Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Seguridad en el ciclo de vida de los sistemas TIC

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-9261-151117*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*17/11/2015*
N° de Páginas	*1 de 10*

1 TABLA DE CONTENIDOS

2 OBJETO

Es objeto de este documento es concienciar la necesidad del tratamiento de los requisitos de seguridad y la gestión de los riesgos durante el ciclo de vida de sistemas de información. El contenido de este informe está basado en la guía CCN-STIC-205 "Actividades de Seguridad en el Ciclo de Vida de los Sistemas TIC" del CCN-CERT, al cual remitimos para una descripción pormenorizada.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía. Este documento debe contemplarse como una guía resumen para el tratamiento de los requisitos de seguridad durante el ciclo de vida de los sistemas.

Por otro lado, indicar que existe una serie de metodologías y procesos de desarrollo seguro de referencia, y que no se cubre en este documento, como son el proceso de ciclo de vida de desarrollo de seguridad (SDL, Security Development Lifecycle) de computación confiable de Microsoft, o el esquema de desarrollo de software seguro TSP-Secure (TSP, Team Software Process) del Software Engineering Institute.

4 SITUACIÓN

Los TIC (Sistemas de las Tecnologías de la Información y las Comunicaciones) son un componente básico para conseguir los niveles de calidad y productividad actuales.

Es importante incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la Organización.

Es de vital importancia tomar en consideración la seguridad del sistema antes y durante su desarrollo. La seguridad debe estar embebida en el sistema desde su primera concepción.

Los responsables de planificación, tanto técnica como económica, deberán tener en cuenta la seguridad en todas las fases del ciclo de desarrollo, de forma que haya cobertura técnica, temporal y presupuestaria para implantar las medidas de protección identificadas.

Se pueden identificar dos tipos de actividades diferenciadas:

- SSI: actividades relacionadas con la propia seguridad del sistema de información producido.
- SPD: actividades que velan por la seguridad del proceso de desarrollo del sistema de información.

La mayor parte de esta guía se centrará en la seguridad del sistema de información producido.

Mediante un análisis y un tratamiento sistemático, el desarrollo metódico es la forma mas eficaz de gestionar los riesgos del sistema.

Los requisitos de seguridad deben determinarse a la par que los requisitos funcionales. Así como los costes de las medidas de seguridad deben ser parte de los elementos de decisión entre diferentes arquitecturas del sistema.

Cuando existan productos en el mercado (COTS), se preferirán a desarrollos específicos. También se deberá analizar la opción de adaptar los requisitos del sistema a las posibilidades de sistemas o componentes ya existentes antes que desarrollar nuevos sistemas específicos.

Las medidas de protección aprobadas deben incorporarse durante la fase de adquisición / desarrollo, formando parte integral del sistema que se presenta para su aceptación.

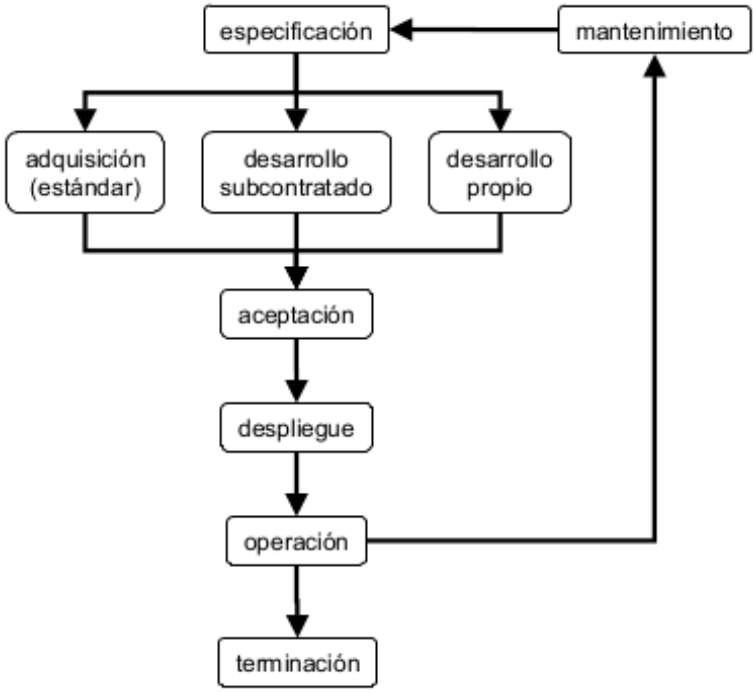
El análisis de riesgos es una actividad fundamental de soporte de un sistema de información por cuanto analiza los bienes a proteger, identifica las amenazas a las que pudieran estar expuestos y ayuda a identificar y calificar las salvaguardas pertinentes. El análisis de riesgos debe verse como un método de análisis del sistema que informa en todo momento de la posición de riesgo y permite tomar decisiones alineadas con el riesgo residual aceptado, cubriendo las fases del ciclo de vida del sistema. El modelo de riesgos debe correr parejo con el sistema de información, recogiendo su evolución propia (activos y salvaguardas) y la del entorno en el que opera (amenazas).

Sin perjuicio de que se aplique en su totalidad lo establecido en la guía CCN-STIC-201, de "Organización y Gestión para la Seguridad de las TIC", los siguientes roles son especialmente significativos en el desarrollo de sistemas:

- Autoridad de acreditación (AA) o en quien esta delegue (ADA): Aprueba formalmente la capacidad para pasar a producción.
- Autoridad de Seguridad TIC (ASTIC): Responsable de las especificaciones y decisiones tomadas a lo largo del ciclo de vida.
- Supervisor de Seguridad TIC (SSTIC): Responsable de la supervisión de las medidas y procedimientos de seguridad de los sistemas a su cargo. Depende del ASTIC.
- Responsable Seguridad del Área (RSA): A cargo de los aspectos de seguridad física de las instalaciones relacionadas con el sistema. Depende del ASTIC.
- Autoridad Operativa de Seguridad TIC (AOSTIC): Responsable de la operación del sistema.
- Administrador de Seguridad del Sistema (ASS): Responsable de la ejecución de las medidas de seguridad. Depende del AOSTIC.
- Equipo de Respuesta a Incidentes de Seguridad (ERIS): Responsable de la gestión de incidencias de operación. Depende del AOSTIC.

5 CICLO DE VIDA

Un sistema sigue un ciclo de vida a través de varias fases expuestas en la siguiente gráfica y apartados:



5.1 Especificación

Es la fase que determina los requisitos que se deben satisfacer en el sistema, tales como qué servicio necesita, o identificación de los requisitos necesarios para establecer los niveles de seguridad de la información, la calidad del servicio, los criterios de aceptación e instrucciones para su adquisición o desarrollo.

Esta fase se encargará de la especificación del los perfiles de usuarios, así como los requisitos de identificación y autenticación. Es la que dará desarrollara las garantías o requisitos de confidencialidad, integridad, disponibilidad y los requisitos de monitorización de controles de entrada salida de datos y registros (log). También se determinan los indicadores de RTO (Recovery Time Objective, tiempo de recuperación del servicio) y el RPO (Recovery Point Objective, margen tolerable de pérdida de datos) para el plan de continuidad.

Especialmente se identifican las salvaguardas y se toman en consideración si ya se encuentran disponibles en el entorno en el que el sistema se desplegará. En este caso se recopilarán y se evaluarán, de forma que los requisitos de seguridad del sistema tengan 2 partes:

- Base: utilización de salvaguardas disponibles.
- Marginal: nuevas salvaguardas o mejoras de las existentes.

Por ejemplo, el modelo de desarrollo del software seguro de Microsoft debe de plantearse de tal forma que el sistema cumpla los principios de:

- Seguro por diseño: la arquitectura, el diseño y la implementación del software se deben realizar de manera que proteja tanto el software como la información que procesa, además de poder resistir ataques.
- Seguro por definición: en el mundo real, el software no es nunca totalmente seguro, por lo que los diseñadores deben asumir que habrá errores de seguridad. Por ejemplo, el software debe ejecutarse con los mínimos privilegios necesarios y los servicios y las características que no sean necesarios de manera habitual deben deshabilitarse de manera predeterminada o establecer que sólo unos pocos usuarios puedan tener acceso a ellos.
- Seguro en distribución: se debe incluir con el software información y herramientas que ayuden a los administradores y a los usuarios a utilizar este software con seguridad. Además, la implementación de las actualizaciones debe ser sencilla.
- Comunicaciones: los programadores de software deben estar preparados para detectar las vulnerabilidades de seguridad del producto y deben comunicarse de manera abierta y responsable con los usuarios y los administradores para ayudarles a tomar las medidas de protección adecuadas (como la actualización o la implementación de soluciones alternativas).

5.2 Adquisición o desarrollo

En esta fase se estudia si se adquiere software estándar (COTS), mediante desarrollo propio o contratos de adquisición y mantenimiento.

El modelo de análisis de riesgos de activos se enriquecerá con los activos identificados en la fase de especificación, con nuevas amenazas sobre los nuevos componentes. En la identificación se tendrá en cuenta el perfil de exposición de cada activo a la exposición a amenazas de origen natural o industrial, los posibles mecanismos de ataque y las diferentes vías de ataque. En la valoración se tendrá en cuenta:

- Caracterización de los posibles atacantes (naturales, industriales y personas).
- Características del atacante (formación, experiencia, etc).
- Motivación del atacante (deseo de poseer, deseo de destruir, posibles ganancias económicas).
- Potencia del atacante (conocimientos, capacidad técnica y económica) .
- Tiempo requerido para la perpetración del ataque (distinguiendo entre ataques fulgurantes y ataques que requieren tiempo).

5.3 Aceptación

Tanto si es un sistema nuevo como si es modificación de un sistema anterior, nunca un sistema debe entrar en operación sin haber sido formalmente aceptado.

Tal aceptación conlleva unas pruebas de aceptación, validación de documentación y la formación de administradores, operadores y usuarios.

Esta fase también puede incluir elementos que garanticen la seguridad del sistema, mediante certificaciones de seguridad y acreditaciones.

Las salvaguardas identificadas en las fases anteriores son inspeccionadas para cerciorarse de que están dispuestas y operativas con la calidad requerida.

Hay que establecer el marco de seguridad de los servicios externos que se utilicen estableciendo acuerdos de nivel(es) de servicio y acordar las condiciones de inspección de la seguridad de sistemas ajenos.

Ha de revisarse que se ha cumplido unas técnicas de programación segura y una gestión correcta del código fuente, tales como un correcto control de acceso y versiones. Las pruebas que corresponden la fase de aceptación son las siguientes:

- Inspección de servicios y código: Engloba fugas de información, puertas traseras de acceso, escalado de privilegios y problemas de desbordamiento de registros (Buffer Overflow).
- Datos de prueba: Los datos deben ser realistas y si no se puede evitar que sean reales, hay que controlar las copias y los accesos.
- Pruebas funcionales: Las pruebas se realizaran de los servicios de seguridad, de tal manera que se realizará una simulación de ataques, intrusiones controladas (Hacking ético) y pruebas de carga.

La aceptación puede incluir una certificación de la seguridad por un tercero y una autorización formal mediante una acreditación para operar.

5.4 Despliegue

Esta fase lleva a cabo la instalación del sistema, la integración en su entorno, configuración y la carga de datos iniciales. Todo ello incluyendo su respectivo plan de continuidad.

Para la realización del despliegue será necesario un inventario de aplicación en operación, llevar un control de gestión de cambios de normativas y procedimientos, establecer un criterio de claves y una formación inicial tanto administradores, operadores y usuario final.

5.5 Operación

Los usuarios usan el sistema y son atendidos por parte de los administradores y/o los operadores en los incidentes de seguridad. Por otra parte, los operadores y administradores se encargan de la configuración, mantenimiento y gestión de los registros de actividad. Se llevarán a cabo las normativas y procedimientos de gestión de usuarios, claves, registros (log) y la gestión de las incidencias y sus fases (registro, escalado, plan de emergencia y recuperación).

Esta fase se analizará continuamente el estado de riesgo del sistema, incorporando el mejor conocimiento que en cada momento se tenga de las amenazas, vulnerabilidades, incidentes y variación en las técnicas de un atacante; con objeto de evitar la exposición y aumentar la protección de las salvaguardas.

En el ciclo de mantenimiento se analizaran normativas y procedimientos de solicitud y aprobación, incluyendo el análisis diferencial de riesgos y aprobación de las nuevas medidas. Se tendrán en cuenta si es necesario la re-certificaciones y re-acreditaciones de los sistemas.

La incorporación de un mejor conocimiento del entorno puede llevar a una nueva evaluación del riesgo al que está expuesto el sistema, puede ser el desencadenante de un ciclo de mantenimiento.

5.6 Mantenimiento

Esta fase es necesaria cuando el sistema requiera un mantenimiento que obligue a regresar a cualquiera de las etapas anteriores, en última instancia a la especificación básica, ya sea por la aparición de nuevos requisitos, o por la detección de un fallo en el sistema. Los ciclos de mantenimiento pueden iniciarse por varios motivos:

- Cambio de las funcionalidades del sistema: bien por inclusión de nuevas funciones, por modificación de las existentes o por retirada de las mismas.
- Nuevo entorno de servicios subcontratados.
- Nuevos requisitos de seguridad.
- Nuevos perfiles de ataque: cambios en la caracterización de los atacantes o en las vías y mecanismos de ataque.

En cualquiera de los casos es necesario realizar un nuevo ciclo de gestión de riesgos en los que se incluya el análisis, evaluación, decisión relativa al tratamiento y, en su caso, implantación de un nuevo sistema de salvaguardas que será objeto de una fase de aceptación previa a la puesta en operación.

5.7 Terminación

Eventualmente un sistema será retirado del servicio. Esta terminación debe ser ordenada, siguiendo una política que determine qué debe conservarse, qué debe destruirse concienzudamente y que puede ser simplemente desechado.

En esta fase se realizarán las siguientes acciones:

- Destrucción de información.
- Copia y custodia de información.
- Eliminación del código operativo: ejecutable, datos de configuración y cuentas de usuario.
- Eliminación de registros de actividad de sistemas en operación.
- Revisión de las copias de seguridad.
- Destrucción de soportes de información electrónicos y no electrónicos.

Debe realizarse un análisis de riesgos sobre el material retenido teniendo en cuenta el conjunto de información y el equipamiento dispuesto para su custodia. Se identificarán salvaguardas necesarias para garantizar la seguridad de los elementos custodiados.

6 CONCLUSIONES

La seguridad en los sistemas debe ser considerado como un aspecto importante dentro del control interno de cada organización, con un alto porcentaje de automatización de operaciones, y sobre todo estableciendo un uso en las metodologías de ciclo de vida.

En tal sentido, es un proceso integrado no solo inherente a las unidades organizativas que tienen como función explicita la seguridad informática y el control en una organización, sino que involucra desde la alta dirección hasta todo el personal que proyecta, diseña, administra y gestiona los aplicativos.

Considerando lo anteriormente expuesto para el logro de una seguridad razonable en un ambiente automatizado es menester hacer cumplir los componentes de control interno y al menos, los criterios de información confidencialidad, integridad y disponibilidad, en todas las etapas del ciclo de vida de un aplicativo.

Por otra parte y considerando el estado actual de las normativas nacionales sobre el tema, constituye un aporte al logro de la implementación real del tratamiento de los riesgos de automatización en la entidad, lo cual le aporta valor técnico y contribuye a minimizar las vulnerabilidades y sus consecuencias.

7 GLOSARIO

CCN: Centro Criptológico Nacional.

COS: Concepto de Operación del Sistema.

COTS: Commercial off-the-Shelf Software.

DRES: Declaración de Requisitos Específicos de Seguridad.

POS: Procedimientos Operativos de Seguridad.

RPO: Recovery Point Objective.

RTO: Recovery Time Objective.

SDLC: System Development Life Cycle.

SLC: System Life Cycle.

SPD: Seguridad del Proceso de Desarrollo.

STIC: Seguridad de las Tecnologías de la Información y Comunicaciones.

SSI: Seguridad del Sistema de Información.

TIC: Tecnologías de la Información y Comunicaciones.

8 DOCUMENTACION DE REFERENCIA

CCN – Guías STIC, Seguridad en las Tecnologías de Información yComunicaciones,

NIST Special Publications for security guidance

Códigos de Buenas Prácticas de Seguridad. UNE-ISO/IEC 17799

ISO/IEC 27002