ANALISIS DE RIESGOS EN SISTEMAS

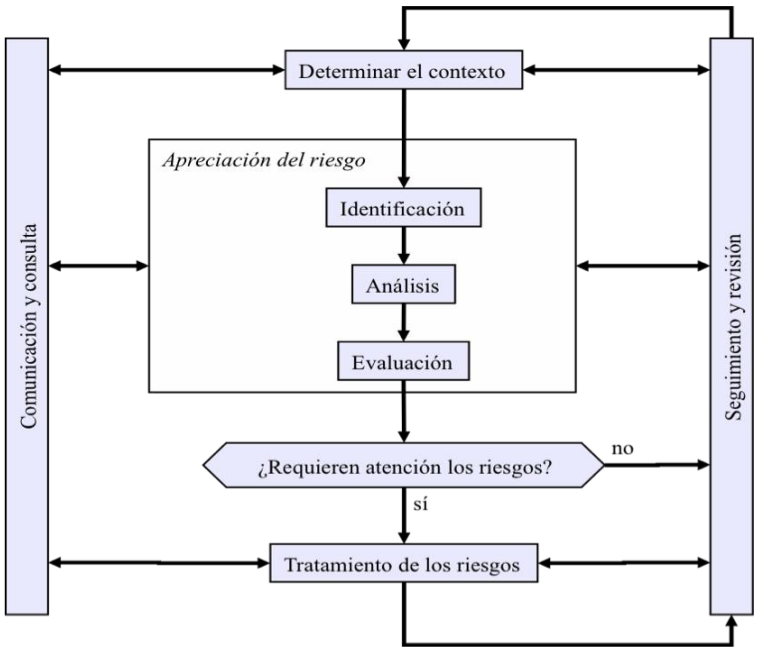
Unidad 5: Proceso de gestión de riesgos II

Objetivo específico 5: El alumno aprenderá como evaluar e interpretar los roles y funciones del proceso de gestión de riesgos, conocerá el contexto, los criterios y evaluación de riesgos, determinara el proceso de toma de decisiones en el tratamiento así como la comunicación que establecerá haciendo el seguimiento y revisión del proceso, tomando en cuenta la documentación y conocer los indicadores de control del proceso de gestión de riesgos.

Conceptos a desarrollar en la unidad: Roles y funciones, Contexto, Criterios, Evaluación de los riesgos, Decisión de tratamiento, Comunicación y consulta, Seguimiento y revisión, Documentación del proceso e Indicadores de control del proceso de gestión de riesgos

Introducción

En este tema vamos a conocer la manera de formalizar los roles y funciones que se llevan a cabo durante el proceso de la gestión de riesgos, los criterios que se llevan a cabo asi como la evaluación de los riesgos a los que nos enfrentamos, tomando decisiones y establecer el modelo de comunicación mas adecuado, el seguimiento que se debe de llevar a cabo así como la revisión y elaboración de los documentos que se llevan a cabo y de los indicadores de control de los procesos que se llevan a cabo en la gestión de riesgos



Proceso de gestión de riesgos

5.1 Roles y funciones

En el proceso de gestión de riesgos aparecen varios actores. Los siguientes párrafos intentan identificarlos de forma somera y explicitar cuales son sus funciones y responsabilidades.

Órganos de gobierno

En este epígrafe se incluyen aquellos que órganos colegiados o unipersonales que deciden la misión y los objetivos de la Organización.

Típicamente se incluyen en esta categoría los altos cargos de los organismos.

Cuando existe un Comité de Seguridad de la Información, suele aparecer en este nivel.

Estos órganos tienen la autoridad última para aceptar los riesgos con que se opera. Se dice que son los “propietarios del riesgo”.

Dirección ejecutiva

En este epígrafe se incluyen aquellos órganos colegiados o unipersonales que toman decisiones que concretan cómo alcanzar los objetivos de negocio marcados por los órganos de gobierno.

Típicamente se incluyen en esta categoría los responsables de unidades de negocio, los responsables de la calidad de los servicios prestados por la organización, etc.

Dirección operacional

En este epígrafe se incluyen aquellos órganos colegiados o unipersonales que toman decisiones prácticas para materializar las indicaciones dadas por los órganos ejecutivos.

Típicamente se incluyen en esta categoría los responsables de operaciones, de producción, de explotación y similares.

Esquema Nacional de Seguridad

En el Esquema Nacional de Seguridad de identifican ciertos roles que pueden verse involucrados en el proceso de gestión de riesgos:

Responsable de la información

Típicamente a nivel de gobierno. Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la Organización.

A este nivel se suele concretar la responsabilidad sobre datos de carácter personal y sobre la clasificación de la información.

A veces este role lo ejerce el Comité de Seguridad de la Información.

Responsable del servicio

Típicamente a nivel de gobierno, aunque a veces baja a nivel ejecutivo. Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la Organización.

A veces este role lo asume el Comité de Seguridad de la Información.

Responsable de la seguridad

Típicamente a nivel ejecutivo, actuando como engranaje entre las directrices emanadas de los responsables de la información y los servicios, y el responsable del sistema. A su vez funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información.

A veces se denomina a esta figura CISO (*Chief Information Security Officer*).

En lo que respecta al proceso de gestión de riesgos, es la persona que traslada la valoración de los activos esenciales, que aprueba la declaración de aplicabilidad de salvaguardas, los procedimientos operativos, los riesgos residuales y los planes de seguridad. En esta función de informante, suele ser la persona encargada de elaborar los indicadores del esto de seguridad del sistema.

Responsable del sistema

A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

En lo que respecta al proceso de gestión de riesgos, es la persona que propone la arquitectura de seguridad, la declaración de aplicabilidad de salvaguardas, los procedimientos operativos y los planes de seguridad. También es la persona responsable de la implantación y correcta operación de las salvaguardas.

Administradores y operadores

Son las personas encargadas de ejecutar las acciones diarias de operación del sistema

según las indicaciones recibidas de sus superiores jerárquicos.

Matriz RACI

La matriz que se expone a continuación es orientativa y cada organismo deberá adecuarla a su organización particular.

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un órgano colegiado.

	rol	descripción
R	Responsible	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	Accountable	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	Consulted	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	Informed	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Roles en procesos distribuidos

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
aceptación del riesgo residual	I	A	A	R	I	
implantación de las medidas de seguridad		I	I	C	A	R
					C	R

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad				A	C	
planes de concienciación y formación				A	C	
planes de continuidad				C	A	
seguridad en el ciclo de vida				C	A	

Matriz RACI - Tareas relacionadas con la gestión de riesgos

Siendo
Dirección – Alta Dirección, Órganos de Gobierno RINFO – Responsable de la Información
RSERV – Responsable del Servicio
RSEG – Responsable de la Seguridad

RSIS – Responsable (operacional) del Sistema

ASS – Administrador(es) de la Seguridad del Sistema

5.2 Contexto

Hay que documentar el entorno externo en el que opera la Organización: cultural, social y político. Esto incluye tanto aspectos nacionales como internacionales, viniendo marcados por el ámbito de actividad de la Organización.

Hay que identificar las obligaciones legales, reglamentarias y contractuales. Por ejemplo, suele haber obligaciones asociadas a

- tratamiento de datos de carácter personal,
- tratamiento de información clasificada,
- tratamiento de información y productos sometidos a derechos de propiedad intelectual
- prestación de servicios públicos
- operación de infraestructuras críticas
- etc.

Hay que identificar el entorno en cuanto competencia y posicionamiento respecto de la competencia.

Hay que identificar el contexto interno en el que se desenvuelve la actividad de la Organización: política interna, compromisos con los accionistas y con los trabajadores o sus representantes.

La identificación del contexto en el que se desarrolla el proceso de gestión de riesgos debe ser objeto de una revisión continua para adaptarse a las circunstancias de cada momento.

5.3 Criterios

Múltiples aspectos relacionados con los riesgos son objeto de estimaciones. Conviene que las estimaciones sean lo más objetivas que sea posible o. al menos, que sean repetibles, explicables y comparables.

En particular conviene establecer escalas de valoración para

- valorar los requisitos de seguridad de la información
- valorar los requisitos de disponibilidad de los servicios
- estimar la probabilidad de una amenaza
- estimar las consecuencias de un incidente de seguridad
- estimar el nivel de riesgo a partir de las estimaciones de impacto y probabilidad
- … (ver “Libro II – Catálogo de Elementos”)

Hay que establecer reglas y/o criterios para tomar decisiones de tratamiento:

- umbrales de impacto
- umbrales de probabilidad
- umbrales combinados de impacto y probabilidad
- umbrales de nivel de riesgo
- impacto en la reputación de la Organización o de las personas responsables
- impacto en la posición de competencia

— impacto comparado con otras áreas de riesgo: financiero, regulatorio, medioambiental, seguridad industrial, etc

— combinaciones o concurrencia de riesgos que pudieran tener un efecto combinado

— amenazas especialmente sensibles (puede ser por motivos técnicos, porque adolecen de una amplia incertidumbre o porque su ocurrencia causaría una notable alarma social con grave daño para la reputación o la continuidad de las operaciones de la Organización, incluso si sus consecuencia técnicas o materiales son modestas)

5.4 Evaluación de los riesgos

Se sigue la metodología descrita en el capítulo anterior.

La primera vez que se ejecuta esta actividad puede ser conveniente lanzar un proyecto específico de análisis de riesgos. Ver capítulo siguiente.

5.5 Decisión de tratamiento

Se pueden tomar las diferentes opciones mencionadas al principio de este capítulo.

Hay múltiples formas de reducir el riesgo:

— eliminar el riesgo eliminando sus causas: información tratada, servicios prestados, arquitectura del sistema,

— reducir o limitar el impacto

— reducir la probabilidad de que la amenaza ocurra

— en el caso de amenazas derivadas de defectos de los productos (vulnerabilidades técnicas): reparar el producto (por ejemplo, aplicar los parches del fabricante)

— implantar nuevas salvaguardas o mejorar la calidad de las presentes

— externalizar partes del sistema

— contratar seguros de cobertura

A veces la decisión consiste en aceptar un incremento del riesgo:

— aceptando trabajar con nueva información o prestar nuevos servicios

— alterando la arquitectura del sistema

— reduciendo las salvaguardas presentes

— reduciendo la calidad de las salvaguardas presentes (es decir, dedicando menos recursos)

En última instancia siempre hay que acabar aceptando un cierto riesgo residual, en cuyo caso es posible que se decide reservar fondos para hacer frente a alguna contingencia.

5.6 Comunicación y consulta

Antes de tomar ninguna decisión relativa al tratamiento de un riesgo hay que entender para qué se usa el sistema y cómo se usa.

Esto quiere decir mantener un contacto fluido con varios actores

— los órganos de gobierno y decisión, pues toda decisión debe estar alineada con la misión de la Organización

— los usuarios y técnicos de sistemas, pues toda decisión debe tener en cuenta su impacto en la productividad y sobre la usabilidad del sistema

— los proveedores, pues toda decisión debe contar con su colaboración

Hay que tener en cuenta que cualquier medida de seguridad que merme la productividad, dificulte la operación del sistema, o requiera una elaborada formación de los usuarios, está condenada al fracaso,

Toda medida de seguridad debe estar

- apoyada por la Dirección
- amparada por la Política de Seguridad de la Organización
- apoyada por normativa clara y legible, ampliamente divulgada
- explicada de forma breve, clara y directa en procedimientos operativos de seguridad

Por último es interesante disponer de indicadores que midan el grado de aceptación por parte de los usuarios, identificando tanto el grado de cumplimiento como los problemas que causa su seguimiento.

5.7 Seguimiento y revisión

El análisis de los riesgos es un ejercicio formal, basado en múltiples estimaciones y valoraciones que pueden no compadecerse con la realidad. Es absolutamente necesario que el sistema esté bajo monitorización permanente. Los indicadores de impacto y riesgo potenciales son útiles para decidir qué puntos deben ser objeto de monitorización.

Y debe estar preparado un sistema de detección precoz de posibles incidentes (en base a indicadores predictivos) así como un sistema de reacción a incidentes de seguridad.

Se procurará disponer de un conjunto de indicadores clave de riesgo (*KRI – Key Risk Indicators*). Estos indicadores:

- son propuestos por el Responsable de la Seguridad;
- su definición es acordada por el Responsable de la Seguridad y el propietario del riesgo; la definición indicará exactamente:
  - en qué medidas se basan,
  - cuál es el algoritmo de cálculo,
  - la periodicidad de evaluación y
  - los umbrales de aviso y alarma (atención urgente)
- se le presentan al responsable correspondiente
  - rutinariamente, con la periodicidad establecida,
  - puntualmente, por demanda del propietario del riesgo medido,
  - y extraordinariamente cuando se supera un umbral de riesgo
- estos indicadores estarán a disposición de los auditores

La responsabilidad de monitorizar un riesgo recae en su propietario, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

Cada vez que la realidad difiere de nuestras estimaciones conviene hacer un ciclo de revisión del análisis y las decisiones de tratamiento.

Servicios subcontratados

Cuando dependemos de terceros es especialmente importante conocer el desempeño de nuestros proveedores, tanto con un buen sistema de reporte, escalado y resolución de los incidentes de seguridad, como en el establecimiento de indicadores predictivos. Del análisis de dependencias realizado durante el análisis de riesgos, tenemos información de en qué medida y en qué dimensiones de seguridad dependemos de cada proveedor externo. De esta información se sigue qué elementos debemos monitorizar para asegurarnos que satisfacen nuestros requisitos de seguridad.

5.9 Documentación del proceso

Documentación interna

- Definición de roles, funciones y esquemas de reporte
- Criterios de valoración de la información
- Criterios de valoración de los servicios
- Criterios de evaluación de los escenarios de impacto y riesgo

Documentación para otros

- Plan de Seguridad

5.10 Indicadores de control del proceso de gestión de riesgos

√	**actividad**	**tarea**
	Se han definido los roles y responsabilidades respecto de la gestión de riesgos	4.2.1
	Se ha establecido el contexto de gestión de riesgos	4.2.2
	Se han establecido los criterios de valoración de riesgos y toma de decisiones de tratamiento	4.2.3
	Se han interpretado los riesgos residuales en términos de impacto en el negocio o misión de la Organización	4.2.4
	Se han identificado y valorado opciones de tratamiento de los riesgos residuales (propuesta de programas de seguridad)	4.2.5
	Los órganos de gobierno han adoptado una propuesta de tratamiento — evitar el riesgo — prevenir: mitigar la probabilidad de que ocurra — mitigar el impacto si ocurriera — compartir el riesgo con un tercero — asumir el riesgo	4.2.5
	Se han previsto recursos para acometer el plan de seguridad	4.2.5

√	**actividad**	**tarea**
	Se han previsto recursos para atender a contingencias	4.2.5
	Se han comunicado las decisiones a las partes afectadas	4.2.6
	Se ha desplegado un sistema de monitorización constante para detectar modificaciones en los supuestos de análisis de riesgos	4.2.7
	Se han establecido las normas y procedimientos de actuación en caso de detectar desviaciones de los supuestos	4.2.7