ANALISIS DE RIESGOS EN SISTEMAS

Unidad 8: Desarrollo de sistemas de información

Objetivo específico 8: El alumno aprenderá como se desarrollan los sistemas de información basándose en los sistemas de seguridad de información, desde su fase de especificación, la fase de diseño, la puesta en marcha observación, mantenimiento la documentación y la elaboración de la seguridad del proceso de desarrollo.

Conceptos a desarrollar en la unidad: Desarrollo de sistemas de información, Inicialización de los procesos, SSI – Seguridad del sistema de información, Ciclo de vida de las aplicaciones, Contexto, Fase de especificación: adquisición de datos, Fase de diseño: estudio de opciones, Soporte al desarrollo: puntos críticos, Aceptación y puesta en marcha: puntos críticos, Operación: análisis y gestión dinámicos, Ciclos de mantenimiento: análisis marginal, Terminación, Documentación de seguridad, SPD – Seguridad del proceso de desarrollo y Referencias

Introducción

Las aplicaciones *(software)* constituyen un tipo de activos frecuente y nuclear para el tratamiento de la información en general y para la prestación de servicios basados en aquella información. La presencia de aplicaciones en un sistema de información es siempre una fuente de riesgo en el sentido de que constituyen un punto donde se pueden materializar amenazas. A veces, además, las aplicaciones son parte de la solución en el sentido de que constituyen una salvaguarda frente a riesgos potenciales. En cualquier caso es necesario que el riesgo derivado de la presencia de aplicaciones esté bajo control.

El análisis de los riesgos constituye una pieza fundamental en el diseño y desarrollo de sistemas de información seguros. Es posible, e imperativo, 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 un hecho reconocido que tomar en consideración la seguridad del sistema antes y durante su desarrollo es más efectivo y económico que tomarla en consideración a posteriori. La seguridad debe estar embebida en el sistema desde su primera concepción.

El riesgo como pieza fundamental de la seguridad de los sistemas en varios de sus principios básicos son:

La seguridad como un proceso integral.

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar

su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Durante el desarrollo de un sistema de información, se pueden identificar dos tipos de actividades diferenciadas:

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

8.1 Inicialización de los procesos

Hay varias razones que pueden llevar a plantear el desarrollo de un nuevo sistema de información o la modificación de uno ya existente:

Nuevos servicios y/o datos.

- Requiere el desarrollo de un nuevo sistema o la modificación de un sistema ya operativo. Puede implicar la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de desarrollo, actuando el responsable de seguridad como subsidiario.

Evolución tecnológica. Las tecnologías TIC se encuentran en evolución continua, pudiendo presentarse cambios en las técnicas de desarrollo de sistemas, en los lenguajes o las plataformas de desarrollo, en las plataformas de explotación, en los servicios de explotación, en los servicios de comunicaciones, etc.

- Requiere el desarrollo de un nuevo sistema o la modificación de un sistema ya operativo. Puede implicar la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de desarrollo, actuando el responsable de seguridad como subsidiario.

Modificación de la calificación de seguridad de servicios o datos.

- Típicamente requiere la modificación de un sistema ya operativo. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

Consideración de nuevas amenazas. La evolución de las tecnologías y los servicios de comunicaciones pueden habilitar nuevas amenazas o convertir amenazas que eran despreciables en el pasado en amenazas relevantes en el futuro.

- Típicamente requiere la modificación del sistema, bien en sus componentes o, más frecuentemente, en sus condiciones de explotación. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

Modificación de los criterios de calificación de riesgos. Puede venir inducido por criterios de calidad operativa, por novedades en la legislación aplicable, en la reglamentación sectorial o por acuerdos o contratos con terceros.

- Típicamente requiere la modificación del sistema. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

8.2 SSI – Seguridad del sistema de información

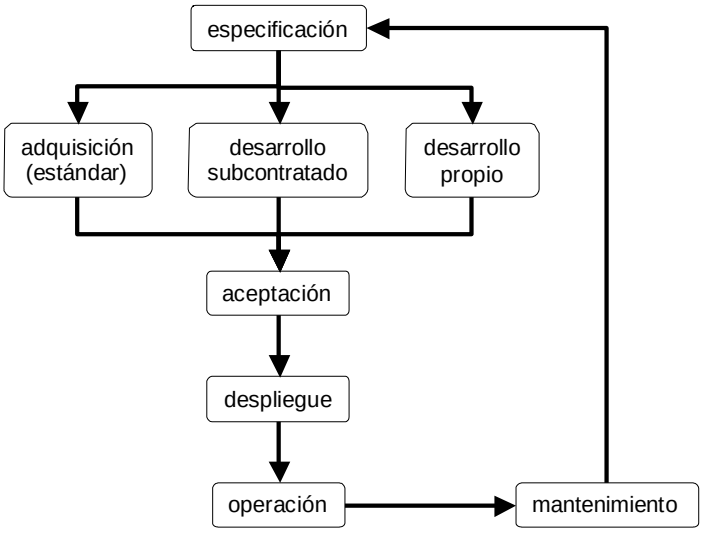
Toda la existencia de un sistema de información puede verse como etapas de concreción creciente, desde una perspectiva muy global durante los procesos de planificación hasta una visión en detalle durante el desarrollo y explotación. No obstante, este ciclo de vida no es lineal, sino que frecuentemente habrá que tantear opciones alternativas y revisar decisiones tomadas.

El análisis de riesgos debe basar sus estimaciones de impacto y riesgo en la realidad de los sistemas, concretada en sus activos. En consecuencia, se puede entender el modelo de valor como evolutivo, recogiendo en cada momento el nivel de detalle de que se dispone, estableciéndose como metodología, permite un tratamiento sistemático y homogéneo que es esencial para poder comparar opciones alternativas y para gestionar la evolución de los sistemas.

Como principio básico debe considerarse que el análisis de los riesgos debe seguir fielmente la realidad del sistema de información y su contexto, facilitando el mejor análisis de riesgos posible para poder tomar decisiones de tratamiento adecuadas a cada momento.

8.2.1 Ciclo de vida de las aplicaciones

Típicamente, una aplicación sigue un ciclo de vida a través de varias fases:



Ciclo de vida de las aplicaciones

Especificación. En esta fase se determinan los requisitos que debe satisfacer la aplicación y se elabora un plan para las siguientes fases.

Adquisición o desarrollo. Para traducir una especificación en una realidad, se puede adquirir un producto, o se puede desarrollar, bien en casa, bien por subcontratación externa.

Aceptación. Tanto si es una aplicación nueva como si es modificación de una aplicación anterior, nunca una aplicación debe entrar en operación sin haber sido formalmente aceptada.

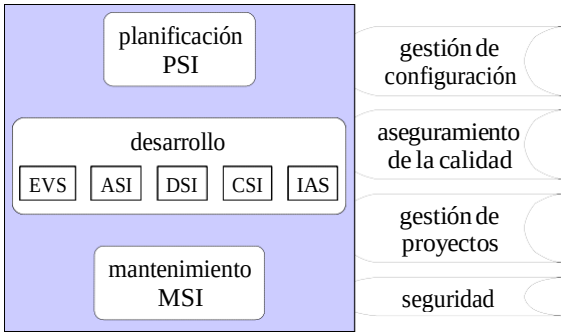
Despliegue. Consistente en instalar el código en el sistema y configurarlo para que entre en operación.

Operación. La aplicación se usa por parte de los usuarios, siendo atendidos los incidentes por parte de usuarios y/o los operadores.

Mantenimiento. Bien porque aparecen nuevos requisitos, bien porque se ha detectado un fallo, la aplicación puede requerir un mantenimiento que obligue a regresar a cualquiera de las etapas anteriores, en última instancia a la especificación básica.

MÉTRICA versión 3

La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento para la sistematización de las actividades que dan soporte al ciclo de vida del *software*. MÉTRICA versión 3 identifica los siguientes elementos:



Métrica 3 - Actividades

Métrica 3

especificación	PSI – Planificación del sistema de información EVS – Estudio de viabilidad del sistema ASI – Análisis del sistema de información
adquisición o desarrollo	DSI – Diseño del sistema de información. CSI – Construcción del sistema de información
aceptación	IAS – Implantación y aceptación del sistema
despliegue	
operación	
mantenimiento	MSI – Mantenimiento del sistema de información

Ciclo de vida y actividades en Métrica 3

8.2.2 Contexto

Se debe determinar el contexto general:

- política de seguridad y normas
- requisitos de cumplimiento normativo
- obligaciones contractuales
- roles y funciones
- criterios de valoración de información y servicios
- criterios de valoración de riesgos
- criterios de aceptación de riesgos

En particular, hay que establecer unos procedimientos operativos que instrumenten la comunicación entre las tareas de desarrollo y las tareas de análisis y tratamiento de riesgos.

- La Dirección aporta los servicios necesarios y la calidad de la seguridad deseada.
- El equipo de desarrollo aporta los elementos técnicos que materializan la aplicación.

- El equipo de análisis de riesgos aporta un juicio crítico sobre la seguridad del sistema.
- La misma Dirección aprueba el riesgo residual.

8.2.3 Fase de especificación: adquisición de datos

Se debe recopilar información sobre

- la información esencial y sus requisitos de seguridad
- los servicios esenciales y sus requisitos de seguridad
- el contexto en el que se va a desarrollar y explotar el sistema

En particular se debe establecer un perfil de amenazas, sean naturales, del entorno o de origen humano, sean accidentales o deliberadas. La caracterización del potencial del atacante debe formar parte de las especificaciones del diseño y su modificación más adelante en el ciclo de vida del sistema será objeto de un nuevo análisis y decisión de tratamiento.

8.2.4 Fase de diseño: estudio de opciones

La toma de decisiones de tratamiento de los riesgos puede recomendar salvaguardas evaluando su efecto en los indicadores de impacto y riesgo. Las decisiones que se adopten dependerán de los criterios establecidos en la política de seguridad de la Organización y de otras consideraciones específicas de cada caso. Si bien la política de seguridad establece un marco de referencia que no puede violentarse, es habitual que no prevea todos los detalles técnicos y coyunturales del servicio para tomar decisiones precisas.

Debido a la interrelación entre los elementos que constituyen un sistema, no es suficiente proteger un cierto tipo de activos para proteger el conjunto. Por ello, la toma de decisiones de tratamiento es local sobre una parte del sistema, pero siempre con un análisis global sobre la seguridad del conjunto.

Análisis y tratamiento de los riesgos

La seguridad requerida para la información que se maneja y los servicios que se prestan quedó fijada en la fase de especificación y no se puede modificar ahora.

El equipo de desarrollo y el equipo de análisis de riesgos trabajan de forma iterativa hasta encontrar una solución que satisfaga a ambas partes. Normalmente la iniciativa la toma el equipo de desarrollo proponiendo una solución técnica que responda a los requisitos funcionales del sistema. El equipo de seguridad analiza la propuesta informando de los riesgos asociados y, en su caso, proponiendo salvaguardas que pudieran dejar el riesgo en niveles aceptables. En la medida en que las salvaguardas propuestas afecten al diseño, el equipo rehará su propuesta para un nuevo análisis.

La especificación de salvaguardas debe incorporar tanto los mecanismos de actuación como los mecanismos de configuración, monitorización y control de su eficacia y eficiencia. Es frecuente que aparezcan algunos desarrollos específicamente destinados a configurar el conjunto de salvaguardas y a monitorizar su operación.

Es posible que el equipo de desarrollo pueda presentar dos o más opciones, en cuyo todas ellas serán evaluadas en lo que respecta a riesgo y salvaguardas requeridas. El informe de riesgos será un elemento más de decisión entre las diferentes opciones.

Cuando ambos equipos lleguen a una situación estable, con un diseño técnicamente viable, con un riesgo aceptable y unos requisitos aceptables de recursos, la propuesta se eleva para su aprobación.

Como resultado de esta fase, dispondremos de especificaciones técnicas de desarrollo acompañadas de un análisis de los riesgos y sus decisiones de tratamiento.

8.2.5 Soporte al desarrollo: puntos críticos

Durante el desarrollo hay que incorporar las salvaguardas aprobadas en la fase de diseño, así como controles que permitan monitorizar su eficacia. Estos requisitos de monitorización se suelen concretar en los siguientes aspectos:

- registros de actividad
- mecanismos para procesar estos registros e informar de la efectividad del sistema de protección
- disparo de alarmas cuando los hecho evidencian un problema de seguridad

El despliegue de estos elementos viene modulado por el nivel de riesgo potencial que se soporta en cada componente del sistema de información.

Durante el desarrollo conviene gestionar los riesgos según se indica en la sección relativa a "Seguridad del Proceso de Desarrollo" más adelante.

8.2.6 Aceptación y puesta en marcha: puntos críticos

Cuando el sistema se prueba antes de ponerlo en funcionamiento, debe revisarse que todos los registros de actividad funcionan correctamente, así como los sistemas de procesamiento y de alarma incorporados al sistema.

También debe comprobarse que el sistema responde al diseño previsto, concretamente que las salvaguardas están desplegadas, que su despliegue es efectivo y que no existen formas de circunvalarlas u obviarlas: es decir que el sistema no permite puertas traseras fuera de control.

Sistema(s) de identificación y autenticación:

— todo acceso al sistema requiere que el usuario se identifique y se autentique según lo previsto, bloqueando cualquier otra forma de acceso

— los mecanismos de identificación y autenticación están protegidos para evitar que un atacante pueda acceder a información o mecanismos que pongan en peligro su efectividad

Sistema(s) de control de acceso:

— todo acceso a la información y a los servicios verifica previamente que el usuario tiene las autorizaciones pertinentes

Servicios externalizados: cuando parte de la operación del sistema está delegada en un tercero:

— hay que revisar los contratos de prestación del servicio

— hay que revisar la completitud de los procedimientos de reporte y gestión de incidencias

Si el sistema no refleja el modelo cuyos riesgos han sido analizados, será rechazado sin pasar a producción.

Hay que verificar que la documentación de seguridad es clara y precisa. Esto incluye normativa, procedimientos operacionales, material de concienciación y de formación.

Sin poder ser exhaustivos, las siguientes líneas muestran pruebas de aceptación que conviene realizar:

— datos de prueba
  - si no son reales, deben ser realistas
  - si no se puede evitar que sean reales, hay que controlar copias y acceso

— pruebas funcionales (de los servicios de seguridad)
  - simulación de ataques: verificando que se detectan y reportan
  - pruebas en carga: verificando que no se obvian las medidas de protección
  - intrusión controlada (*hacking* ético)

— inspección de servicios / inspección de código
    - fugas de información: canales encubiertos, a través de los registros, etc.
    - puertas traseras de acceso
    - escalado de privilegios
    - problemas de desbordamiento de registros *(buffer overflow)*

8.2.7 Operación: análisis y gestión dinámicos

Durante la vida operativa del sistema podemos encontrarnos con cambios en el escenario que invalidan el análisis de riesgos realizado anteriormente. En entornos formales, el sistema requiere una re-acreditación para seguir operando bajo las nuevas condiciones.

Nuevas amenazas

Bien porque se descubren nuevas formas de ataque, bien porque la valoración de la capacidad del atacante se modifica. En estos casos hay que rehacer el análisis y decidir cómo tratar los nuevos resultados.

Vulnerabilidades sobrevenidas

Por ejemplo, defectos reportados por los fabricantes. En estos casos hay que analizar la nueva situación de riesgo y determinar cuál es su tratamiento adecuado para seguir operando. Lo ideal es parchear el sistema; pero bien porque el parche no existe o porque su aplicación requiere unos recursos de los que no disponemos, podemos encontrarnos en una situación nueva ante la cual hay que decidir cómo tratar el riesgo.

Incidentes de seguridad

Los incidentes de seguridad pueden indicarnos un fallo en nuestra identificación de amenazas o en su valoración, obligando a revisar el análisis.

Un incidente de seguridad también puede suponer un cambio en el sistema. Por ejemplo, una intrusión significa que no podemos contar con la defensa perimetral: tenemos un nuevo sistema, con el atacante en un nuevo lugar y con unas opciones nuevas.

Cambios en la utilización del sistema

A veces un sistema ya operacional no se utiliza como estaba previsto:

— nueva información con diferentes requisitos de seguridad

— nuevos servicios con diferentes requisitos de seguridad

— nuevos procedimientos operativos

En términos del análisis de riesgos, esto significa una diferente valoración de los activos o de las salvaguardas desplegadas.

Es posible que la alteración del sistema en alguna de las facetas contempladas en los puntos anteriores lleve a unos niveles de riesgo que no sean aceptables, obligando a un ciclo de mantenimiento que rediseñe el sistema o parte de él.

8.2.8 Ciclos de mantenimiento: análisis marginal

Cuando se propone una modificación del sistema, los nuevos elementos deben llevar a un nuevo análisis de riesgos, regresando a los ciclos iterativos de propuestas y soluciones de la fase de diseño.

8.2.9 Terminación

Cuando un sistema de información se retira del servicio, hay que realizar una serie de tareas de

seguridad proporcionadas al riesgo al que están sometidos los componentes del sistema a retirar. En concreto:

- proteger el valor de la información manejada: retención y control de acceso
- proteger las claves criptográficas de cifra y de autenticación: retención y control de acceso

Todo lo que no sea necesario retener se destruirá de forma segura:

- datos operacionales
- copias de seguridad
- configuración de los sistemas

8.2.10 Documentación de seguridad

La documentación de seguridad evoluciona con el ciclo de vida del sistema:

fase	documentación de seguridad
contexto	se revisa la política de seguridad se revisa la normativa de seguridad
especificación	se amplía la normativa de seguridad
diseño	se prepara el índice de procedimientos operacionales de seguridad
desarrollo	se elaboran los procedimientos operacionales de seguridad
aceptación y puesta en operación	se validan los procedimientos operacionales de seguridad
operación	se actualizan los procedimientos operacionales de seguridad
mantenimiento	se actualizan los procedimientos operacionales de seguridad

Documentación de seguridad a lo largo del ciclo de vida de las aplicaciones

8.3 SPD – Seguridad del proceso de desarrollo

Lo que se comenta en esta sección afecta a todas y cada uno de los procesos y subprocesos que se lleven a cabo y que utilicemos Métricas.

La interfaz de seguridad de Métrica identifica hasta 4 tareas que se repiten en cada proceso. Aquí se tratan de forma compacta:

Activos a considerar

En cada proceso se requiere un análisis de riesgos específico que contemple:

- los datos que se manejan:
  - especificaciones y documentación de los sistemas
  - código fuente
  - manuales del operador y del usuario
  - datos de prueba
- el entorno *software* de desarrollo:
  - herramientas de tratamiento de la documentación: generación, publicación, control de documentación, etc.
  - herramientas de tratamiento del código: generación, compilación, control de versiones, etc.

- el entorno *hardware* de desarrollo: equipos centrales, puestos de trabajo, equipos de archivo, etc.
- el entorno de comunicaciones de desarrollo
- las instalaciones
- el personal involucrado: desarrolladores, personal de mantenimiento y usuarios (de pruebas)

Actividades

Se siguen los siguientes pasos

1. el equipo de desarrollo expone a través del jefe de proyecto los elementos involucrados
2. el equipo de análisis de riesgos recibe a través del director de seguridad la información de los activos involucrados
3. el equipo de análisis de riesgos realiza el análisis
4. el equipo de análisis de riesgos expone a través de su director el estado de riesgo, proponiendo una serie de medidas a tomar
5. el equipo de desarrollo elabora un informe del coste que supondrían las medidas recomendadas, incluyendo costes de desarrollo y desviaciones en los plazos de entrega
6. la dirección califica el riesgo y decide las salvaguardas a implantar oyendo el informe conjunto de análisis de riesgos y coste de las soluciones propuestas
7. el equipo de análisis de riesgos elabora los informes correspondientes a las soluciones adoptadas
8. el equipo de seguridad elabora la normativa de seguridad pertinente
9. la dirección aprueba el plan para ejecutar el proceso con la seguridad requerida

8.4 Referencia (Resultados del análisis y gestión de riesgos)

En todos los casos

- salvaguardas recomendadas
- normas y procedimientos de tratamiento de la información

Otras consideraciones

Aunque cada proceso requiere su análisis de riesgos específico, es cierto que se trata de modelos tremendamente similares por lo que el mayor esfuerzo lo llevará el primero que se haga, siendo los demás adaptaciones de aquel primero.

En los primeros procesos, notablemente en PSI, pueden aparecer contribuciones de alto nivel que afecten a la normativa de seguridad de la Organización e incluso a la propia política de seguridad corporativa.

Entre las normas y procedimientos generados es de destacar la necesidad de una normativa de clasificación de la documentación y procedimientos para su tratamiento.

En todos los procesos hay que prestar una especial atención al personal involucrado. Como reglas básicas conviene:

- identificar los roles y las personas
- determinar los requisitos de seguridad de cada puesto e incorporarlos a los criterios de selección y condiciones de contratación
- limitar el acceso a la información: sólo por necesidad
- segregar tareas; en particular evitar la concentración en una sola persona de aquellas aplicaciones o partes de una aplicación que soporten un alto riesgo