sedian

Seguridad Digital
de Andalucía

Plan de Seguridad y Confianza Digital Andalucía 2020

Periodo 2017-2020

JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

1 Introducción

El desarrollo de las TIC ha generado un nuevo marco de relaciones que incrementa enormemente la rapidez y la facilidad de los intercambios de información. Conceptos de distancia y tiempo se redefinen en el entorno del denominado ciberespacio, y las barreras que pudieran presentar se difuminan. La revisión y transformación de las políticas de seguridad es necesaria en este contexto.

Dichas políticas, unidas a los procedimientos y a las medidas de seguridad, deben tener como finalidad afrontar las continuas y cada vez más peligrosas ciberamenazas que afectan a todos los sectores de la sociedad y tras las que se encuentra una intrincada amalgama de actores que van desde hacktivistas y organizaciones criminales hasta gobiernos. Su desarrollo debe realizarse mediante procesos formales y organizados de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información.

La continua aparición de nuevas amenazas requiere disponer de una estrategia completa de seguridad, en permanente revisión, con actuaciones en diferentes ámbitos y orientada a crear un clima de confianza, ya que conceptos como privacidad, seguridad y riesgo están cada vez más extendidos en la sociedad, pero de una manera parcial y difusa, lo que genera sensación de indefensión y cierta alarma a empresas, consumidores y usuarios.

En el marco de la Administración, la permanente búsqueda de la eficiencia y eficacia en la gestión de la información se refleja en normativa tanto en los ámbitos más generales (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público) como en los más específicos de las TIC (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica).

Otras regulaciones de reciente aparición sobre protección de datos (Reglamento 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 la propia normativa autonómica en materia de seguridad TIC (Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía) hacen que el ámbito de la seguridad TIC en la Administración esté en movimiento y continua adaptación y sea necesario un esfuerzo de coordinación y apoyo en la interpretación y cumplimiento.

Por último, no se debe obviar la dimensión de colaboración con otros organismos públicos, a todos los niveles (autonómico, nacional y europeo) en los marcos del Comité Sectorial de Administración Electrónica o de la reciente Directiva 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 (directiva NIS, *Network and Information Security*).

2 Justificación

Las actividades enmarcadas en este Plan se integran en el desarrollo de las competencias otorgadas a la Dirección General de Telecomunicaciones y Sociedad de la Información por el Decreto 210/2015, de 14 de julio, por el que se regula la estructura orgánica de la Consejería de Empleo, Empresa y Comercio. Entre dichas competencias se encuentran la coordinación y ejecución de las políticas de seguridad de los sistemas de Información y telecomunicaciones de la Administración de la Junta de Andalucía, la promoción de la confianza y la seguridad en el uso de las Redes por parte de empresas y la ciudadanía y el desarrollo de programas de capacitación en el ámbito de las Tecnologías de la Información y la Comunicación.

3 Antecedentes

La Junta de Andalucía viene impulsando el uso generalizado de las Tecnologías de la Información y las Comunicaciones como elemento esencial para el desarrollo económico, el bienestar y el progreso de la sociedad andaluza. Consciente de la importancia de la seguridad de la información en el modelo de relación con los ciudadanos, ha definido una trayectoria que se materializa en distintos documentos que han guiado las políticas de seguridad de la información de la Junta de Andalucía en los últimos años:

- Programa Alcazaba (2007-2009)

- Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía (2010-2013)

- Plan de Seguridad y Confianza Digital Andalucía 2020 para el periodo 2014-2016

Todos ellos están alineados con los requisitos legales, económicos y técnicos y con las directrices marcadas por las respectivas Agendas Digitales para España y Europa.

4 Objetivos

Los cuatro objetivos principales de este Plan son los siguientes:

- Potenciar la adopción de buenas prácticas en materia de seguridad digital en la administración autonómica y local de Andalucía.

- Extender la cultura de confianza y seguridad digital, mediante programas de sensibilización, asistencia y formación, con especial atención a los menores.

- Impulsar el mercado de la seguridad digital y la creación de empleo, mediante el estímulo de la oferta y la demanda de productos, servicios y profesionales de la seguridad digital.

- Reforzar las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía (AndalucíaCERT).

5 Análisis del estado de la Seguridad TIC

Como trabajo previo a la elaboración de este Plan se han estudiado (y particularizado para la Comunidad Autónoma Andaluza cuando ha sido posible) los datos de informes, estudios y encuestas entre los que cabe destacar:

- La Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2016 del Instituto Nacional de Estadística (INE)

- El Estudio sobre la Ciberseguridad y Confianza en los hogares españoles (junio 2016) del Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI).

- El informe Indicadores Destacados de la Sociedad de la Información (febrero 2017) del Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI).

- Los estudios sobre estado de la implantación del ENS en la Junta de Andalucía realizados por la Dirección General de Telecomunicaciones y Sociedad de la Información en los tres últimos años

- La Encuesta de uso de TIC y Comercio Electrónico en las empresas 2015-2016, del Instituto Nacional de Estadística (INE).

El análisis de estos datos junto con la experiencia acumulada por el personal de la Dirección General de Telecomunicaciones y Sociedad de la Información a lo largo de los últimos años en la definición y puesta en marcha de políticas de fomento de la seguridad de la información en Andalucía han permitido realizar un análisis DAFO en el que se detallan las debilidades, fortalezas, amenazas y oportunidades que condicionan el contexto de seguridad y confianza digital en el que se desenvuelven tres ejes clave de la sociedad andaluza: Ciudadanía, Administración Pública y Empresas.

5.1 Ámbito 1: Ciudadanía

Ciudadanía: DEBILIDADES	
Escasa conciencia de los riesgos asociados a las ciberamenazas:	En general, y exceptuando a un sectores muy específicos de la población con conocimientos elevados, el conocimiento sobre ciberamenazas es prácticamente inexistente, limitándose a lo que se publica en los medios, o lo que les ocurre a conocidos. Se perciben las *ciberamenazas* como aquello que le pasa a grandes organizaciones o celebridades y se tiene una visión distorsionada y obsoleta del perfil del hacker.
Escasa formación y conocimiento sobre herramientas de seguridad:	Sin pasar por alto que la cuarta parte de los usuarios deciden no usar ninguna herramienta, los que las usan, aplican medidas básicas, siendo una minoría la que usa otras medidas de seguridad.
Desconfianza en el uso de servicios electrónicos:	Somos reticentes a dar nuestros datos personales, a realizar compras u operar con banca electrónica, por ejemplo.
Escasa formación y falta de recursos en la tutorización de menores en Internet:	Se observa cierto desconocimiento en padres y educadores tanto en medidas técnicas de control como en medidas organizativas y de gestión del uso.
Escasa tutela de los menores en el uso de medios electrónicos:	No se presta tanta atención en la vida digital como en la vida social, en una mezcla de confianza y dejadez. Esto lleva a pensar que se tiene una falta de conciencia de la dimensión del mundo digital y de las repercusiones en el menor.

Ciudadanía: FORTALEZAS	
Existencia de legislación sobre protección de datos	Que permite al usuario ejercer sus derechos.
Existencia de programas específicos en la DGTSI que forman en seguridad	Enmarcados en el Servicio de Acceso a la Sociedad de la Información, programas como Andalucía Compromiso Digital y Guadalinfo organizan actividades de formación y sensibilización en materia de seguridad y confianza digital.
Iniciativas de apoyo al menor	Desde hace algún tiempo existen iniciativas de apoyo al menor, tanto de instituciones públicas como desde el ámbito privado (INCIBE, AEPD, Red.es, Fundación ANAR, Pantallas Amigas, etc.)

Ciudadanía: AMENAZAS	
Incremento sostenido de las ciberamenazas a todos los niveles y en todas las plataformas	Afecta a todos los colectivos, y especialmente a los menores, al ser los más confiados y tener menos experiencia.
Cesión sin límites de información a redes sociales y grandes proveedores de servicios de Internet	Demasiada información en poder de terceros que el usuario no puede controlar.
Pasividad del ciudadano	Percepción de que no ocurre nada, o que no tiene nada que proteger, o que su información no es relevante.
Exhibicionismo digital; necesidad de retransmitir y publicarlo todo	Si bien se empiezan a estudiar ya a nivel sociológico, el rastro de información que se arroja en Internet facilita enormemente los ataques tanto digitales como físicos (ausencias del domicilio)

5.1.1

Ciudadanía: OPORTUNIDADES

Iniciativas de divulgación	Proyectos como Guadalinfo o Andalucía Compromiso Digital contribuyen a educar en seguridad, y constituyen perfectos canales para acceder a la ciudadanía.
Incipiente conciencia de los riesgos y las amenazas de seguridad	Salvo edades maduras donde existe más reticencia, empieza a existir conciencia del deber y la necesidad de proteger la información, tanto protegiendo dispositivos personales como en lo que se publica en las redes.
Conciencia de los peligros de Internet para el menor	La preocupación de progenitores y tutores hace que exista un canal de diálogo abierto donde se alerta de los peligros y amenazas.

5.2 Ámbito 2: Administración Pública

Administración Pública: DEBILIDADES	
Falta de conciencia en seguridad de la información en los niveles directivos de los organismos	Este hecho genera varias consecuencias: • Hace que la seguridad de la información sea percibida como un gasto y no como una inversión. • Un reducido número de organismos de la Junta de Andalucía tiene una política de seguridad. En algunos casos la organización de seguridad no está estructurada ni definida. • La seguridad de la información es gestionada únicamente por los responsables TIC (generalmente sí concienciados) siendo ajena para otras áreas, y asociándose comúnmente seguridad de la información con seguridad informática. • Pasividad a la hora de iniciar proyectos de seguridad.
Insuficiencia de servicios comunes de seguridad para las Administraciones	La gestión de la seguridad es competencia de cada organismo y no están normalizados los servicios y

	soluciones de seguridad corporativos, suponiendo esto una dificultad para los escasos servicios comunes.
En el desarrollo de aplicaciones, la seguridad de la información, está en un nivel de madurez insuficiente	Las metodologías de desarrollo se aplican con laxitud y la seguridad, aunque se tiene en cuenta, no es un aspecto prioritario.

5.2.1

Administración Pública: FORTALEZAS	
Existencia de normativa específica tanto nacional como autonómica en materia de seguridad de la información	La mayoría de estas normas tienen la vocación de hacer una administración más segura y surgen con la intención de hacer de guía de las políticas de seguridad internas de cada organización.
Existencia del Consejo para la Transparencia y Protección de Datos en Andalucía	Entre sus funciones está la de velar por el cumplimiento de la normativa de protección de datos en el ámbito de sus competencias.
Existencia del centro de seguridad TIC AndalucíaCERT	El equipo de respuesta a incidentes de la Junta de Andalucía goza de buena reputación en el grupo atendido, abre la vía a promover medidas técnicas comunes, coordinadas y coherentes y proporciona un ahorro de esfuerzos y costes.
Existencia de la RCJA y Red NEREA en el ámbito de la Administración pública	Permiten comunicaciones seguras en el ámbito de la Administración.
Proyectos horizontales liderados desde la DGTSI	Proyectos como Consulta Teleco, AndalucíaSmart, etc pueden favorecer la implantación de políticas en materia de seguridad en las AALL.
Oficina de soporte al Plan de Seguridad y Confianza Digital	La Junta de Andalucía cuenta desde el año 2011 con un equipo formado y solvente con experiencia y capacitación en ciberseguridad.
Personal TIC de los organismos concienciado en seguridad	En general, los sistemas TIC en los organismos de la Junta de Andalucía están razonablemente protegidos. Sin embargo el esfuerzo de dirección en

	seguridad TIC recae únicamente en los responsables de los sistemas, no transcendiendo a otras áreas.

Administración Pública: AMENAZAS	
Ausencia de régimen sancionador en la normativa vigente	Aunque no debería ser así, en muchos casos el temor a una sanción es un factor que promueve la implantación de medidas de seguridad.
Fuerte dinamismo en la regulación europea en la materia	Los cambios podrían impactar significativamente en las estrategias de la Junta de Andalucía, las cuales se han trazado según las directrices vigentes.
Incremento sostenido de las ciberamenazas a todos los niveles y en todas las plataformas	Las ciberamenazas son de diversa naturaleza, así como su procedencia (estados extranjeros, hacktivistas, hackers, saboteadores...) Con métodos cada vez más sofisticados, pero producidos por herramientas de fácil acceso y que no requieren conocimientos expertos.
Separación difusa entre uso personal y profesional de los terminales y dispositivos móviles tanto corporativos como propios (BYOD)	Es difícil aplicar políticas de seguridad a dispositivos personales aun si estos se conectan a entornos corporativos.
Uso generalizado en el trabajo y para el trabajo de servicios basados en la nube no corporativos	Plataformas de intercambio de ficheros, alojamiento en la nube, redes sociales, etc. facilitan la fuga de información.

Administración Pública: OPORTUNIDADES	
Fortalecimiento de la capacidad de detección y respuesta	Crecimiento de las capacidades e incorporación de nuevos de servicios que se adapten a las necesidades del grupo atendido.
Grupo atendido por AndalucíaCERT	Extensión de la capilaridad de AndalucíaCERT.
Coordinación, asesoramiento y prospectiva.	Desarrollo de acciones de asesoramiento, coordinación y prospectiva para la efectiva y eficiente gestión de la seguridad.
Actuaciones horizontales llevadas a cabo por la DGTSI	Las acciones realizadas en el marco del Plan Director de Seguridad 2010-2013 han sentado unas bases en los organismos de la Junta de Andalucía que deben mantenerse y ampliarse.

5.2.2

5.3 Ámbito 3: Empresas

Empresas: DEBILIDADES	
Recursos limitados; poca inversión en seguridad	En general, solamente se invierte en seguridad de la información cuando la información es vital para el negocio y el presupuesto general (y por tanto, en TIC) es elevado.
Escasa concienciación en seguridad TIC	Debido a que generalmente las empresas subcontratan los servicios TI, la preocupación por la seguridad se traslada a los contratistas.

Escasa formación en ciberamenazas y en seguridad TIC	Generalmente no se realiza formación en seguridad, ésta queda reducida a las noticias, la opinión pública y a las iniciativas personales.
Escasa profesionalización en el soporte TIC	En muchas pequeñas empresas, el soporte y mantenimiento de las TIC recae en manos de empleados con habilidades, pero no con dedicación exclusiva y formación apropiada.

Empresas: FORTALEZAS	
La mayoría emplean medidas básicas de seguridad	La mayoría de las empresas, por pequeñas y modestas que sean, utilizan medidas básicas como antivirus, copias de seguridad (con mayor o menor sofisticación).
Existencia de un servicio con orientación a la Empresa andaluza y en particular el sector TIC andaluz dentro de la DGTSI	Dentro de la DGTSI se lleva trabajando desde hace años con las empresas andaluzas y con el sector TIC por lo que existe un conocimiento profundo sobre las necesidades y características del sector.

5.3.1

Empresas: AMENAZAS	
Incremento sostenido de las ciberamenazas a todos los niveles y en todas las plataformas	La proliferación de amenazas cada vez más extendidas y más complejas constituye un riesgo no por ser las PYMES objetivos estratégicos, sino por ser susceptibles de ataques por múltiples medios.
Empleo generalizado del BYOD y poco control de los dispositivos	La carencia de políticas de seguridad, o normas relajadas en el uso y práctica, hacen que los dispositivos tengan un doble uso personal y profesional, donde en el ámbito personal hay mucha más exposición a los peligros de Internet.

Empresas: OPORTUNIDADES	
Concepto de ciber(in)seguridad cada vez más extendido	El hecho de que casi diariamente la prensa generalista se haga eco de noticias sobre incidentes de seguridad, favorece una conciencia de ciberseguridad, que puede aprovecharse para impulsar la seguridad de las TIC de la PYME.
Existencia de mecanismos que promuevan la modernización del tejido empresarial	La Junta de Andalucía pone a disposición de las empresas mecanismos de financiación orientados a la mejora de su competitividad que pueden favorecer la mejora de sus mecanismos de seguridad.
Proyectos horizontales liderados desde la DGTSI	Proyectos como AOF, Minerva, y el Plan de Acción de Empresa Digital, así como la Estrategia de Impulso al Sector TIC, etc pueden favorecer la implantación de políticas en materia de seguridad.

5.3.2

6 Estructura

La consecución de los objetivos del Plan se articulará mediante la puesta en marcha y desarrollo de cinco líneas de trabajo:

1. **Coordinación de la seguridad TIC en la Administración autonómica**, potenciando la adopción de buenas prácticas y ofreciendo servicios de asesoramiento, apoyo y coordinación.

2. **Formación y concienciación** de los trabajadores del sector público, la ciudadanía y las empresas, y extensión de la cultura de confianza y seguridad digital.

3. **Impulso de la industria de la seguridad digital**, mediante el estímulo de la oferta y la demanda de productos, servicios y profesionales de la seguridad digital, y promoción de la adopción de buenas prácticas y de la cultura de seguridad en el tejido empresarial andaluz.

4. **Coordinación con otras Administraciones** y Organismos Públicos en materia de seguridad TIC.

5. **Protección frente a ciberamenazas**, mediante la mejora de las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía (a través del centro AndalucíaCERT).

Identificados los objetivos y las líneas de trabajo que se han definido para abordarlos, se propone en el apartado 7 un conjunto de medidas para las líneas de actuación anteriormente descritas, cuya ejecución se plantea para los próximos años y hasta 2020, que van a permitir aprovechar las oportunidades detectadas e intentar prepararnos ante las amenazas, teniendo en cuenta nuestras debilidades y fortalezas. Asimismo, se refleja en el apartado 9 una serie de indicadores desglosados por línea de trabajo para medir la eficacia de las actuaciones.

7 Líneas de trabajo y medidas asociadas

7.1 Coordinación de la seguridad TIC en la Administración autonómica

El objetivo de esta línea de trabajo es potenciar la adopción de buenas prácticas en materia de seguridad digital en la Administración de la Junta de Andalucía. En este sentido, el conjunto de acciones que se propone viene a formular servicios de carácter horizontal de utilidad para la Junta de Andalucía que le permita definir e implantar su estrategia de seguridad corporativa. Se proponen asimismo actuaciones orientadas a reforzar el papel de coordinación de la ciberseguridad en la comunidad autónoma, que pasan por disponer de información actualizada acerca del estado de la seguridad en la Administración y por llevar a cabo auditorías de revisión del cumplimiento de la normativa de aplicación. Las medidas propuestas para esta línea de acción son las siguientes:

MEDIDA	DESCRIPCIÓN
Definición e implantación de estrategias corporativas de seguridad TIC	Puesta en marcha de un conjunto de servicios de apoyo a la definición e implantación de estrategias de seguridad en la administración: • Asesoramiento en las áreas de cumplimiento normativo, análisis y gestión de riesgos, planificación, licitaciones y auditorías. • Definición de planes de acción horizontales y soporte a la definición de planes de acción en las entidades de la Junta de Andalucía. • Coordinación para el desarrollo de criterios técnicos y operativos comunes. • Coordinación y definición de cláusulas y requisitos técnicos de seguridad en la elaboración de pliegos de prescripciones técnicas para la compra de productos y servicios TIC, con especial atención a los proyectos de desarrollo software. • Definición de cláusulas y pliegos tipo para la compra de productos y servicios de seguridad digital. • Realización de auditorías técnicas y de cumplimiento.
Análisis del estado de la seguridad de la Administración de la Junta de Andalucía	Diseño de un conjunto de actuaciones que permitan identificar el estado de la seguridad en los organismos de la Junta de Andalucía: • Recogida de información sobre iniciativas e indicadores en los organismos. • Diseño, creación y mantenimiento de un inventario de sistemas de información de categoría media y alta de la Junta de Andalucía.

MEDIDA	DESCRIPCIÓN
	• Diseño de un cuadro de mando que permita disponer de un conjunto básico de indicadores en materia de ciberseguridad y confianza digital. • Elaboración de informes periódicos sobre el estado de la seguridad en la Administración de la Junta de Andalucía. • Reporte centralizado del estado de la seguridad, en cumplimiento del artículo 35 del Real Decreto 3/2010, de 8 de enero.
Actualización del marco regulador.	Continuación de las tareas de desarrollo y tramitación de proyectos normativos, resoluciones, procedimientos de seguridad y guías técnicas, a fin de tener un cuerpo normativo completo y actualizado en materia de ciberseguridad, protección de datos de carácter personal y protección de infraestructuras críticas.
Creación de grupos de trabajo específicos	Establecimiento de un conjunto de temáticas de carácter estratégico a abordar de forma consensuada con el Grupo de Personas Expertas en Seguridad de la Junta de Andalucía, que permita explotar todo el potencial de este grupo y mantenerlo vinculado con la definición y apoyo a las políticas de seguridad de la Junta de Andalucía. Coordinación de reuniones periódicas de las áreas de seguridad de los organismos de la Junta de Andalucía para la misma finalidad.
Análisis de licitaciones de productos y servicios de seguridad TIC	Búsqueda de homogeneización en productos y servicios en seguridad partiendo de un estudio de la licitación en materia de seguridad TIC en la Junta de Andalucía. Detección de tendencias y nuevos productos y servicios ge-

MEDIDA	DESCRIPCIÓN
	néricos. Elaboración y difusión de informes y recomendaciones. Planificación, coordinación, ejecución y evaluación de pilotos de productos y servicios. Difusión de los resultados.

7.2 Formación, concienciación y difusión

Esta línea tiene por objeto la formación y concienciación en materia de seguridad de la información, tanto a los empleados públicos de la Junta de Andalucía como a las empresas y ciudadanía andaluzas. Esta línea está estrechamente relacionada con las restantes, pero debido a la importancia de las personas como activo en la cadena de valor de la información, el refuerzo y la protección de este activo son una prioridad para el Plan.

Del análisis DAFO se desprende la necesidad de poner en marcha actuaciones que contribuyan a la creación de cultura de confianza y seguridad en la sociedad, la Administración y las empresas andaluzas, prestando especial atención a directivos y altos cargos como responsables de dotar de recursos y presupuesto la función de gestión de la seguridad en las organizaciones; a los empleados públicos y privados, que son pieza clave a la hora de preservar la seguridad de su organización; a la ciudadanía para que conozca los riesgos y las herramientas; y especialmente a los menores y su entorno para que entiendan la necesidad de preservar su identidad en las Redes. Asimismo se identifica la necesidad de recopilar, ordenar, actualizar y generar contenidos y recursos formativos que se pongan a disposición de la sociedad andaluza para que cada uno en su contexto pueda definir su particular estrategia de seguridad.

MEDIDA	DESCRIPCIÓN
Plan de formación	Elaboración y ejecución/seguimiento de un plan de formación anual orientado a los perfiles de ciudadanía, empresas y personal de la Administración (personal general, perfiles TIC y personal de gestión de seguridad TIC). El plan buscará la capacitación definiendo actuaciones y materias específicas, adaptadas a distintos perfiles, e integrándose con los organismos existentes en cada ámbito, principalmente con el IAAP.

MEDIDA	DESCRIPCIÓN
Fortalecimiento de los canales de comunicación con la sociedad andaluza en materia de seguridad TIC	Definición de la presencia en web y redes sociales del Plan de Seguridad y Confianza Digital, asociada y en concordancia con la presencia en dichos medios de la Dirección General, de la Consejería y de la propia Administración de la Junta de Andalucía. Generación de un plan de publicación de contenido útil, sistemático y eficaz. Constitución en la presencia web de un repositorio útil y estructurado de toda la información relevante en materia de seguridad y confianza digital.
Difusión de recursos sobre riesgos digitales, privacidad y tecoadicciones	Recopilación y difusión de los recursos existentes en materia de privacidad en Internet, derecho al olvido, derechos de los ciudadanos en Internet, tecnoadicciones y riesgos digitales en general .
Campañas de sensibilización	Realización de actuaciones de concienciación y sensibilización para la Administración de la Junta de Andalucía y las Entidades Locales. Diseño de campañas de sensibilización específicas para distintos colectivos y sobre diversas temáticas, promoviendo en la medida de lo posible colaboraciones públicas o privadas que permitan reaprovechar recursos existentes. En particular: • Sensibilización a la comunidad educativa sobre uso adecuado y responsable de las TIC y fomento de la privacidad en las redes sociales.. • Sensibilización a PYMES en materia de seguridad digital, privacidad y cumplimiento normativo.

MEDIDA	DESCRIPCIÓN
Difusión del marco normativo	Desarrollo de actuaciones informativas sobre marco normativo y organizativo de la seguridad en la Administración de la Junta de Andalucía.
Materiales y recursos formativos multiformato	Recopilación, actualización y elaboración de contenidos y recursos formativos de interés para los distintos colectivos. Difusión a través de distintos canales. Búsqueda de formatos adaptados a los distintos públicos: píldoras formativas, cursos de autoformación, videoguías, etc.
Guías de buenas prácticas	Elaboración de guías de buenas prácticas en materia de seguridad digital para PYMES y Administraciones Locales que doten de recursos tipo a estas organizaciones para definir, ejecutar y actualizar sus estrategias de seguridad particulares conforme a la normativa vigente.

7.3 Impulso de la industria de la seguridad

En el Análisis DAFO se identifica como debilidad que la falta de cultura digital y de seguridad en empresas conlleva que la inversión que llevan a cabo en la compra de servicios y la dotación de recursos dedicados a la seguridad sea insuficiente, lo que no beneficia el fortalecimiento del sector de la ciberseguridad.

MEDIDA	DESCRIPCIÓN
Instrumentos públicos de apoyo	Promover la incorporación de la seguridad y confianza digital como ámbito prioritario en los instrumentos públicos de apoyo de la Junta de Andalucía, tanto en los orientados a la incorporación de tecnología entre el tejido productivo, como los orien-

MEDIDA	DESCRIPCIÓN
	tados a favorecer el propio desarrollo del sector de las TIC en nuestra comunidad. Identificar la seguridad y confianza digital como ámbito prioritario en las políticas y proyectos de la Junta de Andalucía de estímulo del emprendimiento basado en la innovación.
Programas para la generación de talento	Diseño y puesta en marcha de un programa de generación de talento y especialización en ciberseguridad en colaboración público-privada y con las Universidades Andaluzas (becas, tesis doctorales, etc.). Identificación de prioridades de investigación en ciberseguridad, orientadas a sectores estratégicos y servicios esenciales, a través de acuerdos específicos con Universidad y Empresa.
Programas de posicionamiento de empresas del sector de la ciberseguridad	Generación de un mapa de recursos y empresas de seguridad en el que se describan las características esenciales del sector, para identificar actuaciones específicas.
Normalización de perfiles de seguridad	Caracterización y normalización de los perfiles y roles habituales en la gestión, administración y operación de seguridad TI y desarrollo de una guía de referencia para la selección y/o contratación de profesionales por parte de empresas y administraciones.
Apoyo a la certificación de empresas y profesionales	Puesta en marcha de actuaciones orientadas a incentivar la certificación de profesionales en ciberseguridad así como la certificación de empresas andaluzas en estándares relacionados con la seguridad de la información, a través de la difusión y promoción y del establecimiento de acuerdos con enti-

MEDIDA	DESCRIPCIÓN
	dades de certificación.
Promoción de la creación de productos y servicios en materia de ciberseguridad proporcionados por empresas andaluzas	Definición de acciones encaminadas a la creación de soluciones de seguridad y al fomento de la industria de la seguridad en los centros de innovación promovidos por la Administración autonómica. Definición y puesta en marcha de programas de innovación abierta para el desarrollo de soluciones de seguridad que atiendan a retos específicos en el ámbito de las empresas, startups, centros de investigación, estudiantes, universidades ....
Establecimiento de acuerdos de colaboración con grupos de interés	Formalización de acuerdos de colaboración con universidades, entidades públicas, y agrupaciones empresariales específicas del sector, para la definición conjunta de programas específicos de fomento de la Industria de la ciberseguridad en Andalucía.

7.4 Colaboración con otras Administraciones y Organismos Públicos

Establecer la coordinación y colaboración con otras Administraciones Públicas favorecerá el conocimiento en materia de seguridad TIC, la adopción de buenas prácticas y la coordinación de actuaciones que serán de gran valor para el resto de las líneas del Plan.

MEDIDA	DESCRIPCIÓN
Relaciones con Administraciones Locales	Promoción de las interacciones con diputaciones y ayuntamientos. Realización de jornadas y difusión de materiales de

	concienciación.
Relaciones con organismos responsables de la ciberseguridad	Establecimiento y mantenimiento de las relaciones con el CCN-CERT, con el Instituto Nacional de Ciberseguridad (INCIBE). Seguimiento y colaboración en la implementación de lo dispuesto en la Directiva 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.
Relación con la Administración General del Estado y otras Comunidades Autónomas	Mantenimiento de las relaciones con los organismos con competencias en seguridad TIC en el resto de Comunidades Autónomas. Continuación de la participación en el Grupo de Trabajo de Seguridad del Comité Sectorial de Administración Electrónica.

7.5 Protección frente a ciberamenazas

El objetivo de esta línea de trabajo es fortalecer las capacidades de prevención, detección, respuesta y recuperación ante las ciberamenazas del centro AndalucíaCERT, en el DAFO se concluye, que pese a la existencia de la RCJA y de ser AndalucíaCERT un centro reconocido y bien valorado, la gestión de los incidentes de seguridad en la Junta de Andalucía se dificulta debido a que las Competencias TIC están dispersas y las responsabilidades distribuidas. A todo esto se suma la insuficiencia de servicios comunes de seguridad para las Administraciones, circunstancia que se agrava por la falta de normalización tecnológica.

MEDIDA	DESCRIPCIÓN
Mejora de la detección	Ampliación de la capacidad de detección automática de incidentes y amenazas a la seguridad del centro AndalucíaCERT a través del despliegue de nuevas infraestructuras integradas en la Red de Corporativa de Telecomunicaciones de la Junta de Andalucía. Adopción e integración de las herramientas proporcionadas por el CCN-CERT que persigan este objetivo, y participación en pilotos de futuras herramientas.
Ampliación del grupo atendido	Inclusión en el grupo atendido de todos los organismos de la Administración autonómica y extensión a Administraciones Locales.
Consolidación y ampliación del catálogo de servicios prestados por AndalucíaCERT	Definición del catálogo de servicios de AndalucíaCERT, revisando el actual y añadiendo nuevos servicios en base a solicitudes del grupo atendido y estudios de buenas prácticas.
Mejora de los procesos internos de AndalucíaCERT	Consolidación y maduración de los procesos internos de AndalucíaCERT y preparación para ser miembro acreditado del TF-CSIRT (*Task Force on Computer Security Incident Response Teams*) de Terena/GEANT.
Acciones de fomento de la colaboración con otros CERT	Fomento de la colaboración con equipos de respuesta y agentes públicos y privados de ámbito nacional, para el intercambio de buenas prácticas; entre otros adherir AndalucíaCERT en la red nacional de alerta temprana de amenazas de seguridad.
Mejora de la	Optimización de los canales de comunicación de Andalu-

MEDIDA	DESCRIPCIÓN
comunicación con el grupo atendido	cíaCERT con el grupo atendido y provisión de información personalizada y de valor añadido a través de dichos canales.

8 Seguimiento y evaluación

El seguimiento y evaluación del Plan permitirá comprobar el desarrollo de las actuaciones previstas e intervenir en su revisión siempre que sea necesario para conseguir los objetivos establecidos. Las tareas de seguimiento incluirán:

- Recopilación, tratamiento y análisis de la información relativa al sistema de indicadores.
- Realización de una memoria anual de seguimiento del plan, así como de la memoria de evaluación final del mismo.
- Elaboración de las propuestas de modificación de las actuaciones a desarrollar en el marco temporal del plan que se consideren necesarias.
- Coordinación con otros organismos públicos, así como con las empresas y asociaciones sectoriales participantes en la ejecución del plan para el diseño y desarrollo de las actuaciones previstas.
- Modificación y reorientación, en caso necesario, de los planteamientos y medidas a partir de las propuestas desarrolladas.

9 Indicadores

Los indicadores constituyen la principal fuente de información en los procesos de seguimiento y evaluación. A través de los mismos se constata qué se ha realizado, cómo se ha realizado y cuáles son los resultados e impactos que se están generando.

Los indicadores del Plan se encuentran asociados a las líneas de trabajo. La medición de los indicadores y su seguimiento se hará anualmente, y se combinarán mediciones en el periodo para los indicadores que así lo permitan, y mediciones acumulativas para todos los indicadores:

MEDIDA	DESCRIPCIÓN
Coordinación de la seguridad TIC en la Administración autonómica	Número de consultas realizadas a los servicios de asesoramiento.
	Número de organismos diferentes que han realizado consultas.
	Nivel de satisfacción con los servicios de asesoramiento.
	Número de actuaciones de coordinación y soporte realizadas
	Número de organismos diferentes sobre los que se han realizado actuaciones de coordinación y soporte.
	Porcentaje de los ámbitos que han sido desarrollados mediante resoluciones y/o documentos técnicos, sobre el total de los indicados por la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo

MEDIDA	DESCRIPCIÓN
	de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
Formación, concienciación y difusión	Número de acciones de formación o concienciación realizadas (directamente o a través de servicios u organismos propios del ámbito).
	Número de personas beneficiarias de alguna actividad de formación o concienciación (contabilizando sólo aquellas actividades que requieran inscripción).
	Número de recursos elaborados.
	Nivel de satisfacción con las actividades realizadas.
Impulso de la industria de la seguridad	Número de empresas/profesionales beneficiarios de alguna de las actuaciones enmarcadas en la línea de trabajo.
	Número de programas realizados en el ámbito universitario.
	Número de acuerdos de colaboración establecidos.
Colaboración con otras Administraciones y Organismos Públicos	Número de actuaciones realizadas orientadas a las Administraciones Locales.
	Número de actividades de coordinación con organismos responsables de la ciberseguridad, Administración General del Estado y otras Comunidades Autónomas.