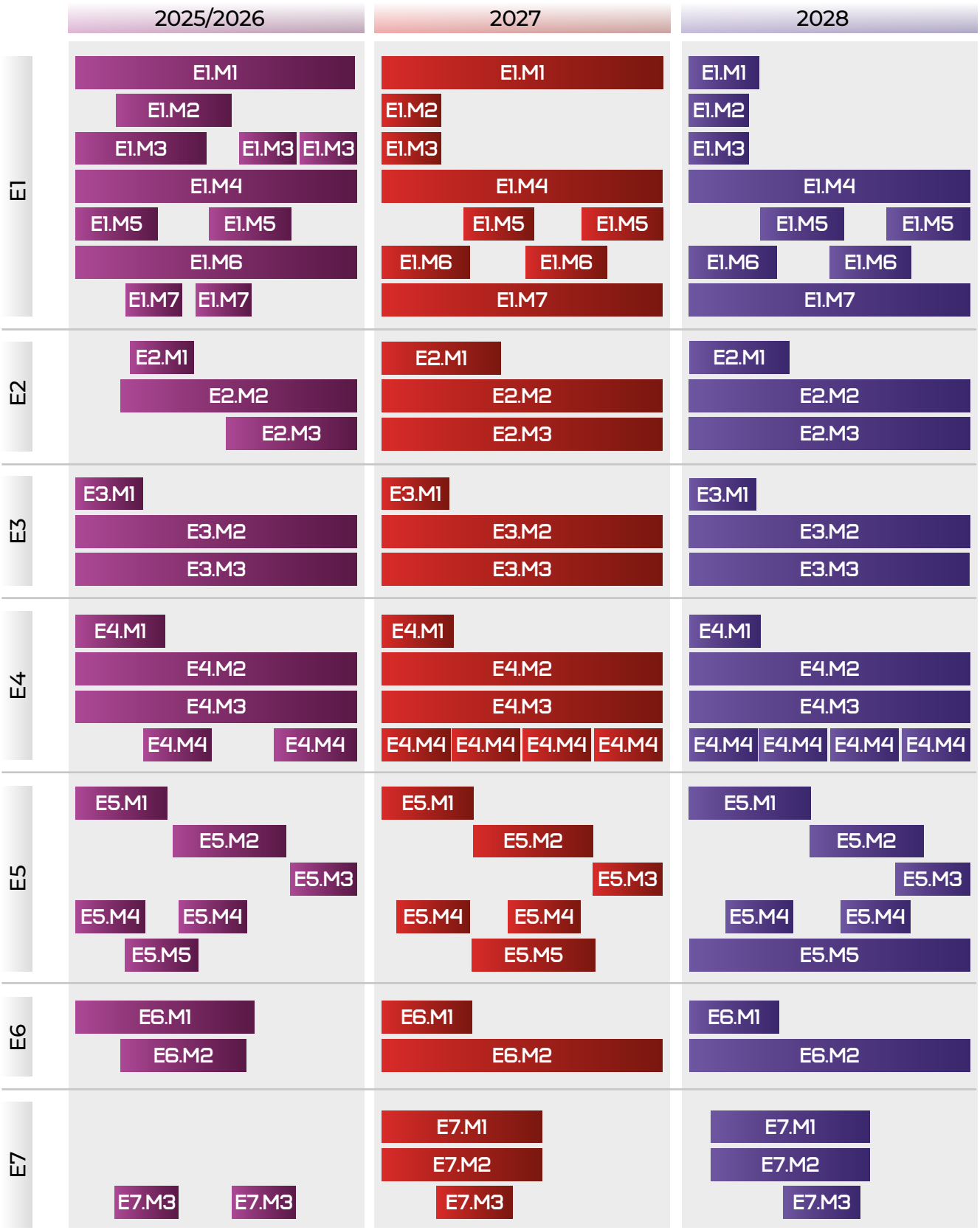
- **Posicionamiento internacional.** Colaborar con multinacionales ayudará a destacar a la Comunidad de Madrid como referente internacional en el sector de la ciberseguridad.

- **Mejora de la resiliencia digital.** Firmar convenios con empresas internacionales ayuda a fortalecer la resiliencia frente a ciberamenazas.

- **Fomento de la Innovación y el Emprendimiento.** El acceso a recursos tecnológicos y la colaboración con empresas líderes fomentarán la **creación de nuevas soluciones** y la **innovación en ciberseguridad,** lo que beneficiará a las **startups locales** y a **nuevos emprendedores** en el ámbito tecnológico.

Planificación de actividades 2025 - 2028

El cronograma a continuación muestra una planificación a alto nivel de las actividades de la Agencia en el 2025-2028 para cada una de las líneas estratégicas.



Plan de ampliación del personal

La plantilla irá aumentando progresivamente para cumplir con la misión encomendada a la Agencia con el objetivo de dar una cobertura de ciberseguridad completa a los ciudadanos, PYMES, entidades locales y organismos públicos de la región.

La estructura organizativa de la Agencia irá evolucionando, incrementando su número de Subdirecciones Generales y definiendo nuevas Oficinas y áreas de acuerdo a las necesidades y retos de ciberseguridad a los que se enfrenta la Comunidad de Madrid.

Asimismo, en respuesta al incremento sostenido de los ciberataques y a las nuevas exigencias normativas, como la directiva NIS2 y el marco regulatorio nacional, la Agencia consolidará áreas clave como la supervisión del cumplimiento, la gestión de crisis cibernéticas y la formación especializada de talento.

Este modelo permitirá una actuación más eficaz frente a los retos específicos del tejido económico y social madrileño.

5.
Seguimiento del Plan Estratégico

AGENCIA DE CIBERSEGURIDAD

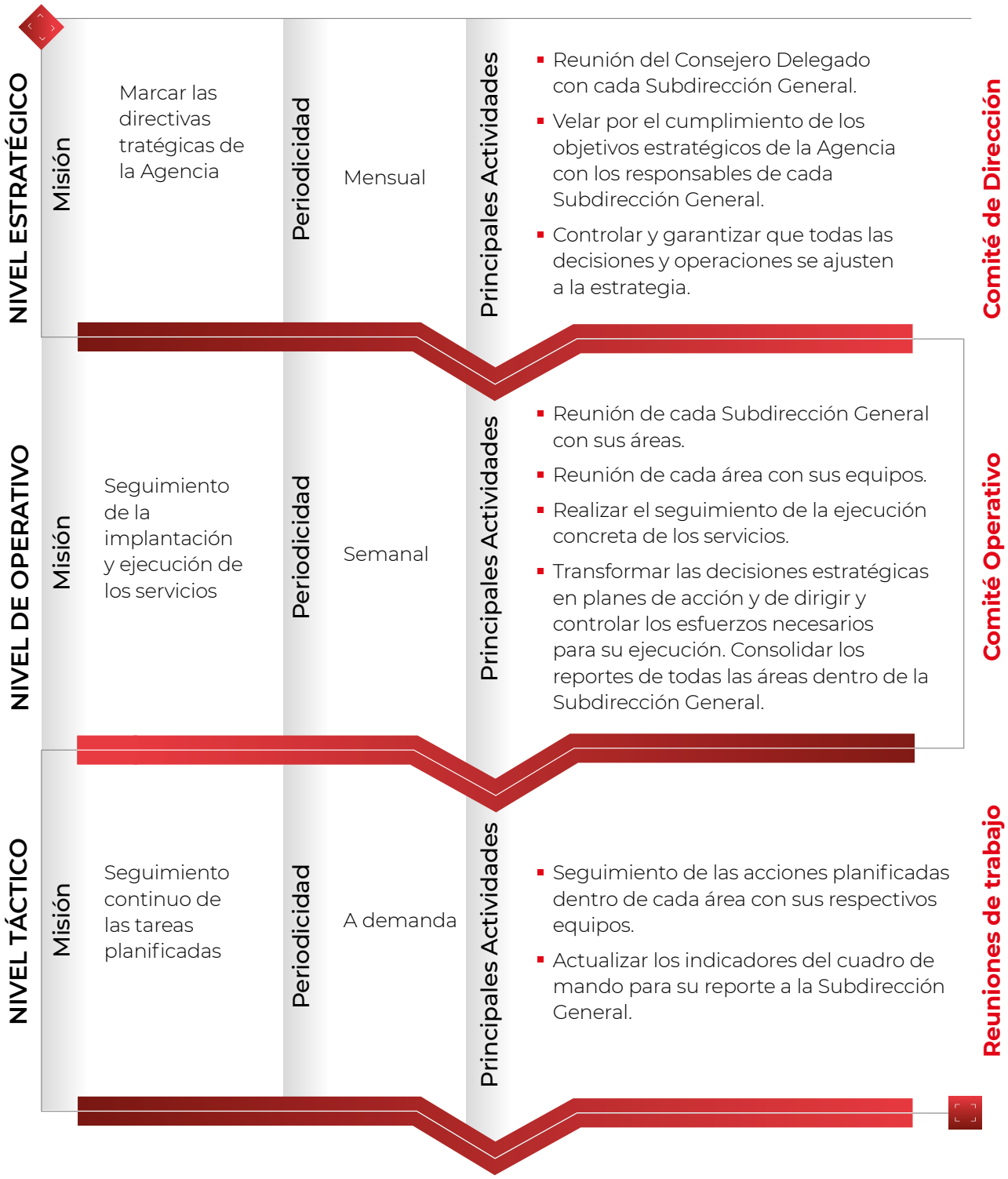
El seguimiento del Plan Estratégico se llevará a cabo mediante el empleo de varios mecanismos: la elaboración de informes de seguimiento, la celebración de comités de seguimiento, así como el uso de indicadores de rendimiento (KPIs).

Comité de Seguimiento

Se elaborarán **informes anuales** para la **evaluación y seguimiento** del plan estratégico de la Agencia de Ciberseguridad, enfocándose en aspectos clave como:

- El **estado general de las medidas asociadas** a cada línea.
- Su **evolución** en el tiempo y las medidas correctoras que fueran necesarias para su mejora.
- Las **incidencias y los riesgos detectados** en la ejecución y las medidas mitigadoras.
- Las **adaptaciones necesarias**, cuando se produzcan cambios sustanciales que modifiquen los objetivos estratégicos del Plan o identifiquen nuevas necesidades y prioridades.
- La **propuesta de nuevas acciones**.

Respecto al funcionamiento interno de la Agencia y el **cumplimiento de los hitos establecidos en el Plan Estratégico,** se establecerá un seguimiento a nivel estratégico, operativo y táctico para garantizar un seguimiento a todos los niveles.



Comité Estratégico	Comité Operativo	Comité Táctico
En el nivel estratégico, el consejero delegado de la Agencia se reunirá con el líder de cada Subdirección General (S.G) con el objetivo de realizar un seguimiento de las grandes líneas de trabajo que son competencia de cada una, y como estas líneas de trabajo dan cumplimiento a los hitos estratégicos definidos en el Plan Estratégico de la Agencia en tiempo y forma. Se elaborará un informe de seguimiento con carácter trimestral donde se indicará de manera ejecutiva cual es el estado de para cada uno de los ejes estratégicos y si existen desviaciones respecto al plan estratégico para realizar los ajustes necesarios.	En estos comités se reúne el líder de cada S.G con sus respectivas áreas para transformar las decisiones estratégicas a un nivel operativo, A nivel de S.G se hará un seguimiento ejecutivo del estado para cada uno de los servicios con las entidades locales y organismos públicos de la Comunidad de Madrid, identificando riesgos y áreas de mejora. Los líderes de cada área deberán de consolidar los informes de seguimiento que han sido elaborados a un nivel táctico por sus respectivos equipos para cada área.	A nivel táctico se realizará un seguimiento de las acciones ejecutadas por cada área con sus respectivos equipos. Se irán actualizando los indicadores del cuadro de mando táctico para generar informes sobre el estado de cada uno de los servicios e iniciativas ejecutadas. Los líderes de las áreas consolidarán la información proporcionada a nivel táctico por los equipos para generar informes que serán escalados al comité operativo.

Indicadores de Rendimiento (KPIs)

1 Definición de indicadores por cada línea Estratégica

Para **cada línea del Plan Estratégico** se deberán establecer unos **indicadores** que posibilitarán un seguimiento preciso del **impacto real de las iniciativas** implementadas.

El conjunto total de éstos conforman el **sistema de métricas** de la Agencia de Ciberseguridad de la Comunidad de Madrid, que facilitará la **evaluación** de la actividad y los **resultados**, así como el **impacto, la efectividad y la eficiencia** de la Estrategia.

Estos indicadores deben ser:

- **Específicos:** Relacionados directamente con los objetivos de la estrategia.
- **Medibles:** Basados en datos cuantificables para facilitar su análisis.
- **Alcanzables:** Realistas y adaptados a los recursos disponibles.
- **Relevantes:** Con impacto directo en la ciberseguridad de la Comunidad de Madrid.
- **Temporales:** Evaluados periódicamente para garantizar un seguimiento continuo.

2 Clasificación de Indicadores

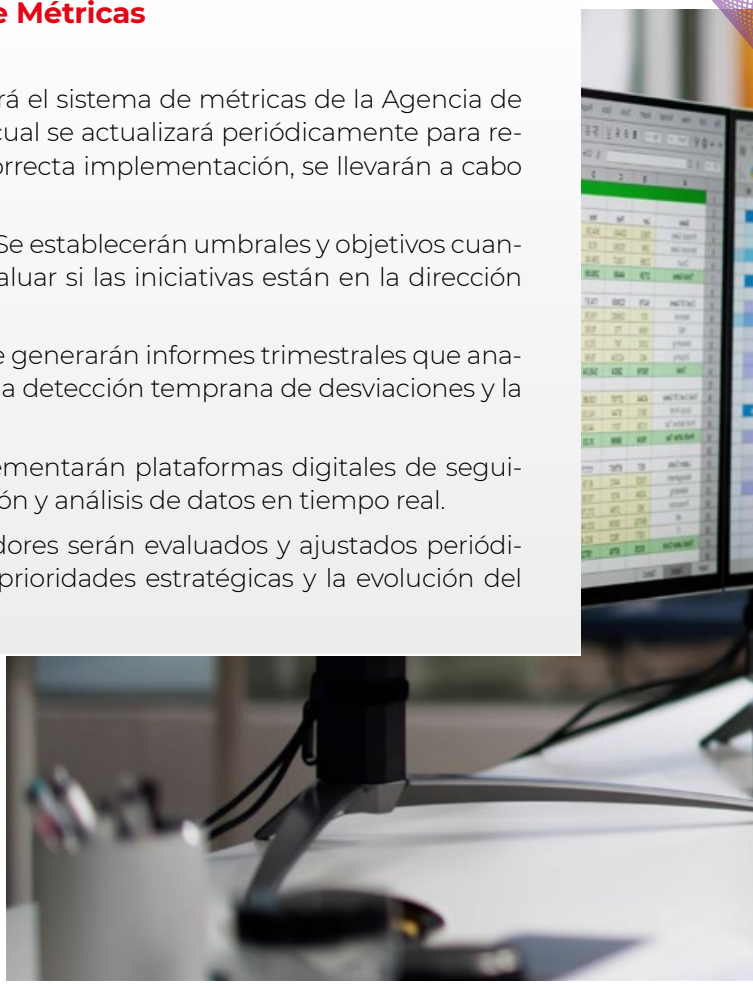
Los indicadores se agruparán en distintas categorías para ofrecer una visión integral del desempeño del plan:

- **Indicadores de Actividad:** Miden la ejecución de las acciones previstas, como el número de campañas de concienciación realizadas o la cantidad de auditorías de seguridad efectuadas.
- **Indicadores de Resultados:** Evalúan el impacto inmediato de las acciones, por ejemplo, el porcentaje de usuarios que adoptan nuevas medidas de ciberseguridad tras una capacitación.
- **Indicadores de Impacto:** Reflejan los efectos a medio y largo plazo de las iniciativas, como la reducción del número de incidentes de ciberseguridad en la Comunidad de Madrid.
- **Indicadores de Eficiencia:** Analizan la relación entre los recursos utilizados y los resultados obtenidos, garantizando una óptima asignación de presupuesto y esfuerzo.
- **Indicadores de Efectividad:** Determinan en qué medida las acciones están logrando los objetivos estratégicos planteados.

3 Implementación del Sistema de Métricas

El conjunto total de estos indicadores conformará el sistema de métricas de la Agencia de Ciberseguridad de la Comunidad de Madrid, el cual se actualizará periódicamente para reflejar los avances del plan estratégico. Para su correcta implementación, se llevarán a cabo las siguientes acciones:

- **Definición de Metas y Valores de Referencia:** Se establecerán umbrales y objetivos cuantificables para cada indicador, permitiendo evaluar si las iniciativas están en la dirección correcta.
- **Monitoreo Continuo y Reportes Periódicos:** Se generarán informes trimestrales que analizarán el estado de cada indicador, facilitando la detección temprana de desviaciones y la adopción de medidas correctivas.
- **Uso de Herramientas Tecnológicas:** Se implementarán plataformas digitales de seguimiento que permitan la recolección, visualización y análisis de datos en tiempo real.
- **Revisión y Ajuste de Indicadores:** Los indicadores serán evaluados y ajustados periódicamente para asegurar su alineación con las prioridades estratégicas y la evolución del panorama de ciberseguridad.



4 Beneficios del Sistema de Indicadores

El uso de estos indicadores proporcionará múltiples beneficios para la Agencia y la Comunidad de Madrid:

- **Mayor Transparencia:** Facilitará la comunicación de los avances y resultados a los ciudadanos y entidades involucradas.
- **Mejor Toma de Decisiones:** Permitirá identificar áreas de mejora y optimizar la asignación de recursos.
- **Alineación Estratégica:** Garantizará que todas las iniciativas contribuyan efectivamente a los objetivos generales de la estrategia.
- **Adaptabilidad:** Permitirá ajustar el plan estratégico según la evolución del contexto y las nuevas amenazas en ciberseguridad.

PLAN ESTRATÉGICO

AGENCIA DE CIBERSEGURIDAD

de la Comunidad de Madrid

AGENCIA DE CIBERSEGURIDAD