ANALISIS DE RIESGOS EN SISTEMAS

Unidad 6: Proyecto de análisis de riesgos

Objetivo específico 6: El alumno aprenderá como evaluar e interpretar los roles y funciones del proceso de gestión de riesgos, conocerá las actividades preliminares de estudio de oportunidad, determinara el alcance del proyecto, la planificación y lanzamiento del proyecto, conocera como elaborar el análisis de riesgos tomando en cuenta la comunicación de resultado y aprenderá a llevar a cabo un control de proyectos.

Conceptos a desarrollar en la unidad: Roles y funciones, Actividades preliminares, Estudio de oportunidad, Determinación del alcance del proyecto, Planificación del proyecto, Lanzamiento del proyecto, Elaboración del análisis de riesgos, Comunicación de resultados, Control del proyecto, Hitos de control, Documentación resultante

Introducción

Las actividades de análisis de riesgo son recurrentes dentro del proceso de gestión, ya que hay que estar continuamente revisando el análisis y manteniéndolo al día. Podemos llamar 'análisis de riesgos marginales' a las salidas de estas actividades que, generalmente, requieren poco volumen de trabajo en cada iteración.

Pero antes de pasar a las iteraciones marginales, hay que disponer de un análisis de riesgos que sirva de plataforma de trabajo. Esto ocurre la primera vez que se realiza un análisis de riesgos y cuando la política de la organización marque que se prepare una nueva plataforma, sea por razones formales o porque los cambios acumulados justifican una revisión completa.

Cuando se realiza un análisis de riesgos partiendo de cero, se consumen una serie de recursos apreciables y conviene planificar estas actividades dentro de un proyecto, sea interno o se subcontrate a una consultora externa.

En esta sección se presentan las consideraciones que se deben tener en cuenta para que este proyecto llegue a buen término.

PAR.1 – Actividades preliminares

PAR.2 – Elaboración del análisis de riesgos

PAR.3 – Comunicación de resultados

6.1 Roles y funciones

Durante la ejecución del proyecto es frecuente que se creen algunos roles específicos para llevar el proyecto a buen fin.

Comité de Seguimiento

Está constituido por los responsables de las unidades afectadas por el proyecto; así como por los responsables de la informática y de la gestión dentro de dichas unidades. También será importante la participación de los servicios comunes de la Organización (planificación, presupuesto, recursos humanos, administración, etc.) En cualquier caso la composición del comité depende de las características de las unidades afectadas.

Las responsabilidades de este comité consisten en

- resolver las incidencias durante el desarrollo del proyecto
- asegurar la disponibilidad de recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración
- aprobar los informes intermedios y finales de cada proceso
- elaborar los informes finales para el comité de dirección

Este comité se suele nombrar por el Comité de Seguridad de la Información, y dicho comité

reporta el avance del proyecto. A veces el Comité de Seguimiento toma la forma de subcomité del Comité de Seguridad de la Información.

Equipo de proyecto

Formado por personal experto en tecnologías y sistemas de información y personal técnico cualificado del dominio afectado, con conocimientos de gestión de seguridad en general y de la aplicación de la metodología de análisis y gestión de riesgos en particular. Si el proyecto se hace con asistencia técnica mediante contratación externa, el subsiguiente personal especialista en seguridad de sistemas de información se integrará en este equipo de proyecto.

Las responsabilidades de este equipo consisten en

- llevar a cabo las tareas del proyecto
- recopilar, procesar y consolidar datos
- elaborar los informes

El Equipo de Proyecto reporta al Comité de Seguimiento a través del Director del Proyecto.

Grupos de Interlocutores

Está formado por usuarios representativos dentro de las unidades afectadas por el proyecto.

Lo constituyen varios posibles subgrupos:

- Responsables de servicio, conscientes de la misión de la Organización y sus estrategias a medio y largo plazo
- Responsables de servicios internos
- Personal de explotación y operación de los servicios informáticos, conscientes de los medios desplegados (de producción y salvaguardas) y de las incidencias habituales

Además de dichos órganos colegiados, hay que identificar algunos roles singulares:

Promotor

Es una figura singular que lidera las primeras tareas del proyecto, perfilando su oportunidad y alcance para lanzar el proyecto de análisis de riesgos propiamente dicho.

Debe ser una persona con visión global de los sistemas de información y su papel en las actividades de la Organización, sin necesidad de conocer los detalles; pero si al tanto de las incidencias.

Director del Proyecto

Debe ser un directivo de alto nivel, con responsabilidades en seguridad dentro de la Organización, de sistemas de información o, en su defecto, de planificación, de coordinación o de materias, servicios o áreas semejantes.

Es la cabeza visible del equipo de proyecto e interlocutor con el Responsable de la Seguridad de la Organización..

Enlace operacional

Será una persona de la Organización con buen conocimiento de las personas y de las unidades implicadas en el proyecto, que tenga capacidad para conectar al equipo de proyecto con el grupo de usuarios.

Es el interlocutor visible del comité de seguimiento con los grupos de usuarios.

Conviene recordar que un proyecto de análisis de riesgos siempre es mixto por su propia

naturaleza; es decir, requiere la colaboración permanente de especialistas y usuarios tanto en las fases preparatorias como en su desarrollo. La figura del enlace operacional adquiere una relevancia permanente que no es habitual en otro tipo de proyectos más técnicos.

El proyecto de análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

PAR – Proyecto de Análisis de Riesgos
PAR.1 – Actividades preliminares
PAR.11 – Estudio de oportunidad
PAR.12 – Determinación del alcance del proyecto
PAR.13 – Planificación del proyecto
PAR.14 – Lanzamiento del proyecto
PAR.2 – Elaboración del análisis de riesgos
PAR.3 – Comunicación de resultados

6.2 Actividades preliminares

6.2.1 Estudio de oportunidad

Se fundamenta la oportunidad de la realización, ahora, del proyecto de análisis de riesgos, enmarcándolo en el desarrollo de las demás actividades de la Organización.

El resultado de esta actividad es el informe denominado “preliminar”.

6.2.2 Determinación del alcance del proyecto

Se definen los objetivos finales del proyecto, su dominio y sus límites.

El resultado de esta actividad es un perfil de proyecto de análisis de riesgos.

6.2.3 Planificación del proyecto

Se determinan las cargas de trabajo que supone la realización del proyecto. Normalmente la evolución del proyecto viene marcada por una serie de entrevistas con los interlocutores que conocen la información relativa a algún activo o grupo de activos del sistema bajo análisis. Se planifican las entrevistas que se van a realizar para la recogida de información: quiénes van a ser entrevistados. Se elabora el plan de trabajo para la realización del proyecto.

En esta actividad se determinan los participantes y se estructuran los diferentes grupos y comités para llevar a cabo el proyecto.

El resultado de esta actividad está constituido por:

- un plan de trabajo para el proyecto
- procedimientos de trabajo

6.2.4 Lanzamiento del proyecto

Se adaptan los cuestionarios para la recogida de información adaptándolos al proyecto presente. Para ello se parte de los criterios establecidos dentro del Proceso de Gestión de Riesgos.

También se realiza una campaña informativa de sensibilización a los afectados sobre las finalidades y requerimientos de su participación.

El resultado de esta actividad está constituido por:

- los cuestionarios para las entrevistas
- el catálogo de tipos de activos

- la relación de dimensiones de seguridad y
- los criterios de valoración

Estudio de oportunidad

PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.11: Determinar la oportunidad***
Objetivos • Identificar o suscitar el interés de la Dirección de la Organización en la realización de un proyecto de análisis de riesgos
Productos de entrada

PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.11: Determinar la oportunidad***
Productos de salida • **Informe preliminar** recomendando la elaboración del proyecto • Sensibilización y apoyo de la Dirección a la realización del proyecto • Creación del comité de seguimiento
Técnicas, prácticas y pautas •
Participantes • El promotor

La Dirección suele ser muy consciente de las ventajas que aportan las técnicas electrónicas, informáticas y telemáticas a su funcionamiento; pero no tanto de los nuevos problemas de seguridad que estas técnicas implican, o de las obligaciones legales o reglamentarias que les afectan

En toda Organización pública o privada es importante transformar en medidas concretas la creciente preocupación por la falta de seguridad de los sistemas de información, por su soporte y en- torno, puesto que sus efectos no sólo afectan a dichos sistemas, sino al propio funcionamiento de la Organización y, en las situaciones críticas, a su propia misión y capacidad de supervivencia.

Desarrollo

La iniciativa para la realización de un proyecto de análisis de riesgos parte de un promotor interno o externo a la Organización, consciente de los problemas relacionados con la seguridad de los sistemas de información, como por ejemplo:

- Incidentes continuados relacionados con la seguridad.
- Inexistencia de previsiones en cuestiones relacionadas con la evaluación de necesidades y medios para alcanzar un nivel aceptable de seguridad de los sistemas de información que sea compatible con el cumplimiento correcto de la misión y funciones de la Organización.
- Reestructuraciones en los productos o servicios proporcionados.
- Cambios en la tecnología utilizada.

- Desarrollo de nuevos sistemas de información.

El promotor puede elaborar un **cuestionario-marco** (documento poco sistematizable que deberá crear en cada caso concreto) para provocar la reflexión sobre aspectos de la seguridad de los sistemas de información por parte de :

Los responsables de las unidades operativas (responsables de servicios).

El cuestionario permite proceder a un examen informal de la situación en cuanto a la seguridad de sus sistemas de información; deben poder expresar su opinión por los proyectos de seguridad ya realizados (con su grado de satisfacción o con las limitaciones de éstos), así como sus expectativas ante la elaboración de un proyecto de análisis de riesgos. Esta aproximación de alto nivel permite obtener una primera visión de los objetivos concretos y las opciones que tendrían que subyacer a la elaboración del proyecto.

Los responsables de informática.

El cuestionario permite obtener una panorámica técnica para la elaboración del proyecto y posibilita abordar el estudio de oportunidad de realización, tras integrar las opciones anteriores.

De las respuestas al cuestionario-marco y de las entrevistas mantenidas con los responsables y colectivos anteriores, el promotor obtiene una primera aproximación sobre las funciones, los servicios y los productos implicados en cuestiones de seguridad de los sistemas de información, la ubicación geográfica de aquéllos, los medios técnicos, los medios humanos, etc.

Con estos elementos el promotor realiza el **informe preliminar** recomendando la elaboración del proyecto de análisis de riesgos e incluyendo estos elementos:

- Exposición de los argumentos básicos.
- Relación de antecedentes sobre la seguridad de los sistemas de información (Plan Estratégico, Plan de Actuación, etc.).
- Primera aproximación al dominio a incluir en el proyecto en función de
  - las finalidades de las unidades o departamentos
  - las orientaciones gerenciales y técnicas
  - la estructura de la Organización
  - el entorno técnico.
- Primera aproximación de los medios, tanto humanos como materiales, para la realización del proyecto.

El promotor presenta este informe preliminar a la Dirección que puede decidir:

- aprobar el proyecto, o bien
- modificar su dominio y/o sus objetivos, o bien
- retrasar el proyecto.

Tarea PAR.12: Determinación del alcance del proyecto

Una vez que se ha constatado la oportunidad de realizar el proyecto y se cuenta con el apoyo de la Dirección, esta actividad estima los elementos de planificación del proyecto, es decir los participantes y sus cargas de trabajo.

En dicha estimación se ha de tener en cuenta la posible existencia de otros planes (por ejemplo un Plan Estratégico de Sistemas de Información o de Seguridad general en las unidades que pueden ser afectadas o en la Organización) y el plazo de tiempo considerado para la puesta en práctica del proyecto. En particular, la existencia de un Plan Estratégico de Sistemas de Información para las unidades que pueden ser afectadas dentro de la Organización puede determinar en gran medida el alcance y la extensión de las actividades que se realicen en esta actividad.

PAR: Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.12: Determinación del alcance del proyecto

Objetivos

- Determinar los objetivos del proyecto, diferenciados según horizontes temporales a corto y medio plazo
- Determinar las restricciones generales que se imponen sobre el proyecto
- Determinar el dominio, alcance o perímetro del proyecto

PAR: Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.12: Determinación del alcance del proyecto

Productos de entrada

- Recopilación de la documentación pertinente de la Organización

Productos de salida

- Especificación detallada de los objetivos del proyecto
- Relación de restricciones generales
- Relación de unidades de la Organización que se verán afectadas como parte del proyecto
- Lista de roles relevantes en la unidades incluidas en el alcance del proyecto
- los activos esenciales
- los puntos de interconexión con otros sistemas
- los proveedores externos

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- *31010:B.1: Brainstorming*
- *31010:B.2: Structured or semi-structured interviews*
- *31010:B.3: Delphi technique*

Participantes

- El comité de seguimiento

Un proyecto de análisis de riesgos puede perseguir objetivos a muy corto plazo tales como el aseguramiento de cierto sistema o un cierto proceso de negocio, o puede pretender objetivos más amplios como fuera el análisis global de la seguridad de la Organización. En todo caso, hay que determinarlo.

Especialmente a la hora de tomar acciones correctoras, hay que tener en cuenta que “no todo vale”, sino que el proyecto se encontrará con una serie de restricciones, no necesariamente técnicas, que establecen un marco al que atenerse. Para incorporar las restricciones al análisis y ges- tión de riesgos, estas se agrupan por distintos conceptos, típicamente:

Restricciones políticas o gerenciales

Típicas de organizaciones gubernamentales o fuertemente relacionadas con organismos gubernamentales, bien como proveedores o como suministradores de servicios.

Restricciones estratégicas

Derivadas de la evolución prevista de la estructura u objetivos de la Organización.

Restricciones geográficas

Derivadas de la ubicación física de la Organización o de su dependencia de medios físicos de comunicaciones. Islas, emplazamientos fuera de las fronteras, etc.

Restricciones temporales

Que toman en consideración situaciones coyunturales: conflictividad laboral, crisis internacional, cambio de la propiedad, reingeniería de procesos, etc.

Restricciones estructurales

Tomando en consideración la organización interna: procedimientos de toma de decisiones, dependencia de casas matrices internacionales, etc.

Restricciones funcionales

Que tienen en cuenta los objetivos de la Organización.

Restricciones legales

Leyes, reglamentos, regulaciones sectoriales, contratos externos e internos, etc.

Restricciones relacionadas con el personal

Perfiles laborales, compromisos contractuales, compromisos sindicales, carreras profesionales, etc.

Restricciones metodológicas

Derivadas de la naturaleza de la organización y sus hábitos o habilidades de trabajo que pueden imponer una cierta forma de hacer las cosas.

Restricciones culturales

La “cultura” o forma interna de trabajar puede ser incompatible con ciertas salvaguardas teóricamente ideales.

Restricciones presupuestarias

La cantidad de dinero es importante; pero también la forma de planificar el gasto y de ejecutar el presupuesto

Alcance

Esta tarea identifica las unidades objeto del proyecto y especifica las características generales de dichas unidades en cuanto a responsables, servicios proporcionados y ubicaciones geográficas. También identifica las principales relaciones de las unidades objeto del proyecto con otras entidades, por ejemplo el intercambio de información en diversos soportes, el acceso a medios informáticos comunes, etc.

La tarea presume un principio básico: el análisis y la gestión de riesgos debe centrarse en un dominio limitado, que puede incluir varias unidades o mantenerse dentro de una sola unidad (según la complejidad y el tipo de problema a tratar), ya que un proyecto de ámbito demasiado amplio o indeterminado podría ser inabarcable, por excesivamente generalista o por demasiado extendido en el tiempo, con perjuicio en las estimaciones de los elementos del análisis.

Para que el alcance quede determinado debemos concretar:

— **los activos esenciales**: información que se maneja y servicios que se prestan

— **los puntos de intercambio** de interconexión con otros sistemas, aclarando qué información se intercambia y qué servicios se prestan mutuamente

— **los proveedores externos** en los que se apoya nuestro sistema de información

6.2.3 Planificación del proyecto

Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.13: Planificación del proyecto

Objetivos

- Definir los grupos de interlocutores: usuarios afectados en cada unidad
- Planificar las entrevistas de recogida de información
- Determinar el volumen de recursos necesarios para la ejecución del proyecto: humanos, temporales y financieros
- Elaborar el calendario concreto de realización de las distintas etapas, actividades y tareas del proyecto
- Establecer un calendario de seguimiento que defina las fechas tentativas de reuniones del comité de dirección, el plan de entregas de los productos del proyecto, las posibles modificaciones en los objetivos marcados, etc

Productos de entrada

- Resultados de la actividad A1.2, Determinación del alcance del proyecto

Productos de salida

- Relación de participantes en los grupos de interlocutores
- Plan de entrevistas
- Informe de recursos necesarios
- Informe de cargas

Técnicas, prácticas y pautas

- Planificación de proyectos

Participantes

- El director de proyecto
- El comité de seguimiento

El plan de entrevistas debe detallar a qué persona se va a entrevistar, cuándo y con qué objetivo. Este plan permite determinar la carga que el proyecto va a suponer para las unidades afectadas, bien del dominio, bien del entorno.

El plan de entrevistas es especialmente importante cuando los sujetos a entrevistar se hayan en diferentes localizaciones geográficas y la entrevista requiere el desplazamiento de una o ambas partes.

También conviene ordenar las entrevistas de forma que primero se recaben las opiniones más técnicas y posteriormente las gerenciales, de forma que el entrevistador pueda evolucionar las preguntas tomando en consideración hechos (experiencia histórica) antes que valoraciones y perspectivas de servicio a terceros.

6.2.4 Lanzamiento del proyecto

Esta actividad completa las tareas preparatorias del lanzamiento del proyecto: empezando por seleccionar y adaptar los cuestionarios que se utilizarán en la recogida de datos y por realizar la campaña informativa de sensibilización a los implicados.

Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.14: Lanzamiento del proyecto

Objetivos

- Disponer de los elementos de trabajo para acometer el proyecto

Productos de entrada

- Marco de trabajo establecido en el Proceso de Gestión de Riesgos: criterios y relaciones con las partes afectadas

Productos de salida

- Cuestionarios adaptados
- Determinar el catálogo de tipos de activos
- Determinar las dimensiones de valoración de activos
- Determinar los niveles de valoración de activos, incluyendo una guía unificada de criterios para asignar un cierto nivel a un cierto activo
- Determinar los niveles de valoración de las amenazas: frecuencia y degradación
- Asignar los recursos necesarios (humanos, de organización, técnicos, etc.) para la realización del proyecto
- Informar a las unidades afectadas
- Crear un ambiente de conocimiento general de los objetivos, responsables y plazos

Técnicas, prácticas y pautas

- Cuestionarios (ver "Catálogo de Elementos")

Participantes

- El director del proyecto
- El equipo de proyecto

La tarea adapta los cuestionarios a utilizar en la recogida de información en el proceso P1 en función de los objetivos del proyecto, del dominio y de los temas a profundizar con los usuarios.

Los cuestionarios se adaptan con el objetivo de identificar correctamente los elementos de trabajo: activos, amenazas, vulnerabilidades, impactos, salvaguardas existentes, restricciones generales, etc. en previsión de las necesidades de las actividades A2.1 (caracterización de los activos), A2.2 (caracterización de las amenazas) y A2.3 (caracterización de las salvaguardas).

La necesidad de una adaptación siempre existe pero el grado mayor o menor de adaptación depende además de las condiciones en que se realice la explotación de dichos cuestionarios. No habrá la misma profundidad de adaptación para entrevistas guiadas por el especialista en seguridad, que para cuestionarios auto administrados por el responsable del dominio o por los usuarios de sus sistemas de información.

6.3 Elaboración del análisis de riesgos

Se siguen los pasos del método descrito en el capítulo X anterior.

La mayor parte de las tareas requerirán dos o tres entrevistas con los interlocutores apropiados:

- una primera entrevista para exponer las necesidades y recabar los datos
- una segunda entrevista para validar que los datos son completos y se han entendido correctamente
- según las circunstancias puede ser necesaria alguna entrevista adicional si la validación levanta muchas inexactitudes o dudas

El todas estas tareas debe procurarse manejar documentación escrita sometida a un proceso formal de gestión; es decir, aprobada y con unos procedimientos de revisión continua. La información de carácter verbal o informal debe limitarse a facilitar la comprensión, no a transmitir elementos sustanciales que no están documentados en parte alguna.

6.4 Comunicación de resultados

La salida de la fase de análisis es la entrada de la fase de tratamiento. Para la tomar decisiones de tratamiento es necesario conocer tanto los indicadores residuales como los indicadores potenciales de impacto y riesgo. Y para cada escenario de riesgo es necesario disponer de información suficiente para poder entender en qué consiste el riesgo, así como su dinámica y los razonamientos o la base de las estimaciones empleadas para derivar resultados. No basta conocer el valor final del indicador, sino que hay que poder analizar el por qué de ese valor.

Por otra parte, las decisiones de tratamiento pueden requerir la realización de modificaciones del análisis de riesgo. Frecuentemente es necesario analizar situaciones hipotéticas (¿qué ocurriría si …?) para poder optar por una decisión u otra. Es por ello que es fundamental el soporte de herramientas que automaticen el cálculo.

Para el informe ejecutivo final basta destacar gráficamente los escenarios de mayor impacto, de mayor nivel de riesgo y combinaciones peligrosas de ambos indicadores (ver los cuadrantes o zonas más arriba).

6.5 Control del proyecto

6.5.1 Hito de control H1.1:

La Dirección procederá a la aprobación o no de la realización del proyecto de análisis de riesgos, basándose en el estudio de oportunidad realizado por el promotor.

Hito de control H1.2:

El comité de seguimiento del proyecto validará el informe de "Planificación del Proyecto de Análisis de Riesgos" que contendrá una síntesis de los productos obtenidos en las actividades realizadas en el proceso P1.

6.5.2 Documentación resultante

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Análisis de los resultados, con la detección de las áreas críticas claves.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Resultados de posibles aplicaciones de métodos de análisis y gestión de riesgos realizadas

anteriormente (por ejemplo catalogación, agrupación y valoración de activos, amenazas, vulnerabilidades, impactos, riesgo, mecanismos de salvaguarda, etc.).

Documentación final

- Modelo de valor: identificación de activos junto con sus dependencias y valoración propia y acumulada
- Mapa de amenazas junto con sus consecuencias y probabilidad de ocurrencia.
- Documento de aplicabilidad de las salvaguardas.
- Informe de valoración de la efectividad de las salvaguardas presentes.
- Informe de insuficiencias o debilidades del sistema de salvaguardas.
- Indicadores de impacto y riesgo, potenciales y residuales.