Título del Proyecto:

SEDIAN. Seguridad Digital de Andalucía, una iniciativa integral de ciberseguridad de la Junta de Andalucía

Implantado en:

JUNTA DE ANDALUCIA

ANTECEDENTES/PROBLEMÁTICA

Las Tecnologías de la Información y las Comunicaciones están cambiando nuestra forma de entender el mundo: cómo nos comunicamos, cómo participamos, cómo nos relacionamos, cómo realizamos transacciones, los modelos de negocio, la forma de trabajar, la manera de acceder a la información, etc. Esto hace que vivamos intercambiando datos digitales con organizaciones, administraciones públicas, empresas y otras personas de forma permanente. A ello se añade el surgimiento permanente de nuevos escenarios y desafíos: Internet de las Cosas (*Internet of Things*, IoT), *cloud computing, big data*, las aplicaciones móviles, etc. Todos estos cambios plantean un reto importante que justifica las iniciativas encaminadas a la transformación digital de la administración, empresas y organizaciones de todo tipo.

Concretamente, en el ámbito de la seguridad de la información, según INCIBE, Andalucía es la tercera comunidad autónoma con más incidentes de ciberseguridad al año, por detrás de Madrid y Cataluña. La media diaria en Andalucía en el año 2017, según el instituto, es de 7.032 incidentes de ciberseguridad al día, siendo Sevilla la provincia con más incidentes diarios con 1.772. Le sigue Málaga con 1.444 incidentes al día, provincia a la que siguen Cádiz, Jaén, Almería, Jerez, Marbella y Huelva[1].

En este contexto social, económico, político y cultural la protección de la información y la privacidad de los datos en la red son temas que despiertan un alto interés y suponen una gran responsabilidad para las administraciones públicas como la Junta de Andalucía. Los ciberdelincuentes encuentran sistemas cada vez más sofisticados para acceder a dicha información y operan de forma cada vez más ingeniosa para robar datos a los usuarios para su propio beneficio personal o el de su organización. Por ello, es importante abordar la seguridad digital desde un punto de vista global y desde todos los ámbitos.

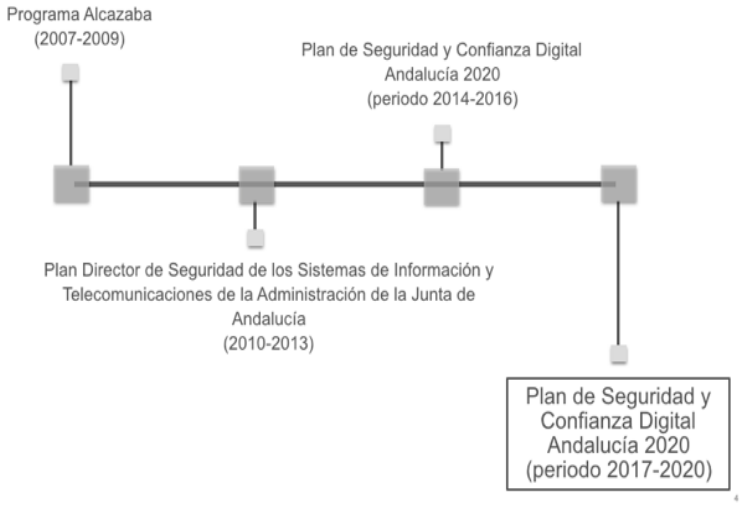
[1] Fuente: Europapress http://www.europapress.es/andalucia/noticia-andalucia-tercera-comunidad-mas-incidentes-ciberseguridad-ano-7000-dia-detras-madrid-cataluna-20171011165833.html

sedian Seguridad Digital de Andalucía

En este marco nace Seguridad Digital de Andalucía, SEDIAN, que da respuesta a un problema real abordándolo de una forma integral. Contempla el ciclo completo de la seguridad y a todos los grupos de interesados: la administración pública de la Junta de Andalucía, las administraciones locales, las empresas y la ciudadanía.

El origen de SEDIAN se enmcarca dentro del proceso de transformación digital de la Junta de Andalucía que tiene como uno de sus objetivos estratégicos el fomento del uso generalizado de las Tecnologías de la Información y las Comunicaciones. De hecho, consciente de la importancia de la seguridad de la información en el modelo de relación con los ciudadanos, la Junta de Andalucía viene desarrollando desde hace varios años distintas políticas de seguridad que se concretan en los siguientes documentos:

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



- Plan de Seguridad y Confianza Digital Andalucía 2020 para el periodo 2017-2020[2].

[2] http://juntadeandalucia.es/export/drupaljda/Plan_Seguridad_Confianza_Digital_2017-2020.pdf

SEDIAN nace del Plan de Seguridad y Confianza Digital Andalucía 2020 y de años de trabajo analizando las necesidades, tendencias y aspiraciones en materia de seguridad TIC de la sociedad en general y de la administración pública en particular. Se alinea con las estrategias imperantes a nivel nacional y europeo y trasciende la pura protección de datos y comunicaciones, aspirando a la creación de un clima de seguridad y confianza digital en Andalucía.

Para ello, apuesta por el diseño de una estrategia que contempla acciones específicas para distintos públicos objetivos en el marco de la administración pública y que da cabida a la ciudadanía y a las empresas como colectivos a integrar en el marco global de la iniciativa. Este enfoque, que conlleva acciones específicas para cada uno de los colectivos, es el que diferencia el proyecto de la Junta de Andalucía por abordarse de forma integral y complementaria analizando necesidades y buscando sinergias.

Administración Pública	Ciudadanía	Empresas
•Junta de Andalucía •Administración local	•General •Colectivos con necesidades especiales	•Pymes de Andalucía •Subsector de la ciberseguridad

OBJETIVOS PERSEGUIDOS

Seguridad Digital de Andalucía, SEDIAN, nace como parte del proceso de transformación digital de la Junta de Andalucía con el objetivo de abordar de manera integral la seguridad TIC, actuando para prevenir, proteger y responder ante incidentes de seguridad y con actuaciones complementarias que contemplan el asesoramiento, auditorías, formación y una serie de actuaciones que completan el ciclo. Se trata de una iniciativa en constante evolución que se adapta a las necesidades de la administración.

Sin duda, la transformación digital supone una gran oportunidad para la administración pública, pero es esencial realizar el proceso con fiabilidad y garantía. Por ello, un proyecto como SEDIAN da soporte transversal a la administración además de ofrecer acciones de sensibilización a empresas y ciudadanía, con el objetivo de aumentar su confianza en su relación digital con la administración, entre otros aspectos.

Entre los objetivos de SEDIAN se contemplan los siguientes:

- Generar confianza en el uso de las TIC para impulsar el proceso de transformación digital en todos los ámbitos de la sociedad andaluza con garantías y conocimientos sobre la seguridad digital. Para ello se recurre, entre otras cosas, a programas de sensibilización, asistencia y formación, con especial atención a los menores.

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

- Reforzar las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía, a través del centro de seguridad TIC AndalucíaCERT.

- 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

FASES DEL PROYECTO – RECURSOS EMPLEADOS

Para poder acometer la estrategia global que se plantea, SEDIAN debe abordar todas sus actuaciones de manera integral y, para ello, diseña un plan de actuación con cuatro grandes ámbitos de actuación vinculados a los objetivos anteriormente citados:

1. Coordinación de la Seguridad TIC en la Junta de Andalucía, asesoramiento y relaciones externas: administraciones locales, CCN, INCIBE...

2. Formación y sensibilización en materia de seguridad y confianza digital para impulsar la transformación digital

3. Gestión de incidentes de seguridad: prevención, detección y respuesta.

4. Impulso de la industria de la Ciberseguridad en Andalucía

Veamos por separado cada una de estas fases:

1. COORDINACIÓN Y RELACIONES EXTERNAS

El servicio de coordinación, asesoramiento y relaciones externas se presta desde dos puntos:

La Consejería de Empleo, Empresa y Comercio desde su Dirección General de Telecomunicaciones y Sociedad de la Información asume la responsabilidad de la coordinación de las políticas de seguridad de la Junta de Andalucía. En el Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, se establece la política de seguridad de las TIC en la Junta de Andalucía y se definen las funciones de la Unidad de Seguridad TIC Corporativa que desarrolla las labores de coordinación en la administración autonómica. Entre las funciones determinadas en el decreto destacan las siguientes:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la Junta de Andalucía y su Grupo de Respuesta a Incidentes TIC, así como de ejecución de las decisiones y acuerdos adoptados.

b) Diseño y ejecución de los programas de actuación de carácter horizontal, así como la dirección de los proyectos y servicios corporativos de seguridad TIC.

c) Desarrollo, mantenimiento y supervisión del marco regulador de seguridad TIC.

d) Generación y supervisión de criterios y directrices corporativas de gestión de la seguridad TIC.

e) Recogida sistemática de información y supervisión del estado de las principales variables de seguridad TIC de la Administración de la Junta de Andalucía, mediante el reflejo, cuando proceda, de los datos referidos a personas desagregados por sexo.

f) Coordinación y seguimiento de la actividad de las Unidades de Seguridad TIC de las Consejerías.

g) Realización de los procedimientos de compra centralizada de productos y servicios corporativos de seguridad TIC a propuesta del Comité de Seguridad TIC en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia y de economías de escala.

h) Realización de auditorías técnicas y de cumplimiento normativo, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia, eficiencia y de economías de escala.

i) Representación de la Administración de la Junta de Andalucía ante los foros y agentes de relevancia del sector.

j) Coordinación del Grupo de Personas Expertas en Seguridad TIC.

En esta labor de coordinación, SEDIAN amplía el foco y activa canales fluidos de comunicación con otras administraciones:

- La administración local por medio de las diputaciones provinciales
- La administración general del estado, fundamentalmente a través del CCN-CERT y del Grupo de Trabajo del Comité Sectorial de Administración Electrónica.
- Otras comunidades autónomas.

Además de las labores de coordinación, se prestan servicios de apoyo y asesoramiento a las consejerías y entidades vinculadas a la Junta de Andalucía desde la Oficina de Apoyo a la Seguridad TIC en materias como:

- Recogida de información sobre el estado de la seguridad y el cumplimiento legal de las entidades de la Junta de Andalucía.

- Aspectos legales y normativos, fundamentalmente sobre el Esquema Nacional de Seguridad, sobre la protección de datos de carácter personal y el marco normativo de la seguridad digital.

- Auditorías técnicas

- Análisis de riesgos

- Otras necesidades bajo demanda.

2. FORMACIÓN Y SENSIBILIZACIÓN

Uno de los pilares fundamentales en los que se sustenta la transformación digital de la administración, empresas y organizaciones es la confianza de las personas en el uso de la tecnología. Desde SEDIAN se identifica la necesidad de realizar actuaciones de sensibilización y formación como medidas de prevención de incidentes de ciberseguridad.

Los ciberdelitos evolucionan a una velocidad difícil de seguir, pero la prevención ayuda a que las personas, el eslabón más débil de la cadena, se encuentren preparadas y conozcan los riesgos y amenazas.

Para poner en marcha las acciones de formación de SEDIAN se elabora un plan de formación anual con la siguiente metodología:

1. Identificación de públicos objetivos

2. Análisis de necesidades formativas

3. Alineación de los resultados con la estrategia

En cuanto a la identificación de los públicos objetivos, el plan de formación contempla los siguientes:

A. JUNTA DE ANDALUCÍA

- Altos cargos de la administración autonómica.
- Responsables de las unidades de Seguridad TIC y responsables de Seguridad TIC.
- Perfiles TIC de la Junta de Andalucía.
- Expertos de seguridad TIC.
- Personal general de la Junta de Andalucía.

B. ADMINISTRACIÓN LOCAL

- Diputaciones provinciales de Andalucía.

C. CIUDADANÍA

- General: confianza digital, buenas prácticas y ciberconvivencia (ciberbulling, tecnoadicciones y privacidad y seguridad en redes sociales).
- Colectivos con necesidades especiales.

D. EMPRESAS

- Pymes de Andalucía

El plan de formación y sensibilización contempla las siguientes líneas de actuación:

1. Ejecución de las acciones formativas y materiales definidos según las necesidades de cada público objetivo garantizando, en la medida de lo posible, el proceso de enseñanza aprendizaje con un alto índice de calidad.

2. Fortalecimiento de los canales de comunicación con la sociedad andaluza en materia de seguridad TIC.

3. Difusión de recursos sobre riesgos digitales, privacidad y tecnoadicciones.

4. Realización de campañas de sensibilización.

5. Difusión del marco normativo.

6. Recopilación, actualización y elaboración de materiales y recursos formativos.

7. Elaboración de guías de buenas prácticas en materia de seguridad digital.

3. GESTIÓN DE INCIDENTES DE SEGURIDAD

La gestión de incidentes de seguridad en SEDIAN se realiza a través de AndalucíaCERT, el centro experto de respuesta incidentes de SEDIAN en la Junta de Andalucía. Se trata de un centro ubicado en el edificio Zoco, en la localidad sevillana de Tomares, que monitoriza toda la Red Corporativa de la Administración de la Junta de Andalucía.

En AndalucíaCERT trabaja un equipo multidisciplinar de expertos en ciberseguridad prestando servicios a todas las consejerías de la Junta de Andalucía y a sus entidades vinculadas 24 *7 (24 horas al día los 7 días de la semana).

En la reunión del Comité de Seguridad TIC de la Junta de Andalucía celebrada el día 2 de noviembre de 2017 se planteó la necesidad de que AndalucíaCERT dispusiera de puntos de contacto e inventario de activos en todos los organismos, con lo que se podrían

tratar los incidentes de seguridad TIC de forma más eficiente y efectiva. El Comité de Seguridad TIC aprobó la propuesta de elaboración de una resolución de la Dirección General de Telecomunicaciones y Sociedad de la Información que regulase la obligada pertenencia al grupo atendido de AndalucíaCERT de todos los organismos en el ámbito del Decreto 1/2011, de 11 de enero. El día 6 de febrero se ha publicado en BOJA la Resolución de 26 de enero de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre integración en el Centro de Seguridad TIC AndalucíaCERT (BOJA 26, de 6 de febrero).

En cuanto a los principales servicios ofrecidos, podemos diferenciar dos tipos: proactivos y reactivos.

Servicios proactivos

- Informes divulgativos.
- Alertas de seguridad
- Servicios de detección de intrusos.
- Análisis de vulnerabilidades.

Servicios reactivos

- Alerta temprana de amenazas de seguridad.
- Tratamiento de incidentes.
- Apoyo a la respuesta a incidentes.
- Coordinación a la respuesta a incidentes.
- Análisis de instancias de código malicioso.

AndalucíaCERT está integrado en el grupo CSIRT.es de Equipos de Ciberseguridad y Gestión de Incidentes españoles (https://csirt.es) y en el foro Trusted Introducer de GÉANT (https://www.trusted-introducer.org). Además, AndalucíaCERT trabaja de forma coordinada con el Centro Criptológico Nacional (CCN), y usa las principales herramientas desarrolladas por el CCN-CERT

- Gestión de incidentes (Lucía)
- Monitorización (SAT-SARA, SAT-INES)
- Detección de APT (Carmen)
- Inteligencia de ciberamenazas (Reyes)
- Análisis de binarios (Marta)

4. IMPULSO DE LA INDUSTRIA DE LA CIBERSEGURIDAD

SEDIAN tiene entre sus objetivos el 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. Como se ha descrito anteriormente, el impulso de la transformación digital pasa por la promoción de la adopción de buenas prácticas y de la cultura de seguridad en el tejido empresarial andaluz.

En este ámbito, SEDIAN ha definido siete líneas de trabajo específicas:

1. 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 orientados 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.

2. 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.

3. 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.

4. 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.

5. 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 entidades de certificación.

6. 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…

7. 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.

Las tareas en los cuatro ámbitos arriba indicados, además de los medios técnicos necesarios, requieren que SEDIAN disponga de un equipo de trabajo multidisciplinar conformado por:

- Coordinación, estrategia y gestión
- Expertos en gestión de la ciberseguridad
- Expertos en gestión de incidentes de seguridad TIC
- Expertos en aspectos legales y normativos en seguridad digital
- Expertos en auditorías técnicas y riesgos
- Expertos en formación y comunicación

Este equipo se compone de personal de la Dirección General de Telecomunicaciones y Sociedad de la Información de la Consejería de Empleo, Empresa y Comercio y de personal de SANDETEL (Sociedad Andaluza para el Desarrollo de las Telecomunicaciones, empresa pública de la Junta de Andalucía).

MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

La ciberseguridad debe considerarse como una inversión y no como un gasto. Se trata de una inversión que, en el caso de la administración pública, no supone una mejora en los beneficios sino una reducción del coste y una mejora de la eficiencia del gasto.

Aunque la gestión de la seguridad en la Junta de Andalucía depende de cada consejería u organismo, la coordinación de forma integrada por parte de la iniciativa SEDIAN supone:

- Homogeneidad en las relaciones con otros organismos a nivel nacional y europeo.
- Asesoramiento y apoyo por parte de un equipo de expertos en ciberseguridad que da soporte a toda la Junta de Andalucía.
- Prestación de servicios horizontales
- Gestión del conocimiento. Determinados aspectos que pueden ser de aplicación a una entidad pueden ser de aplicación a otras y al realizarse de forma integrada en SEDIAN se logra una mayor eficiencia.
- Sinergias entre consejerías y entidades.

CONCLUSIONES DE LA ENTIDAD

Dentro de la estrategia de impulso de la transformación digital que promueve la Junta de Andalucía, SEDIAN surge como iniciativa para ofrecer un tratamiento integral de la seguridad digital ampliando su horizonte más allá de la administración pública autonómica, contemplando el ciclo completo de la seguridad y todos los grupos de interés implicados:

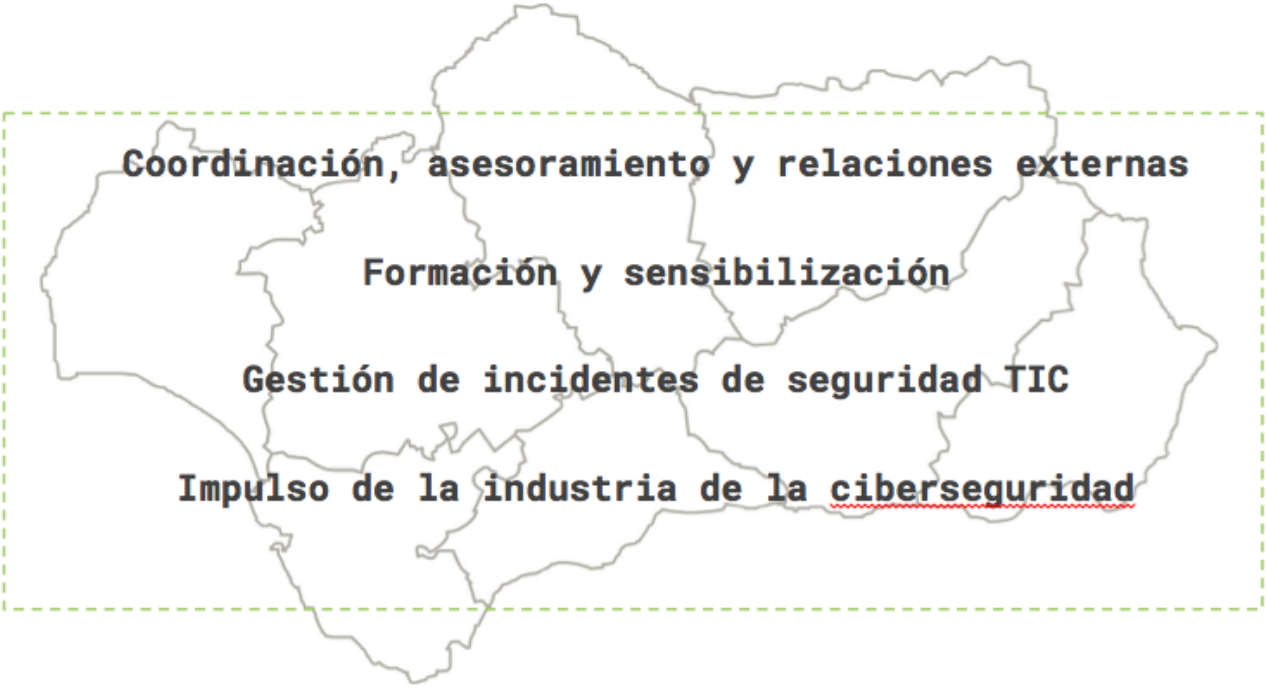
» Administración Pública

- Junta de Andalucía y entidades vinculadas
- Diputaciones provinciales y administración local

» Ciudadanía

» Empresas

A continuación, se describen brevemente los puntos más importantes de cada una de las líneas:



A. **Coordinación, asesoramiento y relaciones externas**. Se presta a través de dos servicios:

- Unidad de Seguridad TIC corporativa, creada por el Decreto 70/2017, de 6 de junio, por el que se modifica el 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.

- Oficina de Apoyo a la Seguridad TIC. Que presta servicios de recogida de información sobre el estado de la seguridad y el cumplimiento legal de las

entidades de la Junta de Andalucía; asesoramiento en aspectos legales y normativos, fundamentalmente sobre el Esquema Nacional de Seguridad, sobre la protección de datos de carácter personal y el marco normativo de la seguridad digital; auditorías técnicas; análisis de riesgos y otras necesidades bajo demanda.

E. **Formación y sensibilización.** Desarrollo de acciones formativas presenciales, en modalidad teleformación, seminarios on line o webinars, MOOC (Masive Open Online Course) y materiales de autoformación, según las necesidades específicas y los objetivos de la formación a impartir.

Las áreas temáticas que se abordan en el plan de formación y sensibilización son las siguientes:

- Sensibilización y conceptos básicos de ciberseguridad.
- Gestión de la seguridad para organizaciones públicas y privadas.
- Aspectos técnicos.
- Cumplimiento normativo y legal.

F. **Gestión de Incidentes de Seguridad TIC**. Desde AndalucíaCERT, el centro experto en gestión de incidentes de seguridad TIC de SEDIAN, se trabaja en la prevención, detección, análisis y respuesta a incidentes de seguridad. Se presta un servicio 24 horas al día los 7 días a la semana (24*7) por expertos en gestión de incidentes de ciberseguridad. En 2017 se gestionaron un total de 6.146 incidentes de seguridad. AndalucíaCERT presta servicios proactivos y reactivos siempre en coordinación con el Centro Criptológico Nacional (CCN CERT) y otros organismos relevantes.

G. **Impulso de la industria de la ciberseguridad** en Andalucía. En 2018 se acomentarán diversas actuaciones para analizar las empresas del Sector TIC

andaluz que prestan servicios en materia de seguridad digital y se realizarán acciones que ayuden al impulso y profesionalización del sector en este ámbito.

En definitiva, SEDIAN promueve que la transformación digital de la Junta de Andalucía, en particular, y de la sociedad andaluza, en general, se realice con garantía velando por la seguridad digital desde los puntos de vista estratégico, organizativo y técnico y desde la formación y la concienciación.