Junta de Andalucía

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa
Agencia Digital de Andalucía

Estrategia Andaluza de Ciberseguridad 2022 - 2025

Contenido

Agencia Digital de Andalucía
Dirección General de Estrategia Digital

T: 955061501
dged.ada@juntadeandalucia.es

1. Resumen ejecutivo

La transformación digital y la evolución de las Tecnologías de Información y Comunicación (TIC) han impulsado un cambio sin precedentes en la sociedad, habilitando la interconexión de personas y dispositivos a través del denominado ciberespacio, creando modelos de trabajo virtuales, y estableciendo nuevos mecanismos de tratamiento y compartición de la información.

Esta situación genera una mayor distribución de los datos, aumentando el nivel de exposición a vulnerabilidades y amenazas, cada vez más complejas, difíciles de detectar, contener y resolver.

Bajo este contexto, la ciberseguridad se ha convertido, más que nunca, en un reto global que traspasa fronteras y que afecta por igual a la ciudadanía, Administraciones Públicas y empresas, tanto a nivel nacional como internacional.

La Administración de la Junta de Andalucía, consciente de la complejidad de este nuevo panorama, identifica la ciberseguridad como uno de los pilares fundamentales sobre los que construir una sociedad y una economía digital, de modo que se potencie la mejora del nivel de ciberseguridad, dotando de confianza y garantías digitales a la ciudadanía andaluza, y velando por la disponibilidad de los operadores críticos, servicios esenciales y sectores estratégicos de la Comunidad Autónoma.

La Estrategia Andaluza de Ciberseguridad (en adelante, Estrategia) constituye el vínculo entre la Administración Autonómica y la ciberseguridad, estableciendo las líneas maestras que deben llevarse a cabo para dar respuesta a los retos y desafíos de la sociedad andaluza.

La Estrategia contiene los retos, objetivos y líneas de actuación en materia de ciberseguridad para los años 2022 – 2025, involucrando a la Administración Pública de Andalucía, la ciudadanía, el sector privado y las entidades más representativas del sector.

La Administración Autonómica debe afrontar cuatro grandes retos, derivados de la digitalización y evolución tecnológica de la sociedad, a los cuales se les pretende dar respuesta a través de un escenario objetivo que permita a Andalucía convertirse en un territorio de referencia en materia de ciberseguridad:

- R1 – Transformación digital de la Administración.
- R2 – Liderazgo en ciberseguridad.
- R3 – Evolución en la Ciberseguridad en el sector privado.
- R4 – Desarrollo y atracción del talento.

La Estrategia define ocho objetivos para hacer frente a los retos identificados anteriormente, teniendo en cuenta el conjunto de principios por los que se rige, orientados a la colaboración entre entidades, la cibercultura en la ciudadanía, la resiliencia ante incidentes y la digitalización segura del sector público y privado:

- OE1 – Fortalecer las estructuras de gobierno.
- OE2 – Reforzar las capacidades de prevención, detección y respuesta a incidentes.
- OE3 – Cooperar y colaborar en aras de extender la capacidad de protección.
- OE4 – Situar a Andalucía como referente a nivel nacional e internacional en ciberseguridad.
- OE5 – Mejorar las capacidades de ciberseguridad en las empresas andaluzas.
- OE6 – Poner en marcha medidas para el desarrollo de una industria de ciberseguridad.
- OE7 – Potenciar el talento y competencias de ciberseguridad en la ciudadanía y profesionales.
- OE8 – Mejorar la cultura y buenas prácticas de ciberseguridad.

Alineadas con los objetivos se establecen ocho líneas de actuación en la Estrategia que posibilitan su implantación exitosa, permitiendo a Andalucía avanzar hacia una sociedad digital segura y confiable:

- LA1 – Evolución y mejora de las estructuras organizativas en materia de ciberseguridad dando cobertura a la visión interna y externa de la Administración de la Junta de Andalucía.
- LA2 – Definición e implantación de un plan de desarrollo y mejora continua de las capacidades de prevención, detección y respuesta a incidentes de AndalucíaCERT.
- LA3 – Fortalecimiento y desarrollo de marcos de cooperación y colaboración en diferentes ámbitos, tanto a nivel autonómico, nacional e internacional.
- LA4 – Creación y desarrollo de un plan de promoción de Andalucía, posicionándola como territorio de referencia en materia de ciberseguridad.
- LA5 – Desarrollo de programas para el impulso y financiación de la ciberseguridad en el sector empresarial andaluz, favoreciendo la mejora de su nivel de madurez.
- LA6 – Establecimiento de planes de desarrollo de una industria especializada en el sector de la ciberseguridad en el territorio andaluz.
- LA7 – Elaboración y despliegue de programas formativos con contenidos de ciberseguridad, así como de planes de formación continua y reciclaje para profesionales del sector.
- LA8 – Promoción de la concienciación y sensibilización en ciberseguridad y fomento de las buenas prácticas en el uso de las TIC en la Administración, ciudadanía y empresas.

2. Propósito y principios de la Estrategia

La digitalización es uno de los ejes prioritarios de actuación para la Administración Autonómica, que actualmente se encuentra inmersa en un proceso de transformación liderado por la Agencia Digital de Andalucía. En esta línea, la ciberseguridad se erige como un pilar estratégico, que persigue proteger a la sociedad andaluza en su conjunto ante el cibercrimen y que, además, pretende aprovechar el alto potencial de crecimiento del sector de la ciberseguridad en Andalucía, de modo que contribuya tanto a la creación de riqueza y empleo en la Comunidad Autónoma como a la consecución de los Objetivos de Desarrollo Sostenible (ODS) y metas establecidas en la Agenda 2030.

Propósito

La Estrategia tiene el propósito de construir el vínculo entre la Administración de la Junta de Andalucía y la ciberseguridad, estableciendo las líneas maestras que deben llevarse a cabo durante el periodo 2022 a 2025 para dar respuesta a los retos y desafíos de la sociedad andaluza. En consecuencia, promueve y habilita el uso seguro de las redes y sistemas de información, prestando especial atención a los operadores críticos, servicios esenciales y sectores estratégicos de la Comunidad Autónoma, y permitiendo el posicionamiento de Andalucía entre las economías digitales más avanzadas.

Principios

Al establecer los principios de la Estrategia es fundamental destacar la necesidad de colaboración y participación de todos los colectivos que forman parte del actual ecosistema digital hiperconectado, donde la responsabilidad en materia de ciberseguridad es compartida: ciudadanía, empresas, instituciones y agentes sociales y económicos.

Bajo esta premisa, se define el conjunto de principios que rigen la presente Estrategia y deben ser la base para una implementación exitosa.

- Colaboración entre entidades. Para un adecuado despliegue de la Estrategia es necesario disponer de modelos organizativos y de relación que habiliten la colaboración entre entidades. En esta línea, es fundamental crear estructuras conjuntas, basadas en marcos de cooperación y alineamiento entre Administraciones Públicas, empresas del sector privado, universidades y organismos de referencia a nivel nacional e internacional. Todo ello facilitará la definición e implantación eficaz y compartida de acciones y planes.

- Ciberseguridad como elemento fundamental en la digitalización. La digitalización de las empresas, administraciones y ciudadanía andaluzas es uno de los elementos clave para la mejora de los servicios públicos prestados y el avance tecnológico de la Comunidad Autónoma. Sin embargo, la evolución de las TIC trae consigo nuevas amenazas y riesgos que deben ser gestionados. Por ello, la ciberseguridad debe incorporarse desde el diseño en los procesos, dando respuesta a los retos a los que se enfrenta Andalucía y generando confianza en la sociedad.

- Cultura de la Ciberseguridad en la sociedad andaluza. Dado que actualmente las TIC se consideran un instrumento fundamental para la comunicación, el libre acceso a la información y la transmisión de datos es necesario hacer un uso seguro y responsable de las mismas. Con este fin,

la cultura en ciberseguridad ha de ser uno de los ejes centrales para el desarrollo de una sociedad capacitada y conocedora de las amenazas y riesgos derivados del entorno digital actual. Por ello, la Administración de la Junta de Andalucía debe integrar la cibercultura como un mecanismo esencial para la correcta utilización de las TIC, en un entorno cada vez más complejo y cambiante.

- Servicios públicos avanzados y seguros. La prestación de servicios públicos avanzados y seguros debe ser uno de los aspectos clave de la Administración de la Junta de Andalucía, que requiere de la utilización de tecnologías emergentes y de la implantación de controles de ciberseguridad en los procesos digitales que cubran las necesidades de la ciudadanía y las empresas. Los servicios públicos deben ser homogéneos, seguros y de fácil acceso, de modo que incorporen ciberseguridad como un elemento clave que permita generar un clima de confianza y seguridad en la utilización de las nuevas tecnologías.
- Resiliencia. La Estrategia debe estar orientada a la mejora de la resiliencia de las redes y sistemas de información de las administraciones y empresas andaluzas, prestando especial atención a los operadores críticos y de servicios esenciales, de modo que Andalucía cuente con una protección adecuada en materia de ciberseguridad, anticipándose de forma eficiente a las ciberamenazas y dando una respuesta eficaz a los posibles incidentes de seguridad que puedan producirse. En esta línea es fundamental la implementación de medidas de ciberseguridad que permitan una gestión adecuada frente a eventos disruptivos que afecten a los activos tecnológicos críticos para la sociedad andaluza.

3. Contexto global de la ciberseguridad

El ecosistema tecnológico ha cambiado de manera exponencial en los últimos años, impulsado por la transformación digital y la evolución de las TIC. Como resultado de ello, se evidencia un nuevo paradigma de interconexión y de relación entre personas usuarias, que tiene su base en el uso y explotación del denominado ciberespacio (ámbito virtual creado por tecnologías digitales interconectadas). Este nuevo escenario ha eliminado barreras como la distancia y la necesidad de espacios físicos en lo que a distribución, compartición y acceso a información se refiere, ocasionando grandes avances tanto en la economía como en la sociedad. Del mismo modo, ha generado una mayor dependencia de las TIC, incrementando la complejidad de los sistemas de información utilizados y aumentando el número de vulnerabilidades y amenazas, que cada vez son más complejas, diversas y difíciles de detectar.

Esta situación se ha visto acentuada por la pandemia provocada por la COVID-19, que ha digitalizado a la sociedad en diferentes ámbitos (relaciones personales, educación, entretenimiento, etc.), cambiando los modelos de trabajo tradicionales, aumentando el nivel de exposición de la ciudadanía, empresas, administraciones y organismos públicos y multiplicado los vectores de ataque.

En los últimos años, la Administración Pública se ha convertido en uno de los principales objetivos de los ciberdelincuentes, siendo ésta una de las preocupaciones de cualquier Estado de Derecho.

Bajo este contexto, la Unión Europea (UE) ha visto la necesidad de salvaguardar a la ciudadanía a través del impulso de medidas de protección en sus sistemas y redes, con especial atención a los operadores críticos

y de servicios esenciales, del fomento de una cultura de ciberseguridad y del refuerzo de la cooperación entre entidades, tanto públicas como privadas, de modo que se pueda hacer frente a los desafíos emergentes de la ciberseguridad. Por ello, a finales de 2020, la UE elaboró la denominada "Estrategia de Ciberseguridad de la UE para la Década Digital", cuyas principales líneas de actuación son: "aumentar la seguridad de los servicios esenciales y de los dispositivos conectados, reforzar las capacidades colectivas para responder a los principales ciberataques y cooperar con socios a nivel mundial para garantizar la seguridad internacional y la estabilidad en un ciberespacio global, abierto, estable y seguro, basado en el Estado de Derecho y libertades fundamentales"[1].

En España, el Consejo de Seguridad Nacional aprobó en 2019 la "Estrategia Nacional de Ciberseguridad", cuyo objetivo, alineado con las principales líneas de actuación de la UE, es: "garantizar el uso fiable y seguro del ciberespacio, protegiendo los derechos y libertades de los ciudadanos y promoviendo el progreso económico"[2].

Recientemente, se ha desarrollado la Estrategia de Seguridad Nacional 2021[3], que constata que la ciberseguridad es una prioridad de organizaciones y gobiernos, aboga por un incremento de las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional para la prevención, detección, respuesta, recuperación, investigación y defensa activa y destaca como aspecto relevante el desarrollo de las infraestructuras de ciberseguridad en las Comunidades y Ciudades Autónomas.

En línea con lo anterior, durante los últimos años la regulación y normativa aplicable, tanto a nivel nacional como internacional, ha evolucionado de manera constante, con el objetivo de dar respuesta a los nuevos retos que plantea la ciberseguridad, así como de regular los principales ámbitos de protección de la información y de sus propietarios.

En este ámbito cabe mencionar las principales regulaciones de referencia en materia de seguridad a nivel nacional:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- 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.
- 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.

1 The EU's Cybersecurity Strategy for the Digital Decade. Fecha: Diciembre 2020. Autor: ENISA

2 Estrategia Nacional de Ciberseguridad 2019. Fecha: Abril 2019. Autor: Departamento de Seguridad Nacional. Presidencia del Gobierno.

3 Estrategia de Seguridad Nacional 2021 Fecha: Diciembre 2021. Autor: Departamento de Seguridad Nacional. Presidencia del Gobierno. (https://www.dsn.gob.es/es/estrategias#publicaciones/estrategias/estrategia-seguridad-nacional-2021)

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por otro lado, las principales regulaciones de referencia en materia de seguridad en el ámbito de la Unión Europea son las siguientes:

- 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).
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- 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»).

En resumen, el mundo está viviendo una transformación global sin precedentes, donde la rápida evolución de la tecnología ha cambiado la forma de interactuar y compartir información entre las personas, dando lugar a nuevos riesgos y desafíos. Para hacer frente a este nuevo escenario, gobiernos y organismos, tanto a nivel nacional como europeo, han definido estrategias, políticas y regulaciones en el ámbito de la ciberseguridad, buscando proteger a la sociedad en su conjunto y combatir el cibercrimen.

4. Evolución y situación actual de la ciberseguridad

Andalucía, en su propósito de garantizar un espacio digital ciberseguro, no puede ser ajena al nuevo escenario al que se enfrenta la sociedad, que impacta directamente en todos los sectores estratégicos de la Comunidad Autónoma e indirectamente en la industria y economía nacional y europea, debiendo considerar el uso seguro de las TIC y la protección de la información como algo imprescindible para el buen funcionamiento de los servicios y sistemas soportados en el ciberespacio, así como ofrecer garantías y confianza digital a la sociedad.

Para adaptarse a la rápida evolución de la tecnología y al entorno cambiante en el que se vive, así como ser capaz de cubrir la demanda de la ciudadanía en materia de ciberseguridad, la Administración de la Junta de Andalucía ha desarrollado múltiples iniciativas a lo largo de los años.

Cabe destacar la definición y ejecución del Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía, y del Plan de Seguridad y Confianza Digital de Andalucía en los que se establecen diferentes líneas de actividad, siendo la más significativa el despliegue y explotación de un centro de seguridad TIC, AndalucíaCERT, como instrumento de referencia para la prevención, detección y respuesta a incidentes y amenazas en el ámbito de la Administración Autonómica Andaluza.

Adicionalmente, la Administración de la Junta de Andalucía cuenta con su política de seguridad, establecida en los Decretos 1/2011, de 11 de enero, y 70/2017, de 6 de junio, y con convenios de colaboración con el Centro Criptológico Nacional (CCN), que recogen medidas y actuaciones coordinadas entre ambas instituciones.

Continuando con su decidida apuesta por la ciberseguridad y la mejora de los servicios públicos a través de soluciones digitales, en 2021, la Administración de la Junta de Andalucía creó la Agencia Digital de Andalucía (ADA), lo que ha supuesto una gran oportunidad para la transformación digital de la Comunidad Autónoma, la racionalización en la prestación de servicios, así como la mejora en la gestión de los recursos tecnológicos y su sostenibilidad económica. Este nuevo organismo facilita el avance hacia una estrategia común en el ámbito de la digitalización y la ciberseguridad.

Ese mismo año, el 3 de agosto, se aprobó el acuerdo para la formulación de la Estrategia Andaluza de Ciberseguridad 2022 – 2025, que dio lugar al presente documento.

En base a lo expuesto en este apartado, se puede concluir que la Junta apuesta de manera determinada por la ciberseguridad, dando respuesta a los retos y desafíos a los que se enfrente una sociedad cada vez más digitalizada e hiperconectada a través de las TIC, e intentando posicionar a Andalucía como una economía digital de referencia a nivel nacional e internacional.

5. Retos

Para la elaboración de la Estrategia Andaluza de Ciberseguridad 2022 – 2025, se considera clave analizar la situación de partida de Andalucía en materia de ciberseguridad, tanto desde una perspectiva interna como externa, permitiendo detectar las debilidades y amenazas a las que se enfrenta, así como las fortalezas y oportunidades de las que dispone. Este análisis permite identificar los principales retos y desafíos de la sociedad andaluza durante los próximos años, derivados principalmente de los procesos de digitalización y evolución tecnológica en los que está inmerso el mundo actual.

5.1. R1 – Transformación digital en la Administración

La transformación digital en la Administración Pública supone un reto, no solo en la adecuación de los procesos y herramientas que soportan la prestación de los servicios públicos digitales, sino por la manera de trabajar, comunicar y dar respuesta a las necesidades y requerimientos de la sociedad.

El 82% de las personas usuarias españolas con acceso a internet participan activamente en los servicios de Administración Electrónica, una puntuación muy superior a la media de la Unión Europea que es del 67%.[4]

En consecuencia, Andalucía debe ser capaz de adaptarse rápidamente a la evolución de la tecnología para responder a la demanda de la ciudadanía a través de nuevas tecnologías, principalmente cloud, big data, automatización robótica de los procesos (RPA) e Inteligencia Artificial (IA).

Estas tecnologías, además de tender a la centralización de las operaciones, hacen un uso masivo de datos, lo que obliga a la Administración a fijar medidas y controles de seguridad adicionales en sus sistemas,

4 Índice de Economía y Sociedad Digital (DESI, por sus siglas en inglés), compara anualmente la evolución digital de los Estados que conforman la Unión Europea.

infraestructura y servicios esenciales para garantizar la protección de la información y afianzar la confianza de la sociedad en los mismos.

5.2. R2 – Liderazgo en ciberseguridad y colaboración entre entidades

En los últimos años, tanto Administraciones Públicas como organismos de referencia se han convertido en uno de los principales objetivos de los ciberataques, que a través de campañas tradicionales de denegación de servicio distribuido (DDoS), infección de ransomware o acciones de phishing, entre otras, han visto comprometidos sus servicios y la seguridad de los datos tratados.

En respuesta a este hecho, por ejemplo, la Comisión Europea promueve la creación de una Unidad Cibernética para hacer frente al número creciente de incidentes de ciberseguridad graves que afectan a servicios públicos, empresas y a la ciudadanía[5].

La Administración de la Junta de Andalucía necesita situarse como referente y mantener una posición firme en materia de ciberseguridad, que permita garantizar servicios y políticas públicas que generen confianza a la ciudadanía. Para ello, el despliegue de la ciberseguridad debe convertirse en uno de los ejes principales sobre los que construir la digitalización de la sociedad andaluza.

Este liderazgo debe permitir impulsar mecanismos de colaboración y cooperación entre diferentes entidades, tanto públicas como privadas, a nivel nacional e internacional, que permitan mejorar las capacidades en materia de ciberseguridad de la Administración Andaluza y proporcionen visibilidad sobre el trabajo realizado en este ámbito.

5.3. R3 – Evolución de la ciberseguridad en el sector privado

Debido al incremento del número de ataques dirigidos a empresas y la dependencia tecnológica de éstas, la ciberseguridad se ha convertido en uno de los riesgos más relevantes. Por ello, el sector privado debe incorporar la ciberseguridad dentro de sus prioridades estratégicas de transformación digital, para asegurar sus servicios, infraestructuras y redes, así como la protección de la información, generando un clima de confianza entre su clientela.

El mercado español de la ciberseguridad seguirá creciendo. En 2022, como ejemplo, se estimó que las cifras de negocio se incrementen en un 7,7% respecto al año anterior, alcanzando los 1.749 millones de euros. El 90% de las empresas españolas sitúan la ciberseguridad entre sus tres principales prioridades de inversión.[6]

Se presenta, por lo tanto, una gran oportunidad para que las empresas andaluzas puedan acometer actuaciones estratégicas orientadas al desarrollo de una industria de ciberseguridad en Andalucía que contribuya a la mejora económica de la Comunidad Autónoma.

Adicionalmente, la Administración de la Junta de Andalucía, ante la creciente demanda de productos y servicios de ciberseguridad, tiene por delante el reto de fomentar la existencia de una industria

5 Unión Europea – Ciberseguridad Fecha: Junio 2021. Departamento de Seguridad Nacional. (https://www.dsn.gob.es/eu/actualidad/seguridad-nacional-ultima-hora/uni%C3%B3n-europea-%E2%80%93-ciberseguridad-22)

6 La agenda del CISO en 2022. Fecha: Febrero 2022. Autor: IDC Research España

especializada que permita cubrir la demanda, utilizando como palanca los centros de investigación e innovación, actuales o futuros, de empresas relevantes en la materia, la atracción de personal experto y empresas cualificadas, la financiación pública y la captación de capital privado.

5.4. R4 – Cultura de ciberseguridad y desarrollo del talento

El incremento de amenazas en los entornos TIC debido al desarrollo de sistemas cada vez más complejos, interconectados y abiertos y, por tanto, más vulnerables, genera la necesidad de incrementar la cultura de ciberseguridad en la sociedad, así como de promover el desarrollo de profesionales especializados en el sector.

Algunos datos[7] apuntan a las necesidades sobre ese aspecto:

- Casi la mitad de la población española (43%) carece de competencias digitales básicas y un 8% jamás ha utilizado internet.
- La proporción de personas graduadas TIC solo representa un 4% del total de graduaciones.
- La proporción de especialistas en TIC en el empleo total es del 3,2%.
- La participación de mujeres especialistas en TIC permanece estancada durante los últimos cuatro años en torno al 1% del empleo femenino total.

En esta línea, la Administración de la Junta de Andalucía debe promover la sensibilización y concienciación en materia de ciberseguridad entre la ciudadanía y empresas andaluzas, a través de planes y acciones específicos, que permitan conocer y entender los riesgos asociados a las nuevas tecnologías, dotando de capacidades técnicas a la sociedad para hacer frente a las amenazas emergentes derivadas de la transformación digital.

Del mismo modo, Andalucía debe hacer un esfuerzo significativo en la generación y desarrollo de talento especializado, persiguiendo que la juventud y, en especial, las mujeres se sientan atraídos por la ciberseguridad. Para ello, se debe poner foco en la formación especializada, las prácticas profesionales y bolsas de empleo, el reciclaje de profesionales y la reorientación del empleo público.

6. Objetivos estratégicos

Para dar respuesta a los retos identificados, la Estrategia establece los ocho objetivos clave que se quieren alcanzar durante el período de ejecución de la misma, de modo que Andalucía se pueda posicionar como un territorio líder en el sector de la ciberseguridad.

6.1. OE1 – Fortalecer las estructuras de gobierno

Objetivo

Fortalecer las estructuras de gobierno y gestión del riesgo en la Administración Autonómica, buscando el cumplimiento normativo, la coordinación y la especialización en ciberseguridad del personal empleado público.

7 Plan España Digital 2025. Fecha: Julio 2020. Autor: Gobierno de España.

Atiende al reto R1 – Transformación digital de la Administración.

Descripción

En los últimos tiempos se han incrementado significativamente los ciberataques a la Administración Pública, convirtiéndose en uno de los principales objetivos de atacantes malintencionados. Estos ataques tienen diferentes motivaciones como generar una pérdida de prestigio, obtener información clasificada, provocar la indisponibilidad de servicios o reivindicar cuestiones políticas, entre otros. Esta situación, genera la necesidad de que la Administración de la Junta de Andalucía ponga foco y priorice la mejora de las estructuras organizativas de ciberseguridad dentro de las instituciones autonómicas, implantando un modelo operativo con enfoque a la gestión de riesgos, así como procesos unificados y homogéneos de ciberseguridad, que permitan establecer mecanismos adecuados para la protección de la información, en base a la regulación vigente, así como políticas, normas y guías de buenas prácticas que promuevan la aplicación de la ciberseguridad desde el diseño en los sistemas y servicios prestados.

6.2. OE2 – Reforzar las capacidades de prevención, detección y respuesta a incidentes

Objetivo

Reforzar las capacidades de prevención, detección y respuesta a incidentes en la Administración de la Junta de Andalucía a través de servicios avanzados de ciberseguridad.

Atiende al reto R1 – Transformación digital de la Administración.

Descripción

Los incidentes en materia de ciberseguridad no solo pueden tener consecuencias a nivel económico, sino también en lo relativo a daños en la reputación de la Administración, pérdida de confianza de la ciudadanía o incremento de costes operativos, entre otros. Por ello, con el fin de controlar el impacto que pueden producir los ciberincidentes en los servicios públicos, la Administración de la Junta de Andalucía debe fortalecer su Centro de Operaciones de Seguridad (AndalucíaCERT), ampliando sus servicios, su ámbito de actuación y mejorando las herramientas utilizadas. Por otro lado, debe impulsar la coordinación con las Fuerzas y Cuerpos de Seguridad para mejorar la prevención y gestión de incidentes, evolucionar los modelos de gestión de crisis y diseñar planes de continuidad que den respuesta a las necesidades de la Administración Autonómica.

6.3. OE3 – Cooperar y colaborar en aras de extender la capacidad de protección

Objetivo

Cooperar y colaborar en aras de extender la capacidad de protección de la Administración Autonómica Andaluza, así como mejorar las capacidades de ciberseguridad del sector privado y la ciudadanía.

Atiende al reto R2 – Liderazgo en ciberseguridad.

Descripción

La Administración de la Junta de Andalucía debe promover la colaboración y cooperación con diferentes entidades e instituciones públicas y privadas, tanto nacionales como internacionales, especializadas en materia de ciberseguridad. En esta línea, es necesario reforzar los mecanismos de alerta temprana de amenazas y de prevención de incidentes, a través del uso de herramientas específicas de notificación y compartición de datos, de modo que se contribuya a la mejora del nivel de ciberseguridad y de las capacidades de protección del conjunto de entidades del sector público andaluz, como diputaciones provinciales, ayuntamientos y otros entes públicos.

6.4. OE4 – Situar a Andalucía como referente a nivel nacional e internacional en ciberseguridad

Objetivo

Situar a Andalucía como referente a nivel nacional e internacional en el estado del arte de la ciberseguridad.

Atiende al reto R2 – Liderazgo en ciberseguridad.

Descripción

Andalucía debe posicionarse como un territorio líder en materia de ciberseguridad. Para alcanzar dicho objetivo, la Administración de la Junta de Andalucía debe reforzar su presencia en conferencias, foros y otros eventos de especial relevancia, tanto dentro como fuera del territorio nacional, que permitan compartir sus principales proyectos y logros, así como difundir sus capacidades de ciberseguridad. Con ese objetivo, la Comunidad Autónoma pretende dar pasos firmes hacia un ecosistema avanzado y líder, que se encuentre posicionado en los principales índices de referencia, adquiriendo visibilidad y presencia no sólo a nivel nacional, sino también a nivel internacional.

6.5. OE5 – Mejorar las capacidades de ciberseguridad en las empresas andaluzas

Objetivo

Mejorar las capacidades de ciberseguridad en las empresas andaluzas, estableciendo directrices y marcos de evaluación, así como programas de ayuda específicos.

Atiende al reto R3 – Evolución en la Ciberseguridad en el sector privado.

Descripción

A medida que aumenta el número de ciberataques dirigidos a empresas, con el objetivo de obtener información sensible de su negocio, llevar a cabo extorsiones o desprestigiar su imagen, resulta necesario promover la implantación y mejora de capacidades técnicas dentro del sector privado andaluz, así como impulsar la financiación y planes de ayuda que permitan el incremento de su nivel de madurez en materia de ciberseguridad.

6.6. OE6 – Poner en marcha medidas para el desarrollo de una industria de ciberseguridad

Objetivo

Definir y poner en marcha un paquete de actuaciones orientadas al desarrollo de una industria de ciberseguridad en Andalucía que contribuya a la mejora económica de la Comunidad Autónoma.

Atiende al reto R3 – Evolución en la Ciberseguridad en el sector privado.

Descripción

Es importante dirigir los esfuerzos de la Comunidad Autónoma hacia la construcción de un tejido empresarial andaluz dedicado a la ciberseguridad, que permita aprovechar las oportunidades que ofrece un sector en constante crecimiento. Por ello, la Administración de la Junta de Andalucía debe fomentar la creación y dinamización de empresas especializadas, generando una comunidad experta en seguridad TIC, con especial atención a la investigación y la innovación, a la colaboración con centros educativos, así como a la captación y aceleración de la industria de ciberseguridad.

6.7. OE7 – Potenciar el talento y competencias de ciberseguridad en la ciudadanía y profesionales

Objetivo

Potenciar el talento y competencias de ciberseguridad en la ciudadanía y profesionales, promoviendo planes y programas formativos con contenidos específicos.

Atiende al reto R4 – Desarrollo y atracción del talento.

Descripción

Actualmente en el sector TIC y, en particular, en el ámbito de la ciberseguridad, la búsqueda de profesionales se presenta como un importante reto, debido a la brecha existente entre la oferta limitada de perfiles especializados y la elevada demanda existente en el mercado. Abordando este reto, Andalucía debe potenciar la educación en ciberseguridad en centros educativos, ciclos formativos de grado medio y superior, así como en estudios universitarios, para que la ciudadanía tenga unos conocimientos mínimos en la materia adecuados al mundo digital actual. Por otro lado, se debe crear una oferta formativa especializada y atractiva, potenciando las prácticas profesionales y los programas inclusivos y equitativos. Del mismo modo, se debe promover el reciclaje y reorientación de perfiles de alta cualificación, tanto en el sector público como privado, con vistas a crear y retener el talento especializado en ciberseguridad.

6.8. OE8 – Mejorar la cultura y buenas prácticas de ciberseguridad

Objetivo

Mejorar la cultura y buenas prácticas de ciberseguridad en la Administración, ciudadanía y empresas.

Atiende al reto R4 – Desarrollo y atracción del talento.

Descripción

La ciberseguridad es un ámbito que alcanza y puede tener impacto en todo el conjunto de la sociedad. Por ello, la Administración de la Junta de Andalucía debe poner foco en el desarrollo de campañas de concienciación y sensibilización dirigidas a la ciudadanía, Administración Pública y empresas, poniendo especial atención a colectivos vulnerables o con un mayor riesgo de ser víctimas de ciberataques, con el objetivo final de construir una sociedad digital plena, consciente y capacitada en materia de ciberseguridad, que haga un uso seguro y responsable de las TIC.

7. Líneas de actuación

En este capítulo se detallan las líneas de actuación a desarrollar para la consecución de los objetivos establecidos en la Estrategia. Cada línea de actuación está compuesta por una serie de actividades esenciales que pretenden dar respuesta a los retos actuales de la sociedad.

En conjunto, todas las líneas de actuación cubren uno o más de los objetivos establecidos.

LA1 – Evolución y mejora de las estructuras organizativas en materia de ciberseguridad dando cobertura a la visión interna y externa de la Administración de la Junta de Andalucía.

Soporte a OE1 – Fortalecer las estructuras de gobierno.

LA2 – Definición e implantación de un plan de desarrollo y mejora continua de las capacidades de prevención, detección y respuesta a incidentes de AndalucíaCERT.

Soporte a OE2 – Reforzar las capacidades de prevención, detección y respuesta a incidentes.

LA3 – Fortalecimiento y desarrollo de marcos de cooperación y colaboración en diferentes ámbitos, tanto a nivel autonómico, nacional e internacional.

Soporte a OE2 – Reforzar las capacidades de prevención, detección y respuesta a incidentes.

Soporte a OE3 – Cooperar y colaborar en aras de extender la capacidad de protección.

LA4 – Creación y desarrollo de un plan de promoción de Andalucía, posicionándola como territorio de referencia en materia de ciberseguridad.

Soporte a OE4 - Situar a Andalucía como referente a nivel nacional e internacional en ciberseguridad.

LA5 – Desarrollo de programas para el impulso y financiación de la ciberseguridad en el sector empresarial andaluz, favoreciendo la mejora de su nivel de madurez.

Soporte a OE4 - Situar a Andalucía como referente a nivel nacional e internacional en ciberseguridad.

Soporte a OE5 – Mejorar las capacidades de ciberseguridad en las empresas andaluzas.

LA6 – Establecimiento de planes de desarrollo de una industria especializada en el sector de la ciberseguridad en el territorio andaluz.

Soporte a OE4 - Situar a Andalucía como referente a nivel nacional e internacional en ciberseguridad.

Soporte a OE5 – Mejorar las capacidades de ciberseguridad en las empresas andaluzas.

Soporte a OE6 - Poner en marcha medidas para el desarrollo de una industria de ciberseguridad.

LA7 – Elaboración y despliegue de programas formativos con contenidos de ciberseguridad, así como además de planes de formación continua y reciclaje para profesionales del sector.

Soporte a OE7 – Potenciar el talento y competencias de ciberseguridad en la ciudadanía y profesionales.

LA8 – Promoción de la concienciación y sensibilización en ciberseguridad, y fomento de las buenas prácticas en el uso de las TIC en la Administración, ciudadanía y empresas.

Soporte a OE8 – Mejorar la cultura y buenas prácticas de ciberseguridad.

7.1. LA1 – Evolución y mejora de las estructuras organizativas en materia de ciberseguridad dando cobertura a la visión interna y externa de la Administración

Actuaciones

- Mejorar las estructuras organizativas especializadas en materia de ciberseguridad dentro de la Administración de la Junta de Andalucía, identificando roles y responsabilidades de modo que sea posible el despliegue de la Estrategia en todos sus ámbitos.
- Definir y consensuar entre las estructuras organizativas un modelo operativo de ciberseguridad con enfoque a la gestión de riesgos, como establecen los principales estándares nacionales e internacionales.
- Fomentar la creación de un Centro de Ciberseguridad de Andalucía que centralice y coordine todas las capacidades en materia de ciberseguridad de la Administración de la Junta de Andalucía.
- Establecer los mecanismos de coordinación dentro de la Administración de la Junta de Andalucía para la compartición de información, asesoramiento especializado, así como formación y concienciación transversal.
- Promover e implantar instrumentos para la cooperación activa en materia de protección de datos y seguridad física dentro de la Administración de la Junta de Andalucía.
- Crear e implantar procesos unificados y homogéneos de gobierno, riesgo y cumplimiento normativo para la Administración Autonómica.
- Establecer las capacidades de ciberseguridad en la Administración, un catálogo de servicios completo, industrializable y escalable, además de las herramientas necesarias para la prestación, tanto interna como externa.
- Definir, actualizar y evolucionar las políticas, normas y guías de buenas prácticas que permitan aplicar la ciberseguridad desde el diseño en los sistemas y servicios prestados por la Administración de la Junta de Andalucía.

- Promover la implantación de medidas de seguridad dentro de Administración Autonómica y de las empresas que le presten servicio, en cumplimiento del Esquema Nacional de Seguridad y otra regulación vigente, prestando especial atención a los operadores críticos y de servicios esenciales.
- Fomentar el refuerzo de los recursos humanos y técnicos especializados en ciberseguridad para las distintas tecnologías habilitadoras digitales.

7.2. LA2 – Definición e implantación de un plan de desarrollo y mejora continua de las capacidades de prevención, detección y respuesta a incidentes de AndalucíaCERT

Actuaciones

- Avanzar en las capacidades del Centro de Operaciones de Seguridad AndalucíaCERT, ampliando sus servicios y su ámbito de actuación, sobre todo, en el ámbito de la vigilancia digital y la resiliencia ante ciberataques.
- Establecer criterios unificados y potenciar el uso de herramientas comunes y compartidas, especializadas en la prevención, detección, respuesta y recuperación que permitan la integración con plataformas nacionales y con orientación a la automatización y a la mejora continua.
- Avanzar en la investigación de los incidentes y ataques, colaborando con centros especializados en la lucha contra las ciberamenazas e informando a los órganos competentes sobre las causas y consecuencias de los mismos.
- Garantizar el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas, fomentando la prevención y alerta temprana.
- Consolidar la colaboración con las FFCCSE (Policía Nacional, Guardia Civil, Unidad de Policía Nacional Adscrita a la Comunidad Autónoma) para la canalización de denuncias, apoyo en investigaciones y compartición de información.
- Actualizar y evolucionar el modelo de gestión de crisis de ciberseguridad, en todos sus niveles, y de forma integrada con el Plan Territorial de Emergencias de Andalucía, asegurando la coordinación técnica y operacional mediante el entrenamiento continuo y la realización de simulacros periódicos.
- Impulsar el diseño de un Plan de Contingencia y Continuidad de Negocio, donde se establezcan los mecanismos y medidas que permitan asegurar las operaciones de la Administración Autonómica en caso de un evento disruptivo en materia de ciberseguridad.

7.3. LA3 – Fortalecimiento y desarrollo de marcos de cooperación y colaboración en diferentes ámbitos, tanto a nivel autonómico, nacional e internacional

Actuaciones

- Desarrollar la extensión y capilaridad de la Red Nacional de SOCs mediante una Red Andaluza de SOC, para ampliar la coordinación y la cooperación entre el sector público y privado, así como con los organismos competentes en materia de ciberseguridad, utilizando cuando sea posible modelos federados de herramientas comunes y compartidas.
- Reforzar los modelos de relación, coordinación y colaboración en materia de ciberseguridad entre las distintas Administraciones Públicas (Ayuntamientos, Diputaciones Provinciales y otros entes públicos) y fomentar su integración en los modelos de relación nacionales.
- Fomentar el establecimiento de un mapa de actores clave en el ámbito de la ciberseguridad, tanto a nivel nacional como internacional: autoridades competentes, CERT/CSIRT, empresas TIC y de ciberseguridad, operadores críticos y de servicios esenciales, entre otros.
- Establecer acuerdos y definir hojas de ruta de cooperación con empresas nacionales e internacionales, mediante instrumentos de colaboración público-privada.
- Promover la utilización de herramientas específicas de notificación y compartición de datos en materia de ciberseguridad entre el sector público y privado andaluz.
- Impulsar el desarrollo de un foro público-privado de responsables de seguridad de la información entre las principales empresas y organismos andaluces, que permita compartir las principales tendencias y retos con la finalidad de promover la mejora en el ámbito de la ciberseguridad.
- Fomentar la colaboración y cooperación con organismos nacionales e internacionales especializados en materia de ciberseguridad.
- Avanzar en la relación de colaboración con el Centro Criptológico Nacional.

7.4. LA4 – Desarrollo de programas para el impulso y financiación de la ciberseguridad en el sector empresarial andaluz, favoreciendo la mejora de su nivel de madurez

Actuaciones

- Impulsar la ciberseguridad en las empresas andaluzas mediante la elaboración y difusión de políticas públicas en ciberseguridad, con especial atención a las actuaciones dirigidas al fomento de la protección y la resiliencia.
- Impulsar el establecimiento de mecanismos de asesoramiento que ayuden a las empresas andaluzas a encontrar financiación en el ámbito de la ciberseguridad, desarrollando y manteniendo un catálogo de ayudas disponibles que recoja los criterios e información asociada de forma clara, sintética y directa.
- Promover la realización de autodiagnósticos en materia de ciberseguridad en el sector empresarial andaluz, de modo que puedan conocer su nivel de madurez y ámbitos de actuación que necesitan desarrollar a futuro.

- Fomentar la inclusión de los aspectos relativos a la ciberseguridad en los procesos de la digitalización e implantación de nuevas tecnologías en empresas andaluzas, así como programas de I+D+i en materia de ciberseguridad y seguridad digital.
- Incentivar planes de ayuda para las empresas andaluzas que permitan la certificación de sus procesos de negocio y servicios bajo estándares de ciberseguridad nacionales e internacionales.
- Promover la elaboración de un libro blanco de ciberseguridad en la cadena de suministro, mediante el cual las empresas andaluzas puedan valorar su nivel de madurez en ciberseguridad como proveedor de productos y/o servicios, así como tener un marco de referencia frente al cual evaluar a sus proveedores.

7.5. LA5 – Establecimiento de planes de desarrollo de una industria especializada en el sector de la ciberseguridad a lo largo del territorio andaluz

Actuaciones

- Promover la elaboración de un mapa de la industria de la ciberseguridad en Andalucía, identificando los distintos actores involucrados, así como los servicios y soluciones que proporcionan.
- Fomentar un diagnóstico del estado del sector de la ciberseguridad en Andalucía, que identifique las capacidades y necesidades existentes.
- Hacer uso de las ventajas de los Digital Innovation Hubs (DIH) previstos y ampliar las capacidades de los DIH existentes para incorporar aspectos de ciberseguridad.
- Fomentar la implantación de centros de investigación e innovación de empresas relevantes en el sector de la ciberseguridad, estableciendo acuerdos estratégicos con las empresas más relevantes en el mercado.
- Promover la cooperación y transferencia de conocimiento desde las universidades y centros de innovación andaluces a la industria de ciberseguridad de la Comunidad Autónoma.
- Impulsar planes de captación de capital privado destinado a la inversión en empresas de ciberseguridad andaluzas, tanto dentro de la Comunidad Autónoma como en el extranjero.
- Promover la creación de mecanismos de financiación pública específicos para el sector privado de la ciberseguridad en Andalucía.
- Diseñar e impulsar programas de aceleración y escalado específicos para empresas dedicadas a la ciberseguridad.
- Estimular la inversión en I+D+i en los ámbitos tecnológicos prioritarios para el desarrollo de la industria en el sector de la ciberseguridad, poniendo especial foco en la adaptación de la tecnología a las necesidades actuales, como Cloud, Big Data, IA, IoT, 5G, etc.

- Promover e incentivar programas para la atracción de empresas especializadas en materia de ciberseguridad al territorio andaluz.
- Fomentar la certificación de profesionales que se dediquen al ámbito de la ciberseguridad dentro del sector empresarial andaluz.

7.6. LA6 – Creación y desarrollo de un plan de promoción de Andalucía, posicionándola como territorio de referencia en materia de ciberseguridad

Actuaciones

- Promover la presencia de Andalucía en conferencias, foros y otros eventos en materia de ciberseguridad de relevancia nacional e internacional.
- Fomentar la creación de capítulos andaluces de asociaciones profesionales del sector de la ciberseguridad.
- Impulsar el diseño de un conjunto de métricas e indicadores que permita evaluar el estado de la ciberseguridad en Andalucía y establecer planes de acción específicos para mejorar el nivel de seguridad de la Comunidad Autónoma.
- Impulsar la creación de un observatorio de ciberseguridad que mantenga un barómetro para medir el nivel de ciberseguridad de Andalucía.
- Promover el posicionamiento de Andalucía en los principales índices externos de referencia en materia de ciberseguridad.
- Aumentar la dimensión de la ciberseguridad andaluza colaborando en proyectos internacionales, especialmente en programas nacionales y europeos.
- Impulsar la difusión de las capacidades de ciberseguridad de Andalucía, apuntalando su posición como referente tecnológico pionero en materia de ciberseguridad.
- Divulgar, tanto a nivel nacional como internacional, los principales proyectos y logros de las empresas de ciberseguridad andaluzas para posicionar a la Comunidad Autónoma como uno de los territorios especializados en el sector.
- Generar alianzas con actores relevantes del sector de la ciberseguridad.

7.7. LA7 – Elaboración y despliegue de programas formativos con contenidos de ciberseguridad, así como de planes de formación continua y reciclaje para profesionales del sector

Actuaciones

- Promover la educación en ciberseguridad desde edades tempranas en los centros de enseñanza (Educación Primaria, Secundaria y Bachillerato), adaptándola e integrándola dentro del currículum educativo a todos los niveles formativos y especialidades.

- Fomentar el diseño y despliegue de estrategias para fomentar la vocación e interés en disciplinas STEM (científicas, tecnológicas, ingeniería y matemáticas) y, concretamente, en materia de ciberseguridad.
- Fomentar y coordinar los contenidos de ciberseguridad, como ámbito de estudio transversal, en ciclos formativos de grado medio y superior, así como en estudios universitarios.
- Impulsar el desarrollo de planes formativos que permitan contar con una oferta especializada en ciberseguridad en estudios universitarios y de formación profesional, de modo que sea posible cubrir las necesidades del mercado.
- Potenciar las prácticas profesionales y bolsas de empleo en materia de ciberseguridad, tanto en entidades públicas como privadas, incrementando la cualificación y especialización de los futuros trabajadores.
- Promover programas inclusivos y equitativos en materia de ciberseguridad, incrementando la presencia de mujeres que se dedican a las TIC e integrando la perspectiva de género en las políticas digitales.
- Impulsar la elaboración e implementación de planes formativos específicos para el personal formador en materia de ciberseguridad, de modo que se pueda dar respuesta a las necesidades de los nuevos programas educativos.
- Promover el reciclaje de perfiles de alta cualificación y especialización a través de programas de formación específicos, para que puedan desempeñar su actividad en el desarrollo de iniciativas y servicios de ciberseguridad, tanto en el sector público como privado.
- Promover iniciativas de generación y detección de talento y especialización en materia de ciberseguridad, a través de colaboraciones públicas- privadas y con los centros educativos y universidades andaluzas, alineándose con el Plan para la Captación y Retención del Talento Innovador y Digital en Andalucía 2021-2024.
- Impulsar, con los centros directivos competentes, el estudio de las necesidades y, en su caso, la creación y dotación de puestos de trabajo relacionados con las TIC y ciberseguridad; al igual que la capacitación en dicha materia.

7.8. LA8 – Promoción de la concienciación y sensibilización en ciberseguridad, así como fomento de las buenas prácticas en el uso de las TIC en la Administración, ciudadanía y empresas

Actuaciones

- Impulsar campañas periódicas de concienciación y sensibilización en ciberseguridad para la Administración, empresas y ciudadanía, que recojan recomendaciones y buenas prácticas en el uso de las TIC.
- Fomentar acciones de concienciación en ciberseguridad específicas para determinados colectivos de personal empleado público que, por sus funciones y necesidades, tienen un mayor riesgo de

estar involucrados en un ciberincidentes o brecha de seguridad, tales como personal de justicia, sanidad o seguridad ciudadana.

- Promover acciones de sensibilización a personal de dirección de la Administración, con el objetivo de que habiliten los recursos y promuevan los proyectos de ciberseguridad necesarios dentro de la Administración de la Junta de Andalucía.
- Favorecer el despliegue de iniciativas y planes de alfabetización digital y de ciberseguridad en los colectivos donde existe una mayor brecha digital, así como campañas específicas de capacitación a víctimas de ciberataques.
- Potenciar el papel de las TIC y de su uso seguro como instrumento de innovación social y de mejora en el acceso a productos y servicios
- Reforzar la confianza digital de la ciudadanía y empresas, mediante iniciativas y acciones específicas que incidan en la seguridad de las TIC.
- Potenciar la creación de canales de difusión de contenidos y alertas de seguridad, así como buscar la colaboración con medios de comunicación para lograr un mayor alcance en las campañas dirigidas a la ciudadanía.
- Mejorar el gobierno digital de Andalucía empoderando a la ciudadanía con políticas de transparencia y participación.

8. Modelo de gobernanza

El impulso e implantación de la Estrategia Andaluza de Ciberseguridad requiere de un modelo de gobernanza sólido y bien estructurado, que involucre a todos los actores relevantes dentro del ecosistema de ciberseguridad de la Comunidad Autónoma, tanto internos como externos a la Administración de la Junta de Andalucía.

Dicho modelo estará compuesto por un conjunto de comités y mecanismos de relación que actúen a diferentes niveles: estratégico, táctico y operativo.

- Comité Estratégico
- Comité Táctico
- Oficina de seguimiento y coordinación
- Comités Operativos
    - Transformación de la Administración
    - Capacitación y concienciación
    - Ciberseguridad en empresas
    - Fomento de la industria de la ciberseguridad

A continuación, se detallan las personas que deben integrar cada uno de los comités, así como sus funciones más relevantes:

COMITÉ ESTRATÉGICO

MIEMBROS

- Presidencia de la Agencia Digital de Andalucía.
- Dirección Gerencia de la Agencia Digital de Andalucía.
- Responsable del Centro de Ciberseguridad de Andalucía.
- Dirección General de Estrategia Digital.

FUNCIONES

- Análisis del cumplimiento y actualización de los objetivos de la Estrategia.
- Supervisión global del riesgo de ciberseguridad en Andalucía.
- Toma de decisiones estratégicas.
- Análisis global de indicadores relevantes.

ÁMBITOS DE ACTUACIÓN

- Transversal

PERIODICIDAD MÍNIMA

- Anual

COMITÉ TÁCTICO

MIEMBROS

- Responsables del Centro de Ciberseguridad de Andalucía.
- Dirección General de Estrategia Digital.
- Responsables de los Centros Directivos con competencias en la implementación de la Estrategia.

FUNCIONES

- Análisis del riesgo de ciberseguridad en Andalucía.
- Medición del cumplimiento de los objetivos de la Estrategia.
- Análisis y gestión de presupuesto.
- Establecimiento de mecanismos de financiación.
- Seguimiento y coordinación de las líneas de actuación.

- Evaluación del impacto de la Estrategia por grupos de interés.
- Análisis de las actividades e hitos completados.
- Planificación de nuevas actividades.
- Toma de decisiones tácticas.
- Definición y supervisión de indicadores.
- Gestión de riesgos.
- Resolución de problemas, escalando aquellos fuera de su ámbito.

ÁMBITOS DE ACTUACIÓN

- Transversal

PERIODICIDAD MÍNIMA

- Trimestral

COMITÉ OPERATIVO

MIEMBROS

- Responsables de las líneas de actuación del Centro de Ciberseguridad de Andalucía.
- Representantes de los Centros Directivos con competencias dentro de cada ámbito de actuación.

FUNCIONES

- Ejecución de presupuestos.
- Definición de metodologías de trabajo y acciones operativas.
- Seguimiento detallado de actividades y tareas asociadas.
- Análisis de las tareas completadas.
- Planificación de nuevas tareas.
- Toma de decisiones operativas.
- Medición y mantenimiento de indicadores.
- Escalado de riesgos.
- Escalado de problemas.

ÁMBITOS DE ACTUACIÓN

- Transformación de la Administración
- Capacitación y concienciación

- Ciberseguridad en empresas
- Fomento de la industria de la ciberseguridad

PERIODICIDAD MÍNIMA

- Mensual

9. Seguimiento y evaluación

La medición de los resultados de las líneas de actuación de ciberseguridad, así como su impacto en la Administración Pública, empresas y ciudadanía es un aspecto imprescindible para analizar la adecuada implantación de la Estrategia Andaluza de Ciberseguridad y enfocar adecuadamente los recursos que la sustentan.

Por ello la Estrategia debe sustentarse en un conjunto riguroso y completo de métricas que permitan medir el progreso hacia los resultados esperados, así como su impacto.

A continuación se establecen los principales objetivos de medición de las métricas asociadas a la Estrategia Andaluza de Ciberseguridad. Dichas métricas deberán definirse una vez se detallen de manera pormenorizada las líneas de actuación y actividades descritas en el presente documento:

1. Nivel de riesgo en materia de ciberseguridad dentro de la Administración de la Junta de Andalucía.
2. Nivel de cumplimiento de las medidas del Esquema Nacional de Seguridad dentro de la Administración Autonómica.
3. Mejora de las capacidades de prevención, detección y repuesta a incidentes del AndalucíaCERT.
4. Nivel de relación y colaboración entre Administraciones Públicas.
5. Acuerdos de colaboración y cooperación con organismos nacionales e internacionales.
6. Diagnósticos en materia de ciberseguridad en el sector empresarial andaluz.
7. Planes de ayuda para las empresas andaluzas que permitan la certificación de sus procesos de negocio y servicios.
8. Estado y madurez del sector de la ciberseguridad en Andalucía.
9. Planes y mecanismos de captación de financiación para empresas dedicadas a la ciberseguridad.
10. Presencia de Andalucía en conferencias, foros y eventos en materia de ciberseguridad.
11. Posicionamiento de Andalucía en índices externos de referencia en el ámbito de la ciberseguridad.
12. Nivel de penetración de la ciberseguridad en los programas formativos a todos los niveles educativos.
13. Oferta de prácticas profesionales y bolsas de empleo en materia de ciberseguridad en entidades públicas y privadas.

14. Nivel de concienciación y sensibilización en ciberseguridad de la ciudadanía.

Las ambiciones de esta Estrategia van más allá del período temporal de tres años, por lo que los objetivos de medición propuestos pueden continuar siendo medidos posteriormente a 2025 y dar cobertura a futuros planteamientos estratégicos de la ciberseguridad en Andalucía.