TÍTULO: PROYECTO DE DESPLIEGUE DEL CENTRO DE SEGURIDAD TIC DE ANDALUCÍA (ANDALUCIA-CERT)

AUTORES: VÍCTOR MANUEL IGLESIAS PALOMO, OLIVER LÓPEZ YELA, NIEVES ESTRADA UMBRÍA

1. Introducción

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.

La estrategia seguida por la Junta de Andalucía 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 todo ello, la Consejería de Innovación, Ciencia y Empresa ha elaborado el Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones 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.

El objeto del Plan Director es definir con claridad la estrategia en materia de seguridad TIC a seguir por la Junta de Andalucía durante el periodo 2010-2013, con el detalle de las diferentes actuaciones a acometer. Permitirá 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 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 del 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.

Dicho Plan Director incluye entre sus proyectos el despliegue y explotación del centro de seguridad TIC de Andalucía (en adelante ANDALUCIA-CERT), mediante el cual 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, Universidad, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía.

ANDALUCIA-CERT se constituye como el instrumento de prevención, detección y respuesta a incidentes y amenazas de seguridad, siendo un proyecto innovador llamado a convertirse en el punto de referencia en cuanto a seguridad de la información en Andalucía se refiere.

La Consejería de Innovación, Ciencia y Empresa publicó en el mes de agosto de 2009 el concurso para la contratación de los servicios y proyectos de implantación del Centro de Seguridad TIC de Andalucía, expediente cuyos dos lotes fueron adjudicados en el mes de enero de 2010 a las empresas INDRA SISTEMAS, S.A. y TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.

ANDALUCIA-CERT se encuentra ubicado en las dependencias de la Sociedad Andaluza para el Desarrollo de la Sociedad de la Información, S.A.U. (SADESI) ubicadas en el edificio Zoco de la localidad de Tomares (Sevilla).

Figura 1: Edificio Zoco en Tomares (Sevilla)

Queremos destacar finalmente el importante apoyo recibido desde el Ministerio de Industria, Turismo y Comercio a través del Plan Avanza.

2. ¿Por qué un centro de seguridad en la Junta de Andalucía?

Entre las principales razones que han llevado a la constitución de ANDALUCIA-CERT podemos destacar las siguientes:

Razones operativas:

- Necesidad de responder de forma centralizada, rápida y eficaz ante incidentes de seguridad que afecten a sistemas de cualquier Organismo.
- Necesidad de coordinación entre los Organismos de la Junta de Andalucía en un entorno interconectado (Red Corporativa de Telecomunicaciones).
- Mayor eficiencia en las operaciones de seguridad TIC, mejorando la calidad y disponibilidad de los servicios (seguridad 24x7x365).
- Necesidad de coordinación con centros de respuesta a incidentes externos (CCN-CERT, INTECO-CERT, CERT-Red Iris, ...) y otras Administraciones (CC.AA., AA.LL., ...).

Razones económicas:

- Creación de economías de escala en el despliegue de plataformas horizontales de gestión de la seguridad.
- Reducción de costes asociados a la indisponibilidad de servicios TIC y daño en la imagen de la Administración.

Razones de contexto:

- Aumento del número y grado de peligrosidad de las amenazas a las que se encuentran expuestos los sistemas de información y comunicaciones.
- Coherencia con la estrategia de seguridad TIC definida en el Plan Director de Seguridad de las Tecnologías de la Información y Comunicaciones de la Junta de Andalucía (fruto del Programa Alcazaba 2007-2009).
- Coherencia con las políticas de desarrollo de la Sociedad de la Información de la Junta de Andalucía.
- Aprovechamiento de sinergias con otros proyectos horizontales de la Junta de Andalucía.
- Alineamiento con la tendencia actual en implantación de buenas prácticas de seguridad y gestión de riesgos emergentes.

- Promoción de un tejido empresarial en seguridad TIC en Andalucía, basado en la prestación de servicios de alto valor añadido e I+D+I.

3. Definición, objetivos y misión de ANDALUCIA-CERT

ANDALUCIA-CERT es el centro experto para la gestión de la seguridad TIC de la Junta de Andalucía. Está formado por un equipo de profesionales especializados en seguridad, organizados según procesos (definidos siguiendo modelos y estándares internacionalmente reconocidos) y dotados de las herramientas específicas necesarias.

Los principales objetivos de ANDALUCIA-CERT son:

- Contribuir a la mejora de la Seguridad de la Información en la comunidad Autónoma Andaluza.

- La mejora de la seguridad y calidad de los servicios prestados por la Administración de la Junta de Andalucía a la ciudadanía.

- La generación de confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública.

La misión fundamental de ANDALUCIA-CERT es la de proporcionar la capacidad de detección y respuesta ante incidentes de seguridad en la Administración de la Junta de Andalucía.

Entendemos que para conseguir con éxito lo anterior, la respuesta a un incidente de seguridad debe comenzar indefectiblemente en su prevención. Por tanto, también es misión esencial de ANDALUCIA-CERT potenciar la formación, concienciación y sensibilización en seguridad dentro de Andalucía.

La evolución de las amenazas y necesidades del grupo atendido de ANDALUCIA-CERT, requerirán inevitablemente la evolución del centro y de sus servicios. Así pues, ANDALUCIA-CERT evolucionará dinámicamente adaptándose y ampliándose para garantizar el cumplimiento de sus objetivos.

4. Servicios iniciales

Para alcanzar los objetivos marcados y desarrollar la misión encomendada, ANDALUCIA-CERT proporcionará a su grupo atendiendo un conjunto de servicios.

Se exponen a continuación los servicios que inicialmente se prestarán desde las instalaciones del centro. A este conjunto elemental de servicios se sumarán otros a medida que evolucionen las necesidades, amenazas y confianza en ANDALUCIA-CERT.

4.1 Servicio de detección y respuesta a incidentes de seguridad

Este servicio da respuesta a la misión fundamental encomendada a ANDALUCIA-CERT y tiene por finalidad:

- Maximizar la capacidad de detección de incidentes de seguridad aportando visibilidad y perspectiva.
- Minimizar el tiempo de respuesta ante incidentes de seguridad.
- Minimizar daños derivados de los incidentes de seguridad acaecidos.

Para ello el servicio de detección y respuesta a incidentes de seguridad cubrirá las funciones de:

- Análisis, tratamiento, seguimiento y resolución de incidencias de seguridad notificadas por cualquier entidad de la Junta de Andalucía o detectadas automáticamente por la plataforma en base al modelo de gestión de incidentes definido por el CERT® Coordination Center (CERT/CC).
- Interlocución con las entidades de la Junta de Andalucía.
- Coordinación con agentes externos a la Junta de Andalucía.
- Operación, explotación y adaptación evolutiva de la plataforma de monitorización de eventos de seguridad, incluidos los sensores remotos.
- Diseño, implantación, actualización y documentación de los patrones de identificación de alertas y corrección de falsos positivos en la Plataforma.

El grupo de respuesta a incidentes de seguridad estará formado por profesionales especializados y dedicados exclusivamente a este servicio. Además el grupo contará con el apoyo externo de empresas de reconocido prestigio en el campo de la seguridad, para la resolución de aquellos incidentes que por su complejidad lo requieran.

El servicio se prestará en horario ininterrumpido todos los días del año (24x7x365).

En cuanto a la resolución efectiva de las incidencias y alarmas de seguridad, el grupo de respuesta a incidentes de seguridad dará soporte remoto a los responsables técnicos de las entidades de la Administración de la Junta de Andalucía, vía teléfono y correo electrónico.

Dentro del proyecto se realizará la definición, implantación, actualización y documentación en el gestor documental del centro de los procesos y procedimientos operativos descritos en el modelo de gestión de incidentes definido por el CERT® Coordination Center (CERT/CC), el estándar ISO/IEC 20000, UNE-

ISO/IEC 27001 y BS 25999. El alcance de los procesos definidos cubrirá todas las funciones de prevención, detección, tratamiento y resolución de incidentes de seguridad.

Para la optimización de los procesos de gestión de incidentes, se desplegará una plataforma central de correlación OSSIM en las dependencias del ANDALUCIA-CERT y la arquitectura distribuida necesaria en las dependencias de los Nodos de Interconexión de la Red Corporativa de Telecomunicaciones y sedes de la Junta de Andalucía.

Dicha plataforma recogerá los eventos de los dispositivos y sistemas monitorizados, realizará la correlación con otras fuentes de información y generará alertas de seguridad basándose en los siguientes requisitos:

- Capacidad de monitorización de dispositivos de seguridad y servidores de la Junta de Andalucía.
- Capacidad de alertar un comportamiento anómalo de la solución ante fallos, como por ejemplo, falta de comunicación con los agentes recolectores u otros.
- Permitir correlación de diferentes fuentes de información, como puedan ser el resultado de escaneo de vulnerabilidades, eventos de dispositivos de seguridad y servidores e inventario de activos.
- Capacidad para implementar distintos enfoques de correlación.
- Facilidad de integración con distintas tecnologías fuente de eventos.
- Al objeto de preservar la autenticidad, confidencialidad e integridad de los datos durante la recolección y transmisión de la información la solución hará uso de mecanismos de autenticación y cifrado.
- Optimización del tráfico generado en red mediante el uso de mecanismos que minimicen el consumo de ancho de banda entre los componentes de la solución.
- La solución permitirá almacenamiento de eventos normalizados para unificar distintos formatos de eventos de los distintos dispositivos y poder ser tratados de forma más eficiente.
- La solución permitirá realizar correlaciones avanzadas sobre los eventos que se produzcan y el establecimiento de reglas para la búsqueda de anomalías.
- Reglas de respuesta ante eventos. Para cada evento posible se podrá definir una respuesta particularizada a la naturaleza del evento y la criticidad para el negocio del activo afectado.

- La herramienta de correlación dispondrá de un sistema de consultas sobre los eventos que permita realizar análisis forense.

- La herramienta ofrecerá funcionalidades SEM, asegurando la integridad de las evidencias y permitiendo su admisión en procesos judiciales.

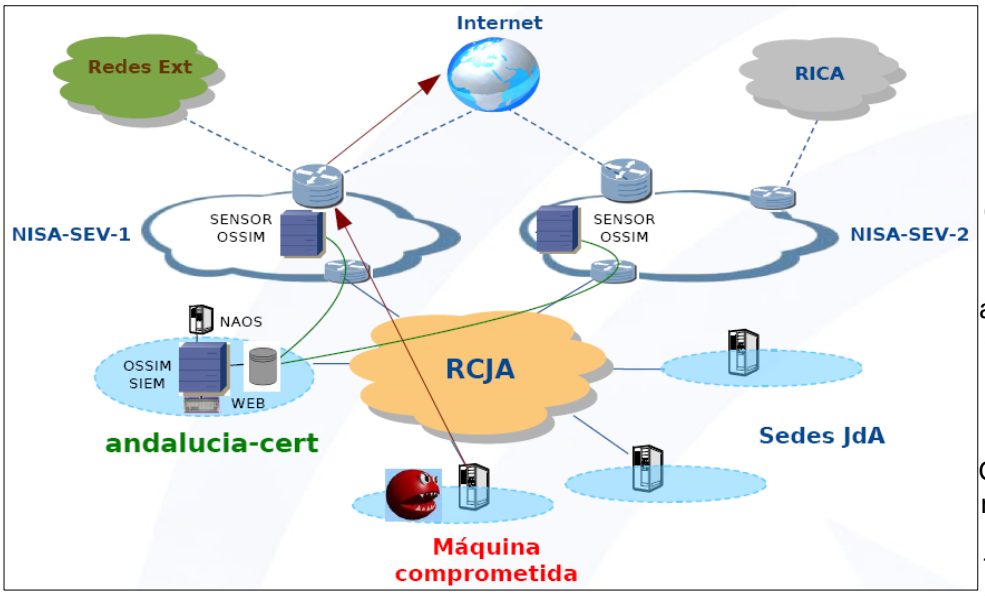

Figura 2: Integración de OSSIM en la arquitectura de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía

4.2 Servicio de información y alerta de amenazas de seguridad

Su objetivo es alertar en tiempo real a las Entidades de la Administración de la Junta de Andalucía de las amenazas de seguridad que puedan afectar a sus activos de información. Se conseguirá de está forma minimizar el tiempo de exposición a estas amenazas y reducir el riesgo asociado.

Igualmente, se difundirá a través de las web pública y privada del centro alertas, noticias e información relevante sobre seguridad mediante boletines periódicos.

La información contenida en los boletines y alertas estará contrastada con diversas fuentes de información e incluirá, para el caso de vulnerabilidades, información detallada de descripción y clasificación de la vulnerabilidad, plataformas afectadas, riesgo/criticidad, solución a la debilidad, acciones preventivas y recursos de ayuda, relación con identificadores estándar e histórico de versiones.

Este servicio incluirá, así mismo, la puesta en marcha de una base de conocimiento de vulnerabilidades y estrategias de respuesta. Dicha base de conocimiento permitirá su explotación y consulta mediante búsquedas avanzadas por parte del personal del centro y de los usuarios a través de las web pública y privada. Además

estará integrada con la plataforma de monitorización de eventos de seguridad siendo una fuente de información más para la correlación de eventos de seguridad.

La información contenida en los boletines y alertas estará en idioma castellano, así como la base de conocimiento de vulnerabilidades y estrategias de respuesta. En la descripción e identificación de las vulnerabilidades se contemplará el uso de los estándares internacionales CVE (Common Vulnerabilities and Exposures), CPE (Common Platform Enumeration) y CVSS (Common Vulnerability Scoring System).

Este servicio permitirá que cada entidad de la Administración de la Junta de Andalucía pueda, a través de la web privada del centro:

- Dar de alta y actualizar su inventario de sistemas y aplicaciones.
- Consultar históricos, estadísticas e informes de análisis.
- Consultar las vulnerabilidades por fecha, plataforma afectada, riesgo/criticidad y palabras clave.
- Configurar los servicios de notificación.

Así mismo, todos los usuarios podrán, a través de la web pública del centro:

- Consultar las vulnerabilidades por fecha, plataforma afectada, riesgo/criticidad y palabras clave.

4.3 Servicio de formación, información y concienciación

La formación y concienciación de todos los agentes involucrados en un sistema de información, desde usuarios hasta personal técnico, es una herramienta valiosísima en la mejora de su seguridad.

Por otro lado, la formación, información y concienciación son multiplicadores de recursos, cuanto más conocimiento sobre amenazas y seguridad tengan todos los agentes involucrados, más óptimo será el trabajo del grupo de respuesta a incidentes.

Las páginas web serán el principal medio de comunicación y acceso a la información de seguridad. Tendrá una web pública y una web privada accesible solamente por las Entidades de la Junta de Andalucía. Y se constituirá como canal multidireccional abierto para la generación y compartición de conocimiento en el ámbito de la seguridad.

La página web pública del centro estará publicada en Internet, y ofrecerá contenidos formativos, de concienciación y sensibilización en seguridad, guías y recomendaciones técnicas de seguridad en sistemas, boletines informativos diarios y resúmenes mensuales. Estos contenidos serán actualizados a diario en

colaboración con empresas y centros de seguridad de la información nacionales e internacionales relevantes.

La página web privada será únicamente accesible desde la Red Corporativa de Telecomunicaciones de la Junta de Andalucía. Ofrecerá contenidos personalizados para las Entidades de la Administración de la Junta de Andalucía, así como informes de seguridad generados por la plataforma de monitorización de eventos de seguridad y el servicio de información y alerta de amenazas de seguridad. Éstos serán únicamente accesibles mediante los correspondientes mecanismos de autenticación.

Los anteriores contenidos se desarrollarán en idioma castellano y adaptarán a los siguientes perfiles y comunidades de usuarios:

- Perfiles de usuario: usuario sin conocimientos en seguridad, usuario con conocimientos en seguridad básicos y usuario con conocimientos avanzados en seguridad.

- Comunidades destino: ciudadanía, empresa, administración local y administración autonómica.

En cuanto a la plataforma tecnológica, los sitios web del ANDALUCIA-CERT emplearán software de servidor web, base de datos, servidor de aplicaciones y sistema gestor de contenidos. Todas las herramientas estarán basada en código abierto. Se usará como sistema gestor de contenidos Drupal.

5. Vocación de servicio público

El centro de seguridad TIC de Andalucía, ANDALUCIA-CERT, nace con una clara vocación de servicio público. Y es este el principio de diseño esencial con el que inicia su andadura y el que marcará su desarrollo futuro.

Su principal razón de ser es la de garantizar a la ciudadanía el derecho a relacionarse con la Administración Pública Andaluza por medios electrónicos seguros. Potenciando la calidad de los servicios públicos basados en Tecnologías de la Información y la Comunicación, y asumiendo la responsabilidad de la administración en este sentido.

La Sociedad de la Información y el Conocimiento, hacia la que Andalucía ya inició su tránsito, es una sociedad basada en la confianza.

En nuestro modelo de sociedad, la confianza es el soporte de todos los procesos, relaciones sociales, económicas y culturales. Para potenciar la confianza en este nuevo modelo, es condición sin equanom garantizar la seguridad de los medios y tecnologías que lo soportan.

Hoy en día somos conscientes de que esa confianza no es ilimitada y lo más importante, una vez que esa confianza se ha perdido, es muy difícil de recuperar.

En este contexto ANDALUCIA-CERT será una valiosa fuente de generación de confianza y una herramienta más, al servicio de la ciudadanía Andaluza, para apoyar el proceso de cambio que ha dado paso a una sociedad interconectada, sin limitaciones espaciales, que se expande a nivel mundial y reinterpreta las relaciones sociales, económicas y culturales.