1. Disposiciones generales

CONSEJERÍA DE ECONOMÍA, INNOVACIÓN Y CIENCIA

ACUERDO de 16 de noviembre de 2010, del Consejo de Gobierno, por el que se aprueba el Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía (2010-2013).

La Administración de la Junta de Andalucía se encuentra entre las organizaciones en las que el uso generalizado de las tecnologías de la información y comunicaciones es vital para el desarrollo de sus actividades. La información, junto a los procesos y sistemas que hacen uso de ella, son pieza fundamental en el buen funcionamiento de la organización. Sin embargo, estos activos están expuestos a un número cada vez más elevado de amenazas, tales como fraude, robo de información, acciones malintencionadas, errores humanos, etc. Tanto una interrupción prolongada de sus recursos de comunicaciones, como la alteración de la confidencialidad, integridad o disponibilidad de la información supondrían un grave perjuicio para esta Administración y para la consecución de sus obligaciones de servicio público.

Esta Administración entiende y reconoce la importancia de que los activos sean gestionados atendiendo a los estándares y buenas prácticas de seguridad aceptadas a nivel nacional e internacional, así como de dar cumplimiento a la legislación aplicable a los procesos de gestión de la seguridad, como garantía de la confianza de la ciudadanía en la correcta gestión de sus datos y de la calidad de los servicios públicos prestados desde la Administración autonómica. Todo ello, de acuerdo a lo establecido en la planificación estratégica existente y en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, así como al 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.

El presente Plan Director concibe la seguridad como una cuestión transversal, entrelazándose en su consecución y mantenimiento distintas dimensiones. El nivel de seguridad de los aplicativos y el de los sistemas que los soportan, los entornos donde se ejecutan y las operaciones que se realizan sobre ellos, que conforman la dimensión técnica. Por otra parte, es imprescindible abordar la dimensión normativa mediante la definición de las políticas de seguridad que establezcan las reglas de necesario cumplimiento. Hay que añadir a las dos dimensiones anteriores la dimensión organizativa, es decir, el modelo en el que se integren y relacionen las personas que son las encargadas de llevar a cabo las políticas de seguridad definidas.

Por ello, la Consejería de Economía, Innovación y Ciencia ha elaborado el Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía, el cual fue presentado a la Comisión Interdepartamental para la Sociedad de la Información en su reunión del día 16 de diciembre de 2009, siendo informado favorablemente.

En su virtud, a propuesta del Consejero de Economía, Innovación y Ciencia, el Consejo de Gobierno, en su reunión celebrada el día 16 de noviembre de 2010, de acuerdo con lo dispuesto en el artículo 27.13 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía,

A C U E R D A

Primero. Aprobar el Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones, como instrumento de planificación de las actuaciones horizontales en materia de seguridad TIC en la Administración de la Junta de Andalucía durante el período 2010-2013, y que se adjunta como Anexo al presente Acuerdo.

Segundo. El ámbito de aplicación del presente plan se extiende a la Administración de la Junta de Andalucía, sus entidades instrumentales y los consorcios en los que sea mayoritaria la representación, directa o indirecta, de la Administración de la Junta de Andalucía.

Tercero. Con el fin de garantizar su conocimiento, el Plan estará disponible en la página web de la Consejería de Economía, Innovación y Ciencia de la Junta de Andalucía (www.juntadeandalucia.es/economiainnovacionyciencia).

Sevilla, 16 de noviembre de 2010

JOSÉ ANTONIO GRIÑÁN MARTÍNEZ
Presidente de la Junta de Andalucía

ANTONIO ÁVILA CANO
Consejero de Economía, Innovación y Ciencia

A N E X O

PLAN DIRECTOR DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES DE LA ADMINISTRACIÓN DE LA JUNTA DE ANDALUCÍA

ÍNDICE

1. INTRODUCCIÓN

1.1. Antecedentes.

El día 12 de abril de 2007, en el marco de la reunión de la Permanente de la Comisión Interdepartamental para la Sociedad de la Información, la Consejería de Innovación, Ciencia y Empresa anunció el lanzamiento de un plan integral que permitiese prevenir y afrontar las amenazas de seguridad que pudieran materializarse sobre los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía.

En base a dicho anuncio, esta Consejería inició ese mismo año el lanzamiento de un programa de seguridad denominado Programa Alcazaba. Entre los principales objetivos de este programa se encontraba la elaboración y aprobación de un Plan Director de seguridad para la Administración de la Junta de Andalucía.

En la actualidad, el Programa Alcazaba constituye uno de los proyectos incluidos en el grupo de Calidad y Control del Plan de Acción para el desarrollo de la Estrategia Pública Digital de la Junta de Andalucía. Este Plan constituye el programa de trabajo a ejecutar en los próximos años, según lo establecido en la planificación estratégica existente y en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Así mismo hay que hacer referencia al 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.

Desde el arranque del proyecto se han realizado una serie de actuaciones que podemos considerar como fuentes de información para la elaboración de este documento. Entre ellas, podemos destacar:

- Mantenimiento de entrevistas de toma de datos entre las personas al cargo de los Servicios con responsabilidad en la gestión de tecnologías de la información y el equipo de proyecto. Dichas entrevistas se basaron en cuestionarios de cumplimiento de los estándares UNE-ISO/IEC 27001 e ISO/IEC 27002.

- Análisis de riesgos y auditoría técnica de seguridad de diversos sistemas de información corporativos de la Administración de la Junta de Andalucía.

- Auditoría técnica de vulnerabilidades de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía.

- Consultoría de diseño y análisis de viabilidad de un centro de prevención, detección y respuesta de amenazas de seguridad.

1.2. Ámbito de aplicación.

El ámbito de aplicación del presente plan se extiende a la Administración de la Junta de Andalucía, sus entidades

instrumentales y los consorcios en los que sea mayoritaria la representación, directa o indirecta, de la Administración de la Junta de Andalucía.

1.3. Referencias metodológicas.

Para la realización del presente plan se han tomado como principales referencias metodológicas las siguientes:

- UNE-ISO/IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad (SGSI). Requisitos.
- La serie de normas ISO/IEC 27000 Information technology –Security techniques–.
- BS 25999-1, Código de buenas prácticas para la gestión de la Continuidad del Negocio.
- BS 25999-2, Especificaciones para los Sistemas de Gestión de la Continuidad del Negocio.
- Metodología de análisis y gestión de riesgos de los Sistemas de Información versión 2 (MAGERIT).

2. OBJETIVOS

El objeto del presente documento es definir con claridad la estrategia en materia de seguridad TIC a seguir por la Administración de la Junta de Andalucía durante el período 2010-2013, con el detalle de las diferentes actuaciones a acometer.

El Plan Director debe permitir establecer y planificar las directrices de actuación necesarias en materia de seguridad TIC al objeto de desplegar un modelo integral de gestión del riesgo en la Administración de la Junta de Andalucía, adaptado a los estándares nacionales e internacionales en la materia, al entorno organizativo y tecnológico de esta Administración y a los condicionantes legales y normativos.

El alcance de este Plan Director comprende un conjunto de proyectos cuyo objetivo es, partiendo del conocimiento de la situación actual, avanzar hacia la consolidación de un nivel de madurez caracterizado por la capacidad para evaluar la efectividad de los procesos de seguridad implantados.

La estrategia desarrollada en el Plan Director aborda la gestión de la seguridad desde tres perspectivas complementarias: las personas, los procesos y la tecnología. En el modelo definido tiene especial relevancia la Red Corporativa de Telecomunicaciones de la Junta de Andalucía siendo el nexo de unión TIC entre organismos y entidades y a su vez, la primera línea de defensa con el exterior.

Cada proyecto contenido en este Plan Director se diseña siguiendo una estrategia de mejora continua cíclica. Para poder llevar a cabo esta estrategia es necesario definir indicadores de seguimiento que permitan medir y evaluar el desarrollo de los proyectos.

Para cada uno de los proyectos identificados se detallarán los siguientes aspectos:

- Antecedentes.
- Objetivos.
- Beneficios.
- Planificación y fases.
- Plazo de ejecución.
- Indicadores de seguimiento.

3. PROYECTOS

3.1. PDS-JDA-P01 Desarrollo y aprobación del marco normativo de seguridad de la Administración de la Junta de Andalucía.

3.1.1. Antecedentes.

Aunque se han realizado programas de gestión de la seguridad TIC, tanto horizontales como en los distintos órganos y entidades, la Administración de la Junta de Andalucía carece en la actualidad de un modelo completo de política de seguridad horizontal, como marco común en el que cada organismo pueda desarrollar su propia política, normalizar los procesos de gestión de la seguridad y articular sus normas y procedimientos operativos.

3.1.2. Objetivos.

Se propone en este proyecto la definición y aprobación de un cuerpo normativo horizontal compuesto por:

- Un documento de política de seguridad: ha de mostrar el compromiso expreso de la dirección con la gestión de la seguridad, sus objetivos y principios básicos, el marco de referencia común y la descripción de la estructura organizativa en la que se apoyará el gobierno de la seguridad en la Administración de la Junta de Andalucía.
- Un conjunto de normas de seguridad: como desarrollo y concreción de la política de seguridad, han de recoger las directrices comunes dentro de un ámbito determinado y establecer el marco para la planificación, ejecución y seguimiento de los controles de seguridad a implantar.

La política y las normas de seguridad a desarrollar en este proyecto serán la piedra angular en torno a la que gire la planificación de la gestión del riesgo y deberá proporcionar a los organismos de la Junta de Andalucía la referencia y el soporte para la implantación y seguimiento de las distintas actuaciones en seguridad.

Dentro de los objetivos prioritarios de la política de seguridad, se establecerá con carácter formal la creación, atribuciones y modo de funcionamiento de un comité de seguridad, como órgano colegiado de coordinación y gobierno en materia de seguridad en el ámbito de la Administración de la Junta de Andalucía.

Sin perjuicio de las directrices establecidas en el marco normativo de seguridad, cada organismo desarrollará y aprobará formalmente su documento de política de seguridad, así como las normas y procedimientos que adecúen, en su caso, las directrices comunes a sus particularidades.

3.1.3. Beneficios.

El marco normativo consolidará la seguridad como un elemento estratégico dentro de la gestión TIC de la Administración de la Junta de Andalucía. Permitirá abordar las actuaciones con perspectiva y alinear los esfuerzos acometidos por cada organismo, mejorando su eficiencia y garantizando el cumplimiento de las recomendaciones y de la legislación aplicable.

El marco normativo promoverá la cooperación entre organismos, incrementará la concienciación de todos los miembros de la organización y generará confianza en los diversos actores que interactúan con la Junta de Andalucía, reforzando la imagen pública de esta Administración.

3.1.4. Planificación y fases.

3.1.4.1. Fase 1: Desarrollo y aprobación del documento de política de seguridad de la Administración de la Junta de Andalucía.

En esta fase se definirán las directrices generales sobre las que se debe asentar la gestión de la seguridad, así como su estructura normativa y de gobierno. Como resultado, se producirá un documento de política de seguridad que deberá ser consensuado en el seno de la Comisión Interdepartamental para la Sociedad de la Información y aprobado con el rango normativo que le corresponda.

La política de seguridad será el documento base y referencia para las futuras normas y procedimientos que se desarrollen, tanto a nivel horizontal como sectorial, para una correcta gestión de la seguridad en la Administración de la Junta de Andalucía.

3.1.4.2. Fase 2: Desarrollo y aprobación de las normas de seguridad en la Administración de la Junta de Andalucía.

En esta fase se materializarán en forma de normas concretas la política de seguridad definida y aprobada en la fase 1. Para desarrollar estas normas el equipo de trabajo se basará en la legislación aplicable y en los estándares nacionales e internacionales de seguridad.

Como resultado, se producirán unos documentos de normas de seguridad que deberán ser consensuadas en el seno del comité de seguridad y aprobadas con el rango normativo que le corresponda.

3.1.5. Plazo de ejecución.

- Fase 1: A finalizar en febrero de 2011.
- Fase 2: A finalizar en diciembre de 2011.

3.1.6. Indicadores de seguimiento.

- Nivel de desarrollo del marco normativo.
- Nivel de aprobación formal del marco normativo.

3.2. PDS-JDA-P02 Adecuación de los procesos de las entidades de la Administración de la Junta de Andalucía a la normativa de seguridad.

3.2.1. Antecedentes.

El PDS-JDA-P01 establece la definición y aprobación de un cuerpo normativo horizontal compuesto por un documento de política de seguridad y un conjunto de normas, como desarrollo y concreción de dicha política.

3.2.2. Objetivos.

Mediante el presente proyecto se dará apoyo a las entidades de la Administración de la Junta de Andalucía para la adecuación de sus procesos y procedimientos de seguridad a la legislación vigente, a las directrices establecidas en el marco normativo y a sus propias normas internas, así como al desarrollo de su documento de política, normas y procedimientos de seguridad.

3.2.3. Beneficios.

El desarrollo y aprobación del marco normativo de seguridad de la Administración de la Junta de Andalucía requerirá de un esfuerzo conjunto de adecuación para alcanzar los objetivos marcados en materia de seguridad. Este marco normativo debe impregnar toda la Administración de la Junta de Andalucía.

Para ello, este proyecto facilitará a los organismos el trabajo de adecuación, ofreciéndoles servicios especializados y permitiendo aprovechar la experiencia normalizadora. De esta forma, se incrementará la eficiencia en la adecuación, optimizando los costes e incrementando los beneficios derivados.

3.2.4. Planificación y fases.

Este proyecto se ejecutará basándose en un Plan de Adecuación Legal.

3.2.4.1. Fase 1: Elaboración del Plan de Adecuación Legal.

En esta fase se concretará la planificación y el alcance de los trabajos, produciéndose un documento de Plan de Adecuación Legal.

Durante los dos últimos meses de cada año se revisarán los resultados de ejecución correspondientes al año anterior, se actualizará el plan en base a los aspectos de mejora identificados y se realizará la planificación anual de actuaciones.

3.2.4.2. Fase 2: Ejecución del Plan de Adecuación Legal.

Para cada uno de los organismos incluidos en el ámbito de aplicación del plan, se realizarán las siguientes tareas:

- Análisis de la estructura organizativa, procesos internos y activos de información de la entidad.
- Identificación de la legislación y la normativa aplicable.
- Revisión de la documentación y de los procedimientos técnicos y organizativos en seguridad.
- Elaboración y entrega del Informe de Adecuación, el cual recogerá el conjunto de actuaciones a emprender por el organismo al objeto de alcanzar un nivel de cumplimiento satisfactorio.
- Desarrollo del documento de política, normas y procedimientos de seguridad identificados en el Informe.

3.2.5. Plazo de ejecución.

- Fase 1: A finalizar en diciembre de 2010.
- Fase 2: A finalizar en diciembre de 2013.

3.2.6. Indicadores de seguimiento.

- Nivel de cumplimiento anual del Plan de Adecuación Legal.

3.3. PDS-JDA-P03 Auditoría de cumplimiento legal y del marco normativo de seguridad de la Administración de la Junta de Andalucía.

3.3.1. Antecedentes.

El PDS-JDA-P02 establece actuaciones de apoyo a las entidades de la Administración de la Junta de Andalucía para la adecuación de sus procesos y procedimientos de seguridad a la legislación vigente y a las directrices establecidas en el marco normativo, así como al desarrollo del documento de política, normas y procedimientos de seguridad propios.

3.3.2. Objetivos.

Mediante el presente proyecto se evaluará el grado de cumplimiento legal y del marco normativo de seguridad por parte de las entidades de la Administración de la Junta de Andalucía. El resultado de esta evaluación ayudará a las entidades a continuar el proceso de adecuación de forma eficiente.

3.3.3. Beneficios.

Este proyecto permitirá a la Administración de la Junta de Andalucía adquirir una visión global, comparable y estratégica del estado de cumplimiento legal y normativo de seguridad.

Después de normalizar y apoyar en la adecuación, es necesario medir el éxito de las iniciativas citadas. Los resultados de estas auditorías permitirán a la Administración de la Junta de Andalucía refinar y mejorar las normativas de seguridad desarrolladas y las estrategias de adecuación adoptadas. El trabajo de auditoría es fundamental para asegurar la mejora cíclica de la gestión de la seguridad.

3.3.4. Planificación y fases.

Este proyecto se ejecutará sobre un alcance limitado de organismos y en base a un Plan de Auditorías de Cumplimiento Legal.

3.3.4.1. Fase 1: Elaboración del Plan de Auditorías de Cumplimiento Legal.

En esta fase se concretará la planificación y el alcance de los trabajos, produciéndose un documento de Plan de Auditorías de Cumplimiento Legal.

Durante los dos últimos meses de cada año se revisarán los resultados de ejecución correspondientes al año anterior, se actualizará el plan en base a los aspectos de mejora identificados y se realizará la planificación anual de actuaciones.

3.3.4.2. Fase 2: Ejecución del Plan de Auditorías de Cumplimiento Legal.

Para cada uno de los organismos incluidos en el ámbito de aplicación del plan, se realizarán las siguientes tareas:

- Análisis de la estructura organizativa, procesos internos y activos de información de la entidad.
- Identificación de la legislación aplicable.
- Revisión de la documentación y de los procedimientos técnicos y organizativos en seguridad.
- Auditoría de cumplimiento en la operativa del organismo de las directrices establecidas en el marco normativo y la legislación vigente, así como de los procesos y procedimientos ya establecidos.
- Elaboración y entrega del Informe de Auditoría de Cumplimiento, el cual dictaminará sobre el nivel de cumplimiento del marco normativo, identificará sus deficiencias y propondrá las medidas correctoras o complementarias necesarias.

3.3.5. Plazo de ejecución.

- Fase 1: A finalizar en diciembre de 2011.
- Fase 2: A finalizar en diciembre de 2013.

3.3.6. Indicadores de seguimiento.

- Nivel de cumplimiento anual del Plan de Auditorías de Cumplimiento Legal.

3.4. PDS-JDA-P04 Cultura y concienciación en seguridad.

3.4.1. Antecedentes.

Uno de los pilares básicos de una correcta gestión de la seguridad pasa por crear las condiciones que permitan que las personas al servicio de la organización adquieran una cultura de buenas prácticas en seguridad, así como conciencia

de los riesgos derivados de un uso incorrecto de los recursos tecnológicos.

Durante las entrevistas de toma de datos que se realizaron al inicio del Programa Alcazaba, las personas al cargo de los Servicios con responsabilidad en la gestión de tecnologías de la información pusieron claramente de manifiesto la necesidad de potenciar las actuaciones encaminadas a crear una cultura de seguridad a todos los niveles, es decir, con un alcance que incluyese desde las personas empleadas a la alta dirección.

3.4.2. Objetivos.

Mediante el presente proyecto se pretende:

- Dar a conocer la existencia de un Plan Director y de un marco normativo de seguridad, así como las actuaciones que de él se derivan.

- Mejorar el nivel de seguridad global de la Administración de la Junta de Andalucía, potenciando la participación activa de todas las personas a su servicio.

- Fomentar el compromiso y el impulso que desde la alta dirección se debe dar a las actuaciones y buenas prácticas en seguridad.

3.4.3. Beneficios.

La seguridad es responsabilidad de todas las personas al servicio de la Administración de la Junta de Andalucía. Las iniciativas y proyectos recogidos en este Plan Director no serán realmente eficaces si esta responsabilidad no es compartida, comprendida y asumida. Este proyecto cubrirá dicha necesidad, maximizando la eficacia en la implantación del Plan Director.

3.4.4. Planificación y fases.

Este proyecto se ejecutará en base a un Plan de Cultura y Concienciación.

3.4.4.1. Fase 1: Elaboración del Plan de Cultura y Concienciación.

En esta fase se concretarán las necesidades, destinatarios, planificación y el alcance de las acciones de divulgación. Como resultado, se producirá un documento de Plan de Cultura y Concienciación.

Las acciones de divulgación incluirán tanto eventos presenciales, como contenidos en formato electrónico, adaptados a las necesidades particulares de los distintos perfiles de personas usuarias identificadas (personal TIC, personal no TIC, alta dirección...).

Durante los dos primeros meses de cada año se revisarán los resultados de ejecución correspondientes al año anterior, se actualizará el plan en base a los aspectos de mejora identificados y se realizará la planificación anual de actuaciones.

3.4.4.2. Fase 2: Ejecución del Plan de Cultura y Concienciación.

En esta fase se ejecutarán los programas de cultura y concienciación de acuerdo a la planificación establecida, además de evaluar el nivel de aceptación y acogida del plan implantado al objeto de revisar y mejorar sus contenidos.

Se pondrá especial atención en alcanzar sinergias con aquellas actuaciones de este Plan Director que puedan potenciar y facilitar la consecución de los objetivos del proyecto.

3.4.5. Plazo de ejecución.

- Fase 1: A finalizar en abril de 2011.

- Fase 2: A finalizar en diciembre de 2013.

3.4.6. Indicadores de seguimiento.

- Nivel de cumplimiento anual del Plan de Cultura y Concienciación.

3.5. PDS-JDA-P05 Plan de formación en seguridad.

3.5.1. Antecedentes.

Desde el año 2006, la Consejería de Economía, Innovación y Ciencia, y más concretamente la Secretaría General de Telecomunicaciones y Sociedad de la Información, lleva ejecutando un plan de formación orientado al personal adscrito a los Servicios con responsabilidad en la gestión de tecnologías de la información.

En línea con el impulso a las actuaciones en seguridad que se pretende alcanzar a través del presente Plan Director, se considera necesario analizar y replantear la estrategia formativa en la materia, al objeto de dotarla de un mayor alcance y profundidad.

3.5.2. Objetivos.

Mediante el presente proyecto se pretende:

- Dar a conocer la existencia de un Plan Director y de un marco normativo de seguridad, así como las actuaciones que de él se derivan.

- Mejorar el nivel de seguridad global de la Administración de la Junta de Andalucía, potenciando la formación en seguridad del personal adscrito a los Servicios con responsabilidad en la gestión de tecnologías de la información.

3.5.3. Beneficios.

Este proyecto garantizará la correcta formación en materia de seguridad de las personas al servicio de la Administración de la Junta de Andalucía, asegurando su homogeneidad, su adaptación por perfiles y el alineamiento con las estrategias definidas a nivel horizontal.

3.5.4. Planificación y fases.

3.5.4.1. Fase 1: Evaluación inicial.

En esta fase se evaluarán los contenidos del plan de formación desarrollado por la Secretaría General de Telecomunicaciones y Sociedad de la Información, así como el nivel de formación base y perfiles de sus personas destinatarias. En relación a este último punto se analizará:

- Perfiles profesionales y tecnologías de uso común de las personas destinatarias del plan de formación.

- Expectativas personales de las personas destinatarias del plan de formación.

- Grado de motivación del grupo para afrontar el proceso.

3.5.4.2. Fase 2: Elaboración del Plan de Formación en Seguridad.

En esta fase se concretarán las necesidades, personas destinatarias, planificación y el alcance de las acciones de formación. Como resultado, se producirá un documento de Plan de Formación en Seguridad que será remitido a los responsables de la Secretaría General de Telecomunicaciones y Sociedad de la Información.

Las acciones que recogerá este plan podrán incluir tanto eventos presenciales, como teleformación, adaptadas a las necesidades particulares de los distintos perfiles identificados (personal TIC, personal no TIC, alta dirección ...).

Durante los dos últimos meses de cada año se revisarán los resultados de ejecución correspondientes al año anterior y se actualizará el plan en base a los aspectos de mejora identificados.

3.5.5. Plazo de ejecución.

- Fase 1: A finalizar en enero de 2011.

- Fase 2: A finalizar en marzo de 2011.

3.5.6. Indicadores de seguimiento.

- Nivel de desarrollo del Plan de Formación en Seguridad.

3.6. PDS-JDA-P06 Revisiones técnicas de seguridad.

3.6.1. Antecedentes.

La ejecución del Programa Alcazaba incluyó la realización de auditorías técnicas de vulnerabilidades de sistemas corporativos y de los elementos de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía. Se pretende mediante el presente proyecto dar continuidad a la realización de revisiones técnicas de seguridad sobre los activos de esta Administración.

3.6.2. Objetivos.

Mediante el presente proyecto se revisará el grado de exposición de los sistemas de información de la Administración de la Junta de Andalucía a ataques derivados del aprovecha-

miento de vulnerabilidades, debilidades en el código, configuraciones incorrectas, etc.

3.6.3. Beneficios.

Este proyecto proporcionará la necesaria visibilidad del estado de la seguridad de los sistemas a nivel técnico, facilitando la toma de decisiones en la implantación de las medidas correctoras necesarias. Por otro lado, permitirá comprobar el cumplimiento de la normativa aplicable en materia de seguridad.

El enfoque horizontal del proyecto homogeneizará las pruebas realizadas y la forma de presentar sus resultados, posibilitando la comparación de los mismos.

3.6.4. Planificación y fases.

Este proyecto se ejecutará sobre un alcance limitado de organismos y en base a un Plan de Revisiones Técnicas.

3.6.4.1. Fase 1: Elaboración del Plan de Revisiones Técnicas.

En esta fase se concretará la planificación y el alcance de los trabajos, produciéndose un documento de Plan de Revisiones Técnicas.

Durante los dos últimos meses de cada año se revisarán los resultados de ejecución correspondientes al año anterior y se actualizará el plan en base a los aspectos de mejora identificados.

3.6.4.2. Fase 2: Ejecución del Plan de Revisiones Técnicas.

Para cada uno de los organismos incluidos en el ámbito de aplicación del plan, se realizarán las siguientes tareas:

- Revisión técnica de vulnerabilidades de los sistemas incluidos en el alcance, mediante la aplicación de técnicas automáticas y manuales de caja blanca y caja negra.
- Análisis de la causa raíz de los problemas detectados.
- Estudio de las medidas y estrategias correctoras a adoptar.
- Elaboración y entrega del Informe de Auditoría Técnica de Seguridad, el cual recogerá el listado de sistemas y servicios analizados, vulnerabilidades encontradas, resultados de su aprovechamiento y recomendaciones para la corrección de las debilidades.

3.6.5. Plazo de ejecución.

- Fase 1: A finalizar en diciembre de 2010.
- Fase 2: A finalizar en diciembre de 2013.

3.6.6. Indicadores de seguimiento.

- Nivel de cumplimiento anual del Plan de Revisiones Técnicas.

3.7. PDS-JDA-P07 Análisis de riesgos.

3.7.1. Antecedentes.

La ejecución del Programa Alcazaba incluyó la realización de análisis de riesgos de sistemas corporativos de la Administración de la Junta de Andalucía. Se pretende mediante el presente proyecto dar continuidad a dicha labor como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos.

3.7.2. Objetivos.

Mediante el presente proyecto se revisará el nivel de riesgo de los sistemas de información de la Administración de la Junta de Andalucía y se propondrá el plan de tratamiento a los riesgos identificados.

3.7.3. Beneficios.

Este proyecto permitirá identificar y analizar las amenazas que afectan a la Administración de la Junta de Andalucía y evaluar el nivel de riesgo al que se ve sometida. Este conocimiento mejorará la definición de estrategias en seguridad y redundará en un mejor aprovechamiento de las inversiones realizadas en este campo.

3.7.4. Planificación y fases.

Este proyecto se ejecutará sobre un alcance limitado de organismos y en base a un Plan de Análisis de Riesgos.

3.7.4.1. Fase 1: Elaboración del Plan de Análisis de Riesgos.

En esta fase se concretará la planificación y el alcance de los trabajos, produciéndose un documento de Plan de Análisis de Riesgos.

Durante los dos últimos meses de cada año se revisarán los resultados de ejecución correspondientes al año anterior y se actualizará el plan en base a los aspectos de mejora identificados.

3.7.4.2. Fase 2: Ejecución del Plan de Análisis de Riesgos.

Para cada uno de los organismos incluidos en el ámbito de aplicación del plan, se realizarán las siguientes tareas:

- Análisis de la estructura organizativa, procesos internos y activos de información de la entidad.
- Análisis de amenazas.
- Análisis de salvaguardas.
- Estimación del riesgo.
- Elaboración y entrega del Informe de Análisis y Tratamiento de Riesgos, el cual recogerá el análisis del estado de riesgo de los activos y las recomendaciones para el tratamiento del mismo.

3.7.5. Plazo de ejecución.

- Fase 1: A finalizar en diciembre de 2010.
- Fase 2: A finalizar en diciembre de 2013.

3.7.6. Indicadores de seguimiento.

- Nivel de cumplimiento anual del Plan de Análisis de Riesgos.

3.8. PDS-JDA-P08 Marco de desarrollo tecnológico de la Junta de Andalucía (MADEJA).

3.8.1. Antecedentes.

Una parte importante de los problemas de seguridad de los sistemas de información tiene su origen en defectos o carencias en las aplicaciones que los integran, lo cual eleva enormemente el riesgo de sufrir un incidente.

Por otra parte, la Administración de la Junta de Andalucía se encuentra desarrollando la construcción de MADEJA, el Marco de desarrollo de la Junta de Andalucía. A finales de julio de 2008 se hace pública su primera versión y desde entonces el proyecto sigue evolucionado, actualizándose y enriqueciéndose con contenido que abarca todo el ciclo de vida de un sistema de información, desde su concepción hasta la implantación y mantenimiento.

Si bien este proyecto se diseñó y comenzó con anterioridad a la elaboración de este Plan Director de seguridad, su naturaleza le hace formar parte de la estrategia de mejora definida en el plan dada la necesidad de incluir los conceptos de seguridad en los procesos de desarrollo de aplicaciones informáticas, así como desarrollar la ordenación administrativa que corresponda.

3.8.2. Objetivos.

El objetivo principal de este proyecto es mejorar la calidad de los sistemas de información, potenciando, entre otros aspectos, la seguridad.

Esta mejora en la seguridad puede ser directa, mediante la definición y verificación de requisitos y normas relativas a la seguridad de los sistemas de información, e indirecta, gracias a la mejora de otros aspectos como la disponibilidad y fiabilidad de los sistemas.

En aquellos casos en los que MADEJA produzca pautas concretas en materia de seguridad, estas serán incorporadas al marco normativo de seguridad cuyo desarrollo se plantea en este Plan Director.

En todos los subsistemas de MADEJA la seguridad es un principio de diseño transversal. Todas las directrices y pautas dictadas en MADEJA y relacionadas con la seguridad se considerarán integradas dentro de dicho marco normativo.

3.8.3. Beneficios.

La mejora de la calidad del código lleva implícita una mejora en aspectos asociados a la seguridad de los sistemas de información. Para minimizar los riesgos inherentes a cualquier producto software, MADEJA establece guías de buenas prácticas, pautas y directrices que incorporan los principios de seguridad desde las primeras fases del ciclo de vida del desarrollo, asegurando que no sea analizada en los productos resultantes sino desde la concepción del sistema hasta su puesta en explotación.

Por otra parte, debido al carácter práctico de MADEJA, se proporcionarán directrices sobre tecnologías concretas y se propondrán, en la medida de lo posible, las herramientas que faciliten el cumplimiento y verificación de dichas directrices. Como beneficio directo tendremos un conjunto de pautas de desarrollo más fáciles de aplicar y de verificar.

En la actualidad se está abordando la creación de la Oficina de Testing de la Oficina de Proyectos Horizontales, que el Plan asume como objetivo propio del mismo, que será la responsable de la verificación de las directrices proporcionadas por MADEJA en los proyectos horizontales. Entre estas directrices se encuentran las relativas a la seguridad de los sistemas de información. La Oficina de Testing pondrá en práctica un modelo que podrá ser extensible a otros organismos de la Administración de la Junta de Andalucía.

3.8.4. Planificación y fases.

3.8.4.1. Fase 1: Incorporación de contenidos iniciales.

Se incorporarán los siguientes contenidos relacionados con la seguridad:

- Pautas de desarrollo seguro, principalmente para tecnología JEE.
- Incorporación de la seguridad en el proceso de desarrollo.
- Herramientas que faciliten la verificación de la seguridad de los sistemas de información.

Se trata de una primera aproximación, que permitirá su puesta en práctica y la recogida de indicadores para la mejora continua.

3.8.4.2. Fase 2: Mejora continua.

Gracias a la experiencia en la aplicación de los productos de la fase anterior se tendrá la oportunidad de identificar mejoras y planificar su aplicación. En concreto, se pueden identificar las siguientes actividades:

- Establecimiento de una correspondencia entre los incidentes ocurridos y las pautas y directrices de MADEJA.
- Detección de las necesidades de nuevas pautas y directrices para rebajar las vulnerabilidades potenciales.

La aplicación práctica de los productos de la fase anterior está asegurada gracias al trabajo desempeñado por la Oficina de Testing citada anteriormente.

3.8.5. Plazo de ejecución.

- Fase 1: A finalizar en septiembre de 2010.
- Fase 2: A finalizar en diciembre de 2013.

3.8.6. Indicadores de seguimiento.

Número de pautas relacionadas con la seguridad.

Número de proyectos verificados por la Oficina de Testing.

Número de incidentes registrados no contemplados en MADEJA.

Número de incidentes registrados contemplados en MADEJA.

3.9. PDS-JDA-P09 Despliegue y explotación de Andalucía-CERT.

3.9.1. Antecedentes.

La ejecución del Programa Alcazaba incluyó la realización de una consultoría de diseño de un centro orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad (en adelante CERT) que pudieran materializarse sobre los sistemas de información de la Administración de la Junta de Andalucía.

3.9.2. Objetivos.

Mediante el presente proyecto se desplegará un conjunto de servicios reactivos, pro-activos y de gestión del riesgo orientados a la mejora y el impulso de la seguridad en el ámbito de la Administración pública, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía.

La puesta en funcionamiento de este centro se incorpora como objetivo del presente Plan.

Dicho centro prestará el siguiente conjunto de servicios:

- Información y alerta de amenazas de seguridad.
- Monitorización de eventos de seguridad.
- Detección de vulnerabilidades en sistemas.
- Detección, análisis y respuesta a incidentes de seguridad.
- Publicación de contenidos formativos, informativos y de concienciación en seguridad.
- Publicación de recomendaciones y guías técnicas.

3.9.3. Beneficios.

Este proyecto dotará a la Administración de la Junta de Andalucía de un centro especializado con el que se conseguirá una mejora de la eficiencia en la resolución de incidentes de seguridad y se reducirá el riesgo al que está sometida.

Gracias a este centro, la detección y respuesta ante incidentes será más rápida y requerirá menos esfuerzo. Por otra parte, será una potente herramienta para la concienciación y formación en materia de seguridad de la propia Administración pública, del sector empresarial y la ciudadanía. La concienciación y formación es fundamental para la generación de confianza y supondrá un importante impulso a la Sociedad de la Información en Andalucía.

3.9.4. Planificación y fases.

3.9.4.1. Fase 1: Implantación de las infraestructuras soporte.

En esta fase se realizará el suministro, instalación y puesta en marcha de las siguientes infraestructuras:

- Infraestructuras básicas de operación del centro.
- Consultoría previa y proyecto de implantación de la plataforma NAOS.
- Plataforma de monitorización de eventos de seguridad.
- Páginas web pública y privada del CERT.

3.9.4.2. Fase 2: Explotación de los servicios.

En esta fase se realizará el despliegue de los siguientes servicios:

- Información y alerta de amenazas de seguridad.
- Monitorización de eventos de seguridad.
- Detección automática de vulnerabilidades.
- Detección, análisis y respuesta a incidentes.
- Explotación y creación de contenidos para las web pública y privada del CERT.

3.9.5. Plazo de ejecución.

- Fase 1: A finalizar en diciembre de 2010.
- Fase 2: A finalizar en diciembre de 2013.

3.9.6. Indicadores de seguimiento.

- Número de servicios de seguridad incluidos en catálogo.
- Número de entidades suscriptoras de servicios.
- Número de peticiones de servicio recibidas.
- Número de peticiones de servicio atendidas.
- Porcentaje de usuarios satisfechos con el servicio.

3.10. PDS-JDA-P10 Sistema de gestión unificada de identidades (GUIA).

3.10.1. Antecedentes.

La Administración de la Junta de Andalucía dispone en la actualidad de un amplio abanico de aplicaciones y sistemas. La gestión de las identidades de todos estos empleados es una tarea compleja que implica a diferentes equipos: recursos humanos, administración, sistemas, desarrollo e infraestructura.

La heterogeneidad de los entornos de las aplicaciones, las diferentes políticas para los permisos y los diferentes equipos implicados en la gestión dan lugar a la inexistencia de un punto centralizado de gestión de identidades y auditoría.

Aunque algunos sistemas comparten el método de autenticación, las técnicas de autorización y permisos son propias de cada aplicación. Esto dificulta la gestión, el mantenimiento y aumenta el coste de los desarrollos nuevos que se acometen.

Si bien este proyecto se diseñó y comenzó con anterioridad a la elaboración de este Plan Director de seguridad, su naturaleza le hace formar parte de la estrategia de mejora definida en el plan dada la necesidad de incluir los conceptos de seguridad en el acceso a los sistemas de información, así como desarrollar la ordenación administrativa que corresponda.

3.10.2. Objetivos.

El proyecto GUIA busca la consecución de los siguientes objetivos:

- Realizar el control y gestión de la identificación digital de forma unívoca e inequívoca para todas las personas que accedan o puedan acceder a cualquiera de los sistemas de información de la Administración de la Junta de Andalucía, ya sea de forma interna o externa, así como el control y gestión de las autorizaciones de acceso, garantizando el cumplimiento de la normativa legal correspondiente.

- Disponer de un directorio corporativo para todos las personas usuarias que acceden a los sistemas de información, con una estructura adecuada y escalable y una arquitectura robusta en términos de disponibilidad, tolerancia a fallos, seguridad y rendimiento.

- Sentar las bases técnicas para la integración de las aplicaciones preexistentes y futuras con el directorio corporativo, facilitando la migración a los nuevos sistemas de autenticación.

3.10.3. Beneficios.

El proyecto GUIA permitirá la gestión unificada de todas las identidades digitales de las personas usuarias de los sistemas de información de la Administración de la Junta de Andalucía, es una solución global de seguridad, que trata de una forma directa la autenticación e identificación de las identidades, además de ser una solución que permite dar garantías de privacidad y seguridad sobre las aplicaciones y sistemas.

Además habilita mecanismos de autenticación robusta, como el acceso basado en certificado digital. La persona usuaria ya no tiene que conocer múltiples claves, con lo que se evitan malas practicas (anotar contraseñas, elección de contraseñas débiles fáciles de recordar pero también de deducir, etc.).

GUIA proporciona mecanismos de auditoría y se almacenan históricos de las autorizaciones solicitadas para los diferentes recursos en cada momento. La visión unificada de las identidades y accesos permite una aplicación inmediata de las políticas de seguridad y mejora la eficiencia en la gestión de la seguridad.

3.10.4. Planificación y fases.

3.10.4.1. Fase 1: GUIA-Administración.

El proyecto GUIA-Administración tiene como objetivo desarrollar, implantar y gestionar el Sistema de Gestión de Identidades de la Junta de Andalucía, que permitirá la identificación digital única y posibilite que el personal al servicio de la Administración de la Junta de Andalucía pueda acceder con una única identificación a los servicios que ofrecen los diferentes organismos garantizando la seguridad y privacidad del acceso.

3.10.4.2. Fase 2: GUIA-Ciudadano.

En esta fase se va a extender el Sistema de Gestión de Identidades a toda la ciudadanía, asegurando la gestión de la información con todas las garantías de seguridad y privacidad exigibles y la identificación digital única, sirviendo de apoyo al desarrollo de la trayectoria digital de la ciudadanía.

3.10.5. Plazo de ejecución.

- Fase 1: A finalizar en diciembre de 2013.
- Fase 2: A finalizar en diciembre de 2013.

3.10.6. Indicadores de seguimiento.

- Porcentaje de organismos/Consejerías integrados en aprovisionamiento de GUIA.
- Porcentaje de organismos/Consejerías integrados en el módulo de SSO de GUIA.
- Porcentaje de organismos/Consejerías integrados en el Directorio Corporativo.
- Número de aplicaciones/sistemas integrados en aprovisionamiento de GUIA.
- Número de aplicaciones/sistemas integrados en autenticación de GUIA.
- Número de aplicaciones/sistemas integrados en el módulo de SSO de GUIA.
- Número de aplicaciones/sistemas que usan el Directorio Corporativo.

3.11. PDS-JDA-P11 Centro de continuidad de aplicaciones TIC para la Administración de la Junta de Andalucía.

3.11.1. Antecedentes.

La Administración de la Junta de Andalucía puso en marcha en el año 2003 el Proyecto FENIX con el objetivo de dotarse de un Centro de Respaldo y Continuidad Informática que permitiera ofrecer servicios de calidad a la ciudadanía y estar protegidos frente a cualquier eventualidad que pudiera originar estados de contingencia en los sistemas de información.

Este proyecto pretende dar continuidad al proyecto FENIX adaptando el Centro de Respaldo a las nuevas tecnologías y soluciones existentes que permitan mejorar sus prestaciones y optimizar los recursos.

Si bien este proyecto se diseñó y comenzó con anterioridad a la elaboración de este Plan Director de seguridad, su naturaleza le hace formar parte de la estrategia de mejora definida en el plan dada la necesidad de gestionar la continuidad en caso de contingencia de los sistemas críticos para el funcionamiento de esta Administración.

Durante la fase de despliegue finalizada en marzo de 2010, se realizó la adquisición y puesta en marcha del nuevo equipamiento a instalar en el Centro de Continuidad y en las instalaciones de las entidades usuarias del servicio, así como la configuración y pruebas del servicio de respaldo en cada organismo.

Las actividades comprendidas en la fase de despliegue se subdividieron en los siguientes grupos de tareas específicas:

- Fase de logística: inventario de componentes hardware y software necesarios para el despliegue inicial de los servicios y activación de los mecanismos para la adquisición de los estos elementos.
- Fase de diseño: definición de los planes necesarios para garantizar la operatividad del hardware a desplegar en el centro de proceso de datos y delimitación del alcance de los trabajos.
- Fase de implantación y despliegue del centro de proceso de datos del Centro de Continuidad: ejecución de todas las tareas relativas a la implantación y despliegue de la infraestructura de procesamiento, almacenamiento y respaldo del Centro de Continuidad.
- Fase de implantación y despliegue en los organismos: implantación en cada uno de los organismos usuarios de los servicios del Centro de Respaldo y la ejecución del correspondiente plan de formación.

3.11.2. Objetivos.

Su objetivo es ofrecer la continuidad de los servicios TIC a la ciudadanía y usuarios con las menores interrupciones posibles en caso de producirse situaciones que impidieran su normal funcionamiento.

3.11.3. Beneficios.

Para la Administración es fundamental generar confianza en los servicios TIC ofrecidos. Las interrupciones en la prestación de los servicios TIC a la ciudadanía y usuarios no solo acarrea costes tangibles, también perjudica la imagen de la Administración y merma la confianza en la misma.

El desarrollo de este proyecto permitirá minimizar los efectos negativos asociados a las interrupciones de los servicios prestados a la ciudadanía.

3.11.4. Planificación y fases.

3.11.4.1. Fase 1: Soporte.

La fase de soporte recoge el desarrollo de un conjunto de procesos que se implementan dentro de la prestación de los servicios del Centro de Continuidad. Los procesos que se incluyen dentro del plan de operaciones son los que se de-

finen según ITIL para el soporte de servicios, la gestión de infraestructuras y la provisión de servicios. La implantación de este modelo de centro de servicios será gradual y conforme a las siguientes fases:

- Plan de transición: tareas necesarias para realizar la transferencia de competencias, incluyendo las actividades de preparación y adecuación del servicio que son necesarias para asumir la explotación y operación con garantías de éxito.

- Plan de transformación:

• Definición del catálogo de servicios.

• Definición del modelo de procesos e implantación de la CMDB.

• Soporte de servicios: puesta en marcha del centro de servicios e implantación de los procesos de gestión de la configuración, gestión de incidencias, gestión de problemas y gestión de cambios.

• Provisión del servicio: implantación de los procesos de gestión de los niveles de servicio, gestión de la capacidad, gestión de la disponibilidad y gestión de la continuidad.

3.11.5. Plazo de ejecución.

- Fase 1: A finalizar en septiembre 2012.

3.11.6. Indicadores de seguimiento.

- Número de servicios de replicación en producción en el centro de respaldo.

- Número de servicios de continuidad en producción en el centro de respaldo.

- Volumen de información replicada en el centro de respaldo.

- Número de cambios registrados por período (altas, bajas y modificaciones de servicios).

- Porcentaje de incidencias atendidas en plazo. (cumplimiento de ANS).

- Porcentaje de incidentes/número de servicios (ratio de calidad).

4. INDICADORES DE IMPACTO GLOBALES

Para el seguimiento y supervisión global de este plan, se definen indicadores de impacto que midan el grado de confianza en la Administración y los servicios que ésta presta. También aquellos que midan el éxito de los esfuerzos de concienciación en aspectos de seguridad de este plan.

- Grado de confianza respecto a Internet de los hogares andaluces.

- Percepción de la evolución del número de incidencias (%).

- Percepción sobre la seguridad en Internet de los hogares andaluces.

- Percepción de las demandas de los usuarios a la Administración.

5. CATÁLOGO DE PROYECTOS

- PDS-JDA-P01 Desarrollo y aprobación del marco normativo de seguridad de la Administración de la Junta de Andalucía.

- PDS-JDA-P02 Adecuación de los procesos de las entidades de la Administración de la Junta de Andalucía a la normativa de seguridad.

- PDS-JDA-P03 Auditoría de cumplimiento legal y del marco normativo de seguridad de la Administración de la Junta de Andalucía.

- PDS-JDA-P04 Cultura y concienciación en seguridad.

- PDS-JDA-P05 Plan de formación en seguridad.

- PDS-JDA-P06 Revisiones técnicas de seguridad.

- PDS-JDA-P07 Análisis de riesgos.

- PDS-JDA-P08 Marco de desarrollo tecnológico de la Junta de Andalucía (MADEJA).

- PDS-JDA-P09 Despliegue y explotación de Andalucía-CERT.

- PDS-JDA-P10 Sistema de gestión unificada de identidades (GUIA).

- PDS-JDA-P11 Centro de continuidad de aplicaciones TIC para la Administración de la Junta de Andalucía.