

Mayo 2011

TÍTULO

Gestión del riesgo

Técnicas de apreciación del riesgo

Risk management. Risk assessment techniques.

Gestion des risques. Techniques d'évaluation des risques.

CORRESPONDENCIA

Esta norma es la versión oficial, en español, de la Norma Europea EN 31010:2010 que a su vez adopta la Norma Internacional ISO/IEC 31010:2009.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el Grupo Específico de Carácter Temporal AEN/GET13 *Gestión de riesgos* cuya Secretaría desempeña AENOR.

Editada e impresa por AENOR
Depósito legal: M 19682:2011

© AENOR 2011
Reproducción prohibida

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR

Génova, 6
28004 MADRID-España

Asociación Española de
Normalización y Certificación

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

100 Páginas

Grupo 55

Versión en español

Gestión del riesgo
Técnicas de apreciación del riesgo
(IEC/ISO 31010:2009)

Risk management. Risk assessment techniques. (IEC/ISO 31010:2009).

Gestion des risques. Techniques d'évaluation des risques. (CEI/ISO 31010:2009).

Risikomanagement. Verfahren zur Risikobeurteilung. (IEC/ISO 31010:2009).

Esta norma europea ha sido aprobada por CENELEC el 2010-05-01. Los miembros de CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional.

Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales, pueden obtenerse en la Secretaría Central de CENELEC, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CENELEC en su idioma nacional, y notificada a la Secretaría Central, tiene el mismo rango que aquéllas.

Los miembros de CENELEC son los comités electrotécnicos nacionales de normalización de los países siguientes: Alemania, Austria, Bélgica, Bulgaria, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Suecia y Suiza.

CENELEC
COMITÉ EUROPEO DE NORMALIZACIÓN ELECTROTÉCNICA
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
SECRETARÍA CENTRAL: Avenue Marnix, 17-1000 Bruxelles

PRÓLOGO

El texto del documento 56/1329/FDIS, futura edición 1 de la Norma IEC/ISO 31010, preparado por el Comité Técnico IEC TC 56, *Confiabilidad*, junto con el Grupo de Trabajo ISO TMB *Gestión del riesgo*, fue sometido a voto paralelo IEC-CENELEC y fue aprobado por CENELEC como Norma EN 31010 el 2010-05-01.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN y/o CENELEC no es(son) responsable(s) de la identificación de dichos derechos de patente.

Se fijaron las siguientes fechas:

- | | | |
|---|-------|------------|
| – Fecha límite en la que la norma europea debe adoptarse a nivel nacional por publicación de una norma nacional idéntica o por ratificación | (dop) | 2011-02-01 |
| – Fecha límite en la que deben retirarse las normas nacionales divergentes con esta norma | (dow) | 2013-05-01 |

El anexo ZA ha sido añadido por CENELEC.

DECLARACIÓN

El texto de la Norma IEC/ISO 31010:2009 fue aprobado por CENELEC como norma europea sin ninguna modificación.

En la versión oficial, para la bibliografía, debe añadirse la siguiente nota para la norma indicada:

IEC 60300-3-11	NOTA	Armonizada como Norma EN 60300-3-11.
IEC 61078	NOTA	Armonizada como Norma EN 61078.
IEC 61165	NOTA	Armonizada como Norma EN 61165.
IEC 61508 serie	NOTA	Armonizada como Norma EN 61508 serie (sin ninguna modificación).
IEC 61511 serie	NOTA	Armonizada como Norma EN 61511 serie (sin ninguna modificación).
IEC 61649	NOTA	Armonizada como Norma EN 61649.
ISO 22000	NOTA	Armonizada como Norma EN ISO 22000.

ÍNDICE

	Página
PRÓLOGO	7
INTRODUCCIÓN.....	9
1 OBJETO Y CAMPO DE APLICACIÓN.....	10
2 NORMAS PARA CONSULTA.....	10
3 TÉRMINOS Y DEFINICIONES	10
4 CONCEPTOS DE APRECIACIÓN DEL RIESGO	10
4.1 Propósito y beneficios.....	10
4.2 apreciación del riesgo y marco de trabajo de la gestión del riesgo.....	11
4.3 apreciación del riesgo y proceso de gestión del riesgo.....	11
4.3.1 Generalidades	11
4.3.2 Comunicación y consultas.....	12
4.3.3 Establecimiento del contexto	12
4.3.4 apreciación del riesgo.....	14
4.3.5 Tratamiento del riesgo	14
4.3.6 Seguimiento y revisión	14
5 PROCESO DE APRECIACIÓN DEL RIESGO	15
5.1 Presentación.....	15
5.2 Identificación del riesgo	15
5.3 Análisis del riesgo	16
5.3.1 Generalidades	16
5.3.2 apreciación de los controles	17
5.3.3 Análisis de las consecuencias	17
5.3.4 Análisis y estimación de la probabilidad	18
5.3.5 Análisis preliminar	19
5.3.6 Incertidumbres y sensibilidades.....	19
5.4 Evaluación del riesgo.....	19
5.5 Documentación	20
5.6 Seguimiento y revisión de la apreciación del riesgo	21
5.7 Aplicación de la apreciación del riesgo durante las fases del ciclo de vida.....	21
6 SELECCIÓN DE TÉCNICAS DE APRECIACIÓN DEL RIESGO.....	22
6.1 Generalidades	22
6.2 Selección de técnicas.....	22
6.3 Disponibilidad de recursos	23
6.4 Naturaleza y grado de la incertidumbre.....	23
6.5 Complejidad.....	23
6.6 Aplicación de la apreciación del riesgo durante las fases del ciclo de vida.....	23
6.7 Tipos de técnicas de apreciación del riesgo	24
ANEXO A (Informativo) COMPARACIÓN DE TÉCNICAS DE APRECIACIÓN DEL RIESGO	25
ANEXO B (Informativo) TÉCNICAS DE APRECIACIÓN DEL RIESGO.....	31
BIBLIOGRAFÍA.....	99

Figura 1 – Contribución de la apreciación del riesgo al proceso de gestión del riesgo	15
Figura B.1 – Curva de dosis-respuesta	43
Figura B.2 – Ejemplo de un FTA según la Norma IEC 60300-3-9.....	56
Figura B.3 – Ejemplo de un árbol de sucesos.....	59
Figura B.4 – Ejemplo de análisis de causa-consecuencia.....	62
Figura B.5 – Ejemplo de diagrama de espina de pescado "Fishbone" o de Ishikawa.....	64
Figura B.6 – Ejemplo de formulación en árbol del análisis de causa-y-efecto.....	65
Figura B.7 – Ejemplo de apreciación de la fiabilidad humana	71
Figura B.8 – Ejemplo de diagrama de pajarita para consecuencias no deseadas.....	73
Figura B.9 – Ejemplo de diagrama Markov	78
Figura B.10 – Ejemplo de diagrama de transición de estado	79
Figura B.11 – Muestra de red Bayes.....	85
Figura B.12 – El concepto ALARP ("tan bajo como razonablemente sea posible").....	88
Figura B.13 – Ejemplo parcial de una tabla de criterios de consecuencia	93
Figura B.14 – Ejemplo parcial de una matriz de clasificación jerárquica del riesgo	93
Figura B.15 – Ejemplo parcial de una matriz de criterios de probabilidad.....	94
 Tabla A.1 – Aplicabilidad de las herramientas utilizadas para la apreciación del riesgo	 26
Tabla A.2 – Atributos de una selección de herramientas para la apreciación del riesgo.....	27
Tabla B.1 – Ejemplos de posibles palabras guía HAZOP.....	39
Tabla B.2 – Matriz Markov.....	77
Tabla B.3 – Matriz Markov final	79
Tabla B.4 – Ejemplo de simulación Monte Carlo.....	82
Tabla B.5 – Datos de la tabla Bayes.....	85
Tabla B.6 – Probabilidades previas para los nudos A y B.....	86
Tabla B.7 – Probabilidades condicionales para el nudo C con el nudo A y el nudo B definidos....	86
Tabla B.8 – Probabilidades condicionales para el nudo D con el nudo A y el nudo C definidos....	86
Tabla B.9 – Probabilidad posterior para los nudos A y B con el nudo D y el nudo C definidos	86
Tabla B.10 – Probabilidad posterior para el nudo A con el nudo D y el nudo C definidos	87

COMISIÓN ELECTROTÉCNICA INTERNACIONAL

Gestión del riesgo
Técnicas de apreciación del riesgo

PRÓLOGO

- 1) IEC (Comisión Electrotécnica Internacional) es una organización mundial para la normalización, que comprende todos los comités electrotécnicos nacionales (Comités Nacionales de IEC). El objetivo de IEC es promover la cooperación internacional sobre todas las cuestiones relativas a la normalización en los campos eléctrico y electrónico. Para este fin y también para otras actividades, IEC publica Normas Internacionales, Especificaciones Técnicas, Informes Técnicos, Especificaciones Disponibles al Público (PAS) y Guías (de aquí en adelante "Publicaciones IEC"). Su elaboración se confía a los comités técnicos; cualquier Comité Nacional de IEC que esté interesado en el tema objeto de la norma puede participar en su elaboración. Organizaciones internacionales gubernamentales y no gubernamentales relacionadas con IEC también participan en la elaboración. IEC colabora estrechamente con la Organización Internacional de Normalización (ISO), de acuerdo con las condiciones determinadas por acuerdo entre ambas.
- 2) Las decisiones formales o acuerdos de IEC sobre materias técnicas, expresan en la medida de lo posible, un consenso internacional de opinión sobre los temas relativos a cada comité técnico en los que existe representación de todos los Comités Nacionales interesados.
- 3) Los documentos producidos tienen la forma de recomendaciones para uso internacional y se aceptan en este sentido por los Comités Nacionales mientras se hacen todos los esfuerzos razonables para asegurar que el contenido técnico de las publicaciones IEC es preciso, IEC no puede ser responsable de la manera en que se usan o de cualquier mal interpretación por parte del usuario.
- 4) Con el fin de promover la unificación internacional, los Comités Nacionales de IEC se comprometen a aplicar de forma transparente las Publicaciones IEC, en la medida de lo posible en sus publicaciones nacionales y regionales. Cualquier divergencia entre la Publicación IEC y la correspondiente publicación nacional o regional debe indicarse de forma clara en esta última.
- 5) IEC no establece ningún procedimiento de marcado para indicar su aprobación y no se le puede hacer responsable de cualquier equipo declarado conforme con una de sus publicaciones.
- 6) Todos los usuarios deberían asegurarse de que tienen la última edición de esta publicación.
- 7) No se debe adjudicar responsabilidad a IEC o sus directores, empleados, auxiliares o agentes, incluyendo expertos individuales y miembros de sus comités técnicos y comités nacionales de IEC por cualquier daño personal, daño a la propiedad u otro daño de cualquier naturaleza, directo o indirecto, o por costes (incluyendo costes legales) y gastos derivados de la publicación, uso o confianza de esta publicación IEC o cualquier otra publicación IEC.
- 8) Se debe prestar atención a las normas para consulta citadas en esta publicación. La utilización de las publicaciones referenciadas es indispensable para la correcta aplicación de esta publicación.
- 9) Se debe prestar atención a la posibilidad de que algunos de los elementos de esta Publicación IEC puedan ser objeto de derechos de patente. No se podrá hacer responsable a IEC de identificar alguno o todos esos derechos de patente.

La Norma IEC/ISO 31010 ha sido elaborada por el comité técnico 56 *Confiabilidad*, junto con el Grupo de Trabajo ISO TMB *Gestión del riesgo*.

El texto de esta norma se basa en los documentos siguientes:

FDIS	Informe de voto
56/1329/FDIS	56/1346/RVD

El informe de voto indicado en la tabla anterior ofrece toda la información sobre la votación para la aprobación de esta norma. En ISO esta norma ha sido aprobada por 17 de los 18 organismos miembros que emitieron voto.

Esta norma ha sido elaborada de acuerdo con las Directivas ISO/IEC, Parte 2.

El comité ha decidido que el contenido de esta norma (la norma base y sus modificaciones) permanezca vigente hasta la fecha de mantenimiento indicada en la página web de IEC "<http://webstore.iec.ch>" en los datos relativos a la norma específica. En esa fecha, la norma será

- confirmada;
- anulada;
- reemplazada por una edición revisada; o
- modificada.

IMPORTANTE – Esta publicación contiene colores que se consideran útiles para el correcto entendimiento de su contenido. Por tanto, los usuarios deberían imprimir este documento utilizando una impresora a color.

INTRODUCCIÓN

Organizaciones de todos los tipos y tamaños se enfrentan a una variedad de riesgos que pueden afectar a la consecución de los objetivos previstos.

Estos objetivos pueden estar relacionados con diferentes actividades de la organización, desde iniciativas estratégicas hasta sus operaciones, procesos y proyectos, y se reflejan en términos sociales, ambientales, tecnológicos, de seguridad y relacionados con la seguridad, comerciales, financieros y de medidas económicas, así como de impactos sociales, culturales, políticos y de reputación.

Todas las actividades de una organización implican riesgos que se deberían gestionar. El proceso de gestión del riesgo ayuda a tomar decisiones teniendo en cuenta la incertidumbre y la posibilidad de futuros sucesos o circunstancias (previstas o imprevistas) y sus efectos sobre los objetivos acordados.

La gestión del riesgo incluye la aplicación de métodos lógicos y sistemáticos para:

- comunicar y consultar a lo largo de este proceso;
- establecer del contexto para la identificación, análisis, evaluación, tratamiento del riesgo asociado con cualquier actividad, proceso, función o producto;
- realizar el seguimiento y revisar los riesgos;
- informar y registrar los resultados de manera apropiada.

La apreciación del riesgo es la parte de la gestión del riesgo que proporciona un proceso estructurado que identifica la manera en que los objetivos pueden resultar afectados, y analiza el riesgo en términos de consecuencias y de sus probabilidades antes de decidir si se necesita un tratamiento adicional.

La apreciación del riesgo trata de dar respuesta a las siguientes cuestiones fundamentales:

- ¿qué puede suceder y porque (para la identificación del riesgo)?
- ¿cuáles son las consecuencias?
- ¿cuál es la probabilidad de su ocurrencia futura?
- ¿existen factores que mitiguen las consecuencias del riesgo o que reduzcan la probabilidad del riesgo?

¿Es el nivel de riesgo tolerable o aceptable y requiere tratamiento adicional?. Esta norma está prevista para reflejar las buenas prácticas actuales en la selección y utilización de las técnicas de apreciación del riesgo, y no se refiere a conceptos nuevos o desarrollados que no hayan alcanzado un nivel satisfactorio de consenso profesional.

Esta norma es de carácter general, por lo que puede proporcionar directrices a seguir por numerosas industrias y diferentes tipos de sistemas. En estas industrias pueden existir normas más específicas que establezcan metodologías y niveles de apreciación preferentes para aplicaciones particulares. Si tales normas están en armonía con esta norma, las normas específicas generalmente serán suficientes.

Gestión del riesgo Técnicas de apreciación del riesgo

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma internacional es una norma de apoyo de la Norma ISO 31000, y proporciona directrices para la selección y aplicación de técnicas sistemáticas para la apreciación del riesgo.

La apreciación del riesgo realizada de acuerdo con esta norma contribuye a otras actividades de gestión del riesgo.

Se presenta la aplicación de una serie de técnicas, con referencias específicas a otras normas internacionales, donde el concepto y la aplicación de técnicas se describen con mayor detalle.

Esta norma no está prevista para fines de certificación, ni para usos reglamentarios o contractuales.

Esta norma no proporciona criterios específicos para identificar la necesidad de aplicar el análisis del riesgo, ni especifica el método de análisis del riesgo que se requiere para una aplicación particular.

Esta norma no hace referencia a todas las técnicas, y la omisión de una técnica en esta norma no significa que dicha técnica no sea válida. El hecho de que un método sea aplicable a una circunstancia particular no significa que éste se debería aplicar necesariamente.

NOTA Esta norma no trata la seguridad de una manera específica. Es una norma genérica para la gestión del riesgo y cualquier referencia a seguridad es simplemente de carácter informativo. La Guía ISO/IEC 51 proporciona directrices sobre la introducción de aspectos de seguridad en las normas IEC.

2 NORMAS PARA CONSULTA

Las normas que a continuación se indican son indispensables para la aplicación de esta norma. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición de la norma (incluyendo cualquier modificación de ésta).

Guía ISO/IEC 73, *Gestión del riesgo. Vocabulario. Directrices para la utilización en las normas.*

ISO 31000 *Gestión del riesgo. Principios y directrices.*

3 TÉRMINOS Y DEFINICIONES

Para los fines de este documento, se aplican los términos y definiciones incluidos en la Guía ISO/IEC 73.

4 CONCEPTOS DE APRECIACIÓN DEL RIESGO

4.1 Propósito y beneficios

La finalidad de la apreciación del riesgo consiste en proporcionar evidencias basadas en información y análisis para tomar decisiones informadas sobre cómo tratar riesgos particulares y cómo hacer la selección entre distintas opciones.

Entre los principales beneficios de realizar la apreciación del riesgo, se incluyen:

- comprender el riesgo y su impacto potencial sobre los objetivos;
- proporcionar información a las personas que toman decisiones;

- contribuir a comprender los riesgos, para ayudar en la selección de las opciones de tratamiento;
- identificar a los factores principales que contribuyan a los riesgos, y los puntos débiles en los sistemas y organizaciones;
- comparar los riesgos en sistemas, tecnologías o enfoques alternativos;
- comunicar los riesgos y las incertidumbres;
- ayudar a establecer prioridades;
- contribuir a la prevención de incidentes en base a investigaciones posteriores de incidentes;
- seleccionar diferentes formas de tratamiento del riesgo;
- cumplir los requisitos reglamentarios;
- proporcionar información que ayudará a evaluar si se debería aceptar el riesgo cuando se compara con criterios predefinidos;
- realizar la apreciación de los riesgos unidos al final de la vida útil.

4.2 Apreciación del riesgo y marco de trabajo de la gestión del riesgo

Esta norma asume que la apreciación del riesgo se realiza dentro del marco de trabajo y del proceso de gestión del riesgo descrito en la Norma ISO 31000.

El marco de trabajo de la gestión del riesgo proporciona las políticas, los procedimientos, y las disposiciones de la organización que permita la integración de la gestión del riesgo a todos los niveles de la organización.

Como parte de este marco de trabajo, la organización debería disponer de una política o estrategia para deducir cómo y cuando se debería realizar la apreciación de los riesgos.

En particular, los responsables de la realización de la apreciación del riesgo deberían tener claro lo relativo a:

- el contexto y los objetivos de la organización;
- al alcance y los tipos de riesgo que son tolerables, así como la forma en que se han de tratar los riesgos inaceptables;
- la forma en que la apreciación del riesgo se integra en los procesos de la organización;
- los métodos y las técnicas que se utilizan para la apreciación del riesgo, y su contribución al proceso de gestión del riesgo;
- las competencias, las responsabilidades y la autoridad para realizar la apreciación del riesgo;
- los recursos disponibles para realizar la apreciación del riesgo;
- cómo se informará y revisará la apreciación del riesgo.

4.3 Apreciación del riesgo y proceso de gestión del riesgo

4.3.1 Generalidades

La apreciación del riesgo comprende los elementos centrales del proceso de gestión del riesgo que se definen en la Norma ISO 31000, y contiene los siguientes elementos:

- comunicación y la consulta;

- establecimiento del contexto;
- apreciación del riesgo (que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo);
- tratamiento del riesgo;
- seguimiento y revisión.

La apreciación del riesgo no es una actividad aislada, y debería estar totalmente integrada con los otros componentes del proceso de gestión del riesgo.

4.3.2 Comunicación y consultas

El éxito de la apreciación del riesgo depende del establecimiento de comunicaciones y consultas eficaces con las partes interesadas.

Las partes interesadas involucradas en el proceso de gestión del riesgo ayudarán a:

- desarrollar un plan de comunicación;
- definir el contexto de manera apropiada;
- asegurar que los intereses de las partes interesadas se comprenden y se tienen en consideración;
- reunir las diferentes áreas de conocimiento técnico para la identificación y el análisis del riesgo;
- asegurar que las diferentes opiniones se tienen en cuenta de forma adecuada en la evaluación de los riesgos;
- asegurar que los riesgos se identifican adecuadamente;
- conseguir la aprobación y el apoyo para un plan de tratamiento.

Las partes interesadas deberían contribuir a establecer la conexión del proceso de apreciación del riesgo con otras disciplinas de gestión, incluidas la gestión de cambios, la gestión de proyectos y programas, así como la gestión financiera.

4.3.3 Establecimiento del contexto

Mediante el establecimiento del contexto se definen los parámetros básicos para gestionar el riesgo y se establece el alcance y los criterios para el resto del proceso. El establecimiento del contexto incluye la consideración de los parámetros internos y externos aplicables a la organización considerada en su totalidad, así como los antecedentes de los riesgos particulares sobre los que se realiza la apreciación.

En el establecimiento del contexto, se determinan y acuerdan los objetivos de la apreciación del riesgo, los criterios de riesgo, y el programa de apreciación del riesgo.

Para una apreciación del riesgo específica, en el establecimiento del contexto se debería incluir la definición del contexto externo e interno de gestión del riesgo y la clasificación de los criterios de riesgo:

- a) El establecimiento del contexto externo implica la familiarización con el entorno donde la organización y el sistema funcionan, incluyendo:
 - los factores culturales, políticos, legales, reglamentarios, financieros, económicos y del entorno, que sean competitivos, a nivel internacional, nacional, regional o local;
 - los factores y tendencias clave que tengan impacto en los objetivos de la organización; y
 - las percepciones y los valores de las partes interesadas externas.

b) El establecimiento del contexto interno implica la comprensión de:

- las capacidades de la organización en términos de recursos y conocimiento;
- los flujos de información y los procesos de toma de decisiones;
- las partes interesadas internas;
- los objetivos y las estrategias a seguir para conseguirlo;
- las percepciones, los valores y la cultura;
- las políticas y los procesos;
- las normas y los modelos de referencia adoptados por la organización; y
- las estructuras (por ejemplo, el gobierno, las funciones y las responsabilidades).

c) El establecimiento del contexto del proceso de gestión del riesgo incluye:

- definir las responsabilidades;
- definir el alcance de las actividades de la gestión del riesgo a realizar, incluyendo inclusiones y exclusiones específicas;
- definir la extensión del proyecto, proceso, función o actividad, en términos de tiempo y de ubicación;
- definir las relaciones entre un proyecto o actividad particular y otros proyectos o actividades de la organización;
- definir las metodologías de apreciación del riesgo;
- definir los criterios de riesgo;
- definir la manera de evaluar el desempeño de la gestión del riesgo;
- identificar y especificar las decisiones y acciones a tomar; e
- identificar los estudios de alcance o de ámbito necesarios, su extensión y sus objetivos, así como los recursos necesarios para tales estudios.

d) La definición de los criterios de riesgo implica decidir:

- la naturaleza y los tipos de las consecuencias a incluir y la manera de medirlas;
- la manera de expresar la probabilidad;
- la manera de determinar el nivel de riesgo;
- los criterios para decidir cuando un riesgo necesita tratamiento;
- los criterios para decidir cuando un riesgo es aceptable y/o tolerable;
- si y cómo se tendrán en cuenta las combinaciones de riesgos.

Los criterios se pueden basar en fuentes tales como:

- los objetivos de proceso acordados;
- los criterios identificados en las especificaciones;
- las fuentes de datos generales;
- los criterios de la industria aceptados normalmente, tales como los niveles de seguridad integral;
- el apetito por el riesgo de la organización;
- los requisitos legales y de otro tipo para equipos o aplicaciones específicos.

4.3.4 Apreciación del riesgo

La apreciación del riesgo es el proceso global de identificación, de análisis y de evaluación del riesgo.

Los riesgos se pueden apreciar a nivel de la organización, a nivel de un departamento, por proyectos, por actividades individuales o por riesgos específicos. En contextos diferentes puede ser apropiado aplicar herramientas y técnicas diferentes.

La apreciación del riesgo proporciona un conocimiento de los riesgos, de sus causas, de sus consecuencias y de sus probabilidades. Esto proporciona datos para tomar decisiones acerca de:

- si se debería realizar una actividad;
- cómo maximizar las oportunidades;
- si los riesgos necesitan tratarse;
- la elección entre opciones con riesgos diferentes;
- la asignación de prioridades a las opciones de tratamiento del riesgo;
- la selección más apropiada de las estrategias de tratamiento del riesgo que llevarán a los riesgos adversos hasta un nivel tolerable.

4.3.5 Tratamiento del riesgo

Una vez completada la apreciación del riesgo, el tratamiento del riesgo implica la selección y el acuerdo para aplicar una o varias opciones pertinentes para cambiar la probabilidad de que los riesgos ocurran, los efectos de los riesgos, o ambas cosas, así como la implantación de estas opciones.

A continuación de esto, sigue un proceso crítico de reapreciación del nuevo nivel de riesgo, con la intención de determinar su tolerancia con respecto a los criterios previamente establecidos, para decidir si se requiere tratamiento adicional.

4.3.6 Seguimiento y revisión

Como parte del proceso de gestión del riesgo, los riesgos y los controles se deberían monitorizar y revisar de manera regular, con objeto de verificar que:

- las hipótesis establecidas en relación con los riesgos continúan siendo válidas;
- las hipótesis en que se ha basado la apreciación del riesgo, incluyendo los contextos externo e interno, continúan siendo válidas;

- se han logrado los resultados previstos;
- los resultados de la apreciación del riesgo están en línea con la experiencia real;
- las técnicas de apreciación del riesgo se han aplicado adecuadamente;
- los tratamientos del riesgo son eficaces.

Se deberían establecer las responsabilidades para el seguimiento y para la realización de las revisiones.

5 PROCESO DE APRECIACIÓN DEL RIESGO

5.1 Presentación

La apreciación del riesgo proporciona a las personas que toman decisiones y a las partes responsables una mejor comprensión de los riesgos que podrían afectar al logro de los objetivos y a la idoneidad y eficacia de los controles ya establecidos. Esto proporciona una base para tomar decisiones sobre el enfoque más apropiado que se debe utilizar para tratar los riesgos. Los resultados de la apreciación del riesgo constituyen datos de entrada para el proceso de toma de decisiones de la organización.

La apreciación del riesgo es el proceso global de identificación, de análisis y de evaluación del riesgo (véase la figura 1). La manera de aplicar este proceso no solo depende del contexto del proceso de gestión del riesgo, sino también de los métodos y técnicas utilizadas para realizar la apreciación del riesgo.

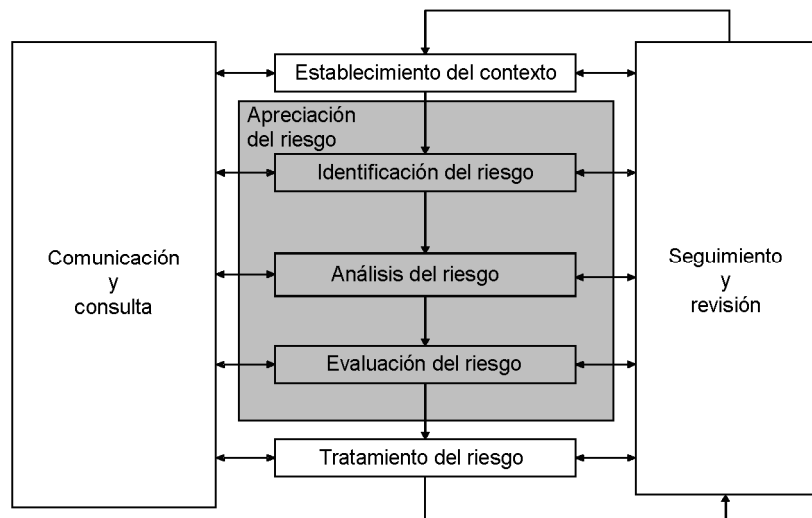


Figura 1 – Contribución de la apreciación del riesgo al proceso de gestión del riesgo

La apreciación del riesgo puede requerir un enfoque multidisciplinario dado que los riesgos pueden cubrir una amplia gama de causas y consecuencias.

5.2 Identificación del riesgo

La identificación del riesgo es el proceso con el que se descubren, reconocen y registran los riesgos.

La finalidad de la identificación del riesgo es identificar los sucesos o las situaciones que pudiesen presentarse y afectar al logro de los objetivos del sistema o de la organización. Una vez que el riesgo está identificado, la organización debería identificar cualquiera de los controles existentes, tales como características de diseño, personas, procesos y sistemas.

El proceso de identificación del riesgo incluye la identificación de las causas y del origen del riesgo (peligro en el contexto de los daños físicos), sucesos, situaciones o circunstancias que pudiesen tener un impacto material sobre los objetivos y la naturaleza del impacto.

Los métodos de identificación del riesgo pueden incluir:

- los métodos basados en evidencias, ejemplos de esto son las listas de verificación y las revisiones de datos históricos;
- los enfoques sistemáticos del equipo, donde un grupo de expertos sigue un proceso sistemático para identificar riesgos por medio de un conjunto estructurado de proposiciones o preguntas;
- las técnicas de razonamiento inductivo, tal como HAZOP.

Para mejorar la precisión y la exhaustividad de la identificación del riesgo se pueden aplicar diversas técnicas de apoyo, incluidas tormenta de ideas y la metodología Delphi.

Con independencia de las técnicas actuales empleadas, cuando se identifica el riesgo es importante dar el debido reconocimiento a los factores humanos y de la organización. Por ello, en el proceso de identificación del riesgo se deberían incluir las desviaciones de los factores humanos y de la organización con respecto a lo esperado, así como los elementos de "hardware" o de "software".

5.3 Análisis del riesgo

5.3.1 Generalidades

El análisis del riesgo implica desarrollar una comprensión del riesgo. Proporciona un elemento de entrada para la apreciación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como las estrategias y los métodos de tratamiento del riesgo más apropiados.

El análisis del riesgo consiste en determinar las consecuencias y sus probabilidades para sucesos de riesgo identificados, teniendo en cuenta la presencia (o no) y la eficacia de todos los controles existentes. Las consecuencias y sus probabilidades se combinan después para determinar un nivel de riesgo.

El análisis del riesgo implica la consideración de las causas y las fuentes del riesgo, sus consecuencias, y la probabilidad de que estas consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y a la probabilidad. Un suceso puede tener múltiples consecuencias y puede afectar a múltiples objetivos. Se deberían tener en cuenta los controles de riesgo existentes y la eficacia de los mismos. En el anexo B se describen varios métodos para la realización de estos análisis. Para aplicaciones complejas se puede requerir más de una técnica.

El análisis del riesgo incluye normalmente una estimación de la gama de posibles consecuencias que se podrían derivar de un suceso, situación, o circunstancia, y de sus probabilidades asociadas, a fin de medir el nivel de riesgo. No obstante, en algunas circunstancias, tales como cuando es probable que las consecuencias sean insignificantes o se espera que la probabilidad sea extremadamente baja, se estima que un solo parámetro puede ser suficiente para tomar una decisión.

En algunas circunstancias se puede producir una consecuencia como resultado de una gama de sucesos o condiciones diferentes, o cuando el suceso específico no está identificado. En este caso, el centro de atención de la apreciación del riesgo está en analizar la importancia y vulnerabilidad de los componentes del sistema, con la intención de definir los tratamientos con respecto a los niveles de protección o a las estrategias de recuperación.

Los métodos que se utilizan en el análisis de riesgos pueden ser cualitativos, semicuantitativos, o cuantitativos. El grado de detalle requerido dependerá de la aplicación particular, de la disponibilidad de datos fiables y de las necesidades de toma de decisiones de la organización. Algunos métodos y el grado de detalle del análisis pueden estar establecidos por la legislación.

La apreciación cualitativa define las consecuencias, la probabilidad y el nivel de riesgo, indicando niveles tales como "alto", "medio" y "bajo", y puede combinar las consecuencias y la probabilidad y evaluar el nivel de riesgo resultante en función de criterios cualitativos.

Los métodos semicuantitativos utilizan escalas de valoración numéricas para las consecuencias y la probabilidad, y las combinan para determinar un nivel de riesgo aplicando una fórmula. Las escalas pueden ser lineales o logarítmicas, o tener alguna otra relación; las fórmulas utilizadas también pueden variar.

El análisis cuantitativo estima valores realistas para las consecuencias y sus probabilidades, y obtiene valores del nivel de riesgo en unidades específicas definidas cuando se desarrolla el contexto. El análisis cuantitativo completo no siempre puede ser posible o deseable debido a insuficiente información acerca del sistema o actividad que se está analizando, a la falta de datos, a la influencia de factores humanos, etc., o porque no se requiere o no está garantizado el resultado del análisis cuantitativo. En estas circunstancias, aún puede ser efectiva una clasificación semicuantitativa o cualitativa de los riesgos realizada por especialistas conocedores de sus respectivos campos de actuación.

En los casos en que el análisis sea cualitativo, se deberían explicar con claridad todos los términos empleados, y se deberían registrar las bases establecidas para todos los criterios.

Incluso cuando se haya realizado la cuantificación total, es necesario reconocer que todos los niveles de riesgo calculados son estimativos. Se debería tener cuidado en confirmar que a estos niveles de riesgo no se atribuye un nivel de exactitud y precisión que sea contradictorio con la precisión de los datos y métodos empleados.

Los niveles de riesgo se deberían expresar en los términos más adecuados para el tipo de riesgo en cuestión, y de una manera que ayude a la evaluación del riesgo. En algunos casos, la magnitud de un riesgo se puede expresar como una distribución de probabilidad sobre una gama de consecuencias.

5.3.2 Apreciación de los controles

El nivel del riesgo dependerá de la idoneidad y eficacia de los controles existentes. Las cuestiones a considerar incluyen:

- ¿cuáles son los controles existentes para un riesgo particular?
- ¿pueden estos controles tratar adecuadamente el riesgo, de manera que quede controlado hasta un nivel que se considere tolerable?
- ¿en la práctica, funcionan los controles de la manera prevista y pueden demostrar que son eficaces cuando se requiere la aplicación de los mismos?

Estas preguntas solamente se pueden contestar con certeza cuando existe la documentación adecuada y se implantan procesos de garantía.

El nivel de eficacia de un control particular, o de una serie de controles relacionados, se puede expresar de forma cualitativa, semicuantitativa o cuantitativa. En la mayoría de los casos, no se garantiza un alto nivel de exactitud. No obstante, puede ser valioso expresar y registrar una medida de la eficacia del control del riesgo, con objeto de poder juzgar si sería mejor emplear el esfuerzo en mejorar ese control o en disponer de un tratamiento diferente del riesgo.

5.3.3 Análisis de las consecuencias

El análisis de las consecuencias determina la naturaleza y el tipo de impacto que se podría producir asumiendo que se ha producido un suceso, situación o circunstancia particulares. Un suceso puede dar lugar a una gama de impactos de diferentes magnitudes, y afectar a una gama de diferentes objetivos y diferentes partes interesadas. Los tipos de consecuencias a analizar y las partes interesadas afectadas se han tenido que decidir cuándo se estableció el contexto.

El análisis de las consecuencias puede variar desde una descripción simple de las consecuencias hasta un modelo cuantitativo detallado o un análisis de vulnerabilidad.

Los impactos pueden tener una consecuencia leve con una alta probabilidad, o una consecuencia grave con una baja probabilidad, o alguna consecuencia intermedia. En algunos casos, es apropiado centrar la atención en riesgos que posiblemente tengan consecuencias muy importantes, dado que con frecuencia son los que conciernen en gran medida a los gestores de la organización. En otros casos puede ser importante analizar por separado los riesgos de consecuencias graves y de consecuencias leves. Por ejemplo, un problema frecuente pero de bajo impacto (o crónico) puede tener efectos grandes por acumulación o efectos a largo plazo. Además, las acciones de tratamiento de estos dos tipos distintos de riesgos son con frecuencia bastante diferentes, por lo que es útil analizarlos por separado.

El análisis de las consecuencias puede implicar:

- tener en consideración los controles existentes para tratar las consecuencias, junto con todos los factores que contribuyen al riesgo de una manera importante y que tienen efecto sobre las consecuencias;
- relacionar las consecuencias del riesgo con los objetivos iniciales;
- tener en consideración tanto las consecuencias inmediatas como las que pueden aparecer después de que haya transcurrido un cierto tiempo, si esto es consecuente con el campo de aplicación de la apreciación;
- tener en consideración las consecuencias secundarias, tales como las que impactan sobre sistemas, actividades, equipos u organizaciones asociadas.

5.3.4 Análisis y estimación de la probabilidad

Para estimar la probabilidad se emplean normalmente tres enfoques generales; estos enfoques se pueden aplicar individualmente o en conjunto:

- a) La utilización de datos históricos importantes para identificar sucesos o situaciones que han ocurrido en el pasado y que permiten extrapolar la probabilidad de que vuelvan a ocurrir en el futuro. Los datos utilizados deberían ser aplicables al tipo de sistema, instalación, organización o actividad que se está considerando, y también a las normas de funcionamiento de la organización implicada. Si los datos históricos existentes muestran que la frecuencia de que el suceso ocurra es muy baja, entonces cualquier estimación de probabilidad será muy incierta. Esto se aplica especialmente cuando la posibilidad de que ocurra es cero, cuando no se puede asumir que el suceso, situación o circunstancia no ocurrirá en el futuro.
- b) Los pronósticos de probabilidad utilizan técnicas de predicción tales como el análisis del árbol de fallos y el análisis del árbol de sucesos (véase el anexo B). Cuando los datos históricos no están disponibles o no son adecuados, es necesario obtener la probabilidad mediante el análisis del sistema, actividad, equipo u organización y sus estados asociados de fallo o de éxito. Los datos numéricos sobre el equipo, las personas, las organizaciones y los sistemas, obtenidos de la experiencia operacional, o de fuentes de datos publicados, se combinan después para obtener una estimación de la probabilidad superior del suceso. Cuando se utilizan técnicas de predicción, es importante comprobar que en el análisis se han introducido las tolerancias oportunas con respecto a la posibilidad de fallos comunes que impliquen el fallo coincidente de un determinado número de partes o componentes diferentes dentro del sistema que se originan por la misma causa. Se pueden requerir técnicas de simulación para generar la probabilidad de fallos del equipo o estructurales debidos al envejecimiento y a otros procesos de degradación, mediante el cálculo de los efectos de las incertidumbres.
- c) La opinión de un experto se puede utilizar en procesos sistemáticos y estructurados para estimar la probabilidad. Los juicios de expertos deberían aportar toda la información aplicable disponible, incluyendo datos históricos, datos específicos del sistema, datos específicos de la organización, datos experimentales, datos de diseño, etc. Existe un determinado número de métodos formales para lograr juicios de expertos que proporcionen una ayuda para formular las preguntas apropiadas. Los métodos disponibles incluyen el enfoque Delphi, las comparaciones pareadas, la clasificación en categorías y los dictámenes de probabilidad absoluta.

5.3.5 Análisis preliminar

Los riesgos se pueden filtrar con objeto de identificar los más importantes, o para excluir los riesgos menos significativos o menores de los análisis posteriores. La finalidad de esto es asegurar que los recursos se dirigirán a los riesgos más importantes. Se debería tener cuidado en no eliminar riesgos pequeños que ocurran frecuentemente y que tengan un efecto acumulado importante.

El filtrado se debería basar en criterios definidos en el contexto. El análisis preliminar determina una o varias de las siguientes vías de acción:

- decidir el tratamiento de los riesgos sin ninguna apreciación adicional;
- establecer los riesgos insignificantes que no justificarían un tratamiento;
- proceder a realizar una apreciación del riesgo más detallada.

Las hipótesis iniciales y los resultados se deberían documentar.

5.3.6 Incertidumbres y sensibilidades

Con frecuencia existe un considerable número de incertidumbres asociadas con el análisis del riesgo. Para interpretar y comunicar el análisis del riesgo de una manera eficaz es necesario tener un conocimiento adecuado de las incertidumbres. El análisis de las incertidumbres asociadas con los datos, métodos y modelos utilizados para identificar y analizar el riesgo juega un papel muy importante en su aplicación. El análisis de la incertidumbre implica la determinación de la variación o imprecisión en los resultados, originada por la variación colectiva de los parámetros e hipótesis que se han utilizado para definir los resultados. Un área muy relacionada con el análisis de la incertidumbre es el análisis de sensibilidad.

El análisis de sensibilidad implica la determinación del tamaño y la importancia de la magnitud de riesgo a cambios en parámetros de entrada individuales. Este análisis de sensibilidad se utiliza para identificar aquellos datos que se necesita que sean precisos, y los datos que son menos sensibles y por tanto tienen menos efecto sobre la exactitud en general.

Se debería declarar de la forma más completa posible la exhaustividad y la exactitud del análisis de riesgo. Cuando sea posible, se deberían identificar los orígenes de incertidumbre y consignar las incertidumbres de los datos y del modelo/método. También se deberían consignar los parámetros para los cuales el análisis es sensible así como el grado de sensibilidad.

5.4 Evaluación del riesgo

La evaluación del riesgo implica la comparación de niveles estimados de riesgo con los criterios de riesgo definidos cuando se estableció el contexto, con objeto de determinar la importancia del nivel y tipo de riesgo.

En la evaluación del riesgo se aplica el conocimiento del riesgo obtenido durante el análisis del riesgo, para tomar decisiones sobre acciones futuras. Las consideraciones éticas, legales, financieras y de otros tipos, incluidas las percepciones de riesgo, también son factores de entrada para la toma de decisiones.

Las decisiones pueden incluir:

- si el riesgo necesita tratarse;
- las prioridades de tratamiento;
- si se debería emprender una actividad;
- el camino que se debería seguir.

La naturaleza de las decisiones que sean necesarias tomar y los criterios que se utilizarán para tomar las decisiones se decidieron cuando se estableció el contexto, pero es necesario revisarlos con más detalle en esta etapa, cuando ya se conocen mejor los riesgos particulares identificados.

El marco de trabajo más simple para definir los criterios de riesgo es un solo nivel que separe los riesgos que necesitan tratamiento de los que no necesitan tratamiento. Esto proporciona unos resultados aparentemente simples pero que no reflejan las incertidumbres implicadas tanto en la estimación de riesgos como en la definición de los límites entre los que necesitan tratamiento y los que no lo necesitan.

La decisión sobre si se debe tratar el riesgo y de cómo tratarlo, puede depender de los costes y de los beneficios de aceptar el riesgo y de los costes y beneficios de implantar controles mejorados.

Un enfoque común consiste en dividir los riesgos en tres bandas:

- a) una banda superior, donde el nivel de riesgo se considera intolerable, cualquiera que sean los beneficios que la actividad puede proporcionar, y donde el tratamiento del riesgo es esencial cualquiera que sea su coste;
- b) una banda media (o zona "gris"), donde los costes y los beneficios se tienen en cuenta y las oportunidades se compensan con respecto a las consecuencias potenciales;
- c) una banda inferior, donde el nivel de riesgo se considera insignificante o tan pequeño que no es necesario tomar medidas para el tratamiento del riesgo.

El sistema de criterio "tan bajo como razonablemente sea posible" o ALARP que se utiliza en aplicaciones de seguridad, también se sigue en este enfoque, donde, en la banda media existe una escala gradual para riesgos bajos donde los costes y los beneficios se pueden comparar directamente, mientras que para riesgos altos se debe reducir el potencial de perjuicios hasta que los costes de una reducción adicional sean totalmente desproporcionados con respecto a los beneficios de seguridad obtenidos.

5.5 Documentación

El proceso de apreciación del riesgo se debería documentar junto con los resultados de la apreciación. Los riesgos se deberían expresar en términos inteligibles, y las unidades en que se expresa el nivel de riesgo deberían ser claras.

La extensión del informe dependerá de los objetivos y del campo de aplicación de la apreciación. Excepto para apreciaciones muy simples, la documentación puede incluir lo siguiente:

- los objetivos y el campo de aplicación;
- la descripción de las partes pertinentes del sistema y sus funciones;
- un resumen del contexto externo e interno de la organización, y de cómo se relaciona con la situación, sistema o circunstancias que se están apreciando;
- los criterios de riesgo aplicados y la justificación de los mismos;
- las limitaciones, los supuestos y la justificación de las hipótesis;
- la metodología aplicada en la apreciación;
- los resultados de la identificación del riesgo;
- los datos, los supuestos y sus orígenes y validación;
- los resultados del análisis del riesgo y la evaluación de los mismos;

- los análisis de sensibilidad y de incertidumbre;
- los supuestos críticos y otros factores sobre los que se necesita hacer seguimiento;
- la discusión de los resultados;
- las conclusiones y recomendaciones;
- las referencias.

Si la apreciación del riesgo sirve de apoyo al proceso continuo de gestión del riesgo, dicha apreciación se debería realizar y documentar de manera que se pueda mantener durante todo el ciclo de vida del sistema, de la organización, del equipo o de la actividad. La apreciación se debería actualizar cuando se disponga de nueva información significativa y de cambios en el contexto, de acuerdo con las necesidades del proceso de gestión.

5.6 Seguimiento y revisión de la apreciación del riesgo

El proceso de apreciación del riesgo dará importancia al contexto y a otros factores de los que se espera que pudiesen variar con el tiempo y, por tanto, cambiar o invalidar la apreciación del riesgo. Estos factores se deberían identificar específicamente para que sean objeto de seguimiento y revisión, de manera que la apreciación del riesgo se pueda actualizar cuando sea necesario.

También se deberían identificar y recopilar los datos de los que se ha hecho seguimiento con objeto de mejorar la apreciación del riesgo.

También se debería hacer seguimiento y documentar la eficacia de los controles con objeto de disponer de datos para su uso en el análisis del riesgo. Se deberían definir las responsabilidades para la creación y la revisión de la evidencia y la documentación.

5.7 Aplicación de la apreciación del riesgo durante las fases del ciclo de vida

Se puede considerar que muchas actividades, proyectos y productos tienen un ciclo de vida que comienza a partir del concepto y la definición iniciales y continúa con su realización hasta que se lleva a cabo su terminación final, que podría incluir la retirada de servicio y la eliminación del material.

La apreciación del riesgo se puede aplicar en todas las etapas del ciclo de vida, y normalmente se aplica muchas veces con diferentes niveles de detalle para ayudar en la toma de decisiones en cada fase.

Las fases del ciclo de vida tienen requisitos diferentes y necesitan técnicas diferentes. Por ejemplo, durante la fase de concepto y definición, cuando se identifica una oportunidad, la apreciación del riesgo se puede utilizar para decidir si se procede o no.

Cuando existen varias opciones disponibles, la apreciación del riesgo se puede utilizar en la evaluación de conceptos alternativos para ayudar a decidir cuál de ellos proporciona el mejor balance entre los riesgos positivos y negativos.

Durante la fase de diseño y desarrollo, la apreciación del riesgo contribuye a:

- asegurar que los riesgos del sistema son tolerables;
- el proceso de mejora del diseño;
- los estudios de eficacia de los costes;
- la identificación de los riesgos que impactan en las fases siguientes del ciclo de vida.

A medida que avanza la actividad, la apreciación del riesgo se puede utilizar para proporcionar información que ayude a desarrollar procedimientos para condiciones normales y de emergencia.

6 SELECCIÓN DE TÉCNICAS DE APRECIACIÓN DEL RIESGO

6.1 Generalidades

Este capítulo describe cómo se pueden seleccionar técnicas para la apreciación del riesgo. Los anexos listan y describen una gama de herramientas y técnicas que se pueden utilizar para realizar una apreciación del riesgo o para ayudar en el proceso de apreciación del riesgo. Algunas veces puede ser necesario emplear más de un método de apreciación.

6.2 Selección de técnicas

La apreciación del riesgo se puede realizar con diferentes grados de profundidad y de detalle, y utilizando uno o varios métodos que varían desde simples a complejos. La forma de la apreciación y de sus resultados debería ser consecuente con los criterios de riesgo desarrollados como parte del establecimiento del contexto. El anexo A muestra la relación conceptual entre las amplias categorías de técnicas de apreciación del riesgo y los factores presentes en una situación de riesgo dada, y proporciona ejemplos ilustrativos de cómo las organizaciones pueden seleccionar las técnicas apropiadas de apreciación del riesgo para una situación particular.

En términos generales, las técnicas adecuadas deberían tener las siguientes características:

- deberían ser justificables y apropiadas a la situación u organización que se está considerando;
- deberían proporcionar resultados de una forma que mejoren la comprensión de la naturaleza del riesgo y de cómo se puede tratar;
- deberían poderse utilizar de una manera que sea trazable, reproducible y verificable.

Se deberían dar las razones para la elección de técnicas, en cuanto a la importancia y a la idoneidad. Cuando se integran los resultados procedentes de estudios diferentes, las técnicas utilizadas y los resultados deberían ser comparables.

Una vez que se ha tomado la decisión de realizar una apreciación del riesgo, y se han definido los objetivos y el campo de aplicación, las técnicas se deberían seleccionar en base a factores aplicables tales como:

- los objetivos del estudio. Los objetivos de la apreciación del riesgo tendrán una repercusión directa sobre las técnicas utilizadas. Por ejemplo, si se está realizando un estudio comparativo entre diferentes opciones, puede ser aceptable utilizar modelos de consecuencias menos detalladas para partes del sistema que no se vean afectadas por las diferencias;
- las necesidades de las personas que han de tomar decisiones. En algunos casos se necesita un alto nivel de detalle para tomar una buena decisión, mientras que en otros es suficiente una comprensión más general;
- el tipo y la gama de riesgos que se analizan;
- la posible magnitud de las consecuencias. La decisión sobre la profundidad con que se ha de realizar la apreciación del riesgo debería reflejar la percepción inicial de las consecuencias (aunque es posible que se tenga que modificar una vez que se haya completado la evaluación preliminar);
- el grado de conocimientos técnicos, y de recursos humanos y de otros tipos que se necesitan. Un método sencillo, bien aplicado, puede proporcionar mejores resultados que un procedimiento más sofisticado pero aplicado deficientemente, en la medida en que cumpla los objetivos y campo de aplicación de la apreciación del riesgo. Por lo general, el esfuerzo que se ponga en la apreciación debería ser consecuente con el nivel potencial del riesgo que se está analizando;
- la disponibilidad de información y de datos. Algunas técnicas requieren más información y datos que otras;

- la necesidad de modificación/actualización de la apreciación del riesgo. En un futuro puede ser necesario modificar/actualizar la apreciación del riesgo, y a este respecto, algunas técnicas son más fáciles de modificar que otras;
- todos los requisitos contractuales y reglamentarios.

En la selección de un enfoque para la apreciación del riesgo influyen diversos factores, tales como la disponibilidad de recursos, la naturaleza y el grado de incertidumbre de los datos y de la información disponibles, y la complejidad de la aplicación (véase la tabla A.2).

6.3 Disponibilidad de recursos

Los recursos y las capacidades que pueden afectar a la elección de técnicas de apreciación del riesgo, incluyen:

- la capacidad y aptitud en cuanto a experiencia profesional del equipo de personas que ha de realizar la apreciación del riesgo;
- las limitaciones en tiempo y en otros recursos dentro de la organización;
- el presupuesto disponible si se requieren recursos externos.

6.4 Naturaleza y grado de la incertidumbre

La naturaleza y el grado de la incertidumbre requieren una correcta comprensión de la calidad, cantidad e integridad de la información disponible relativa al riesgo que se está considerando. Esto incluye la amplitud de la información disponible sobre el riesgo, sus orígenes y sus causas, así como sus consecuencias para la consecución de los objetivos. La incertidumbre se puede deber a la deficiente calidad de los datos o a la falta de datos esenciales y fiables. Por ejemplo, los métodos de recopilación de datos pueden cambiar la forma en que las organizaciones aplican tales métodos puede cambiar, o las organizaciones pueden utilizar un método de recopilación de datos que no sea eficaz o que los datos recopilados no correspondan al riesgo identificado.

La incertidumbre también puede ser inherente al contexto externo e interno de la organización. Los datos disponibles no siempre proporcionan una base fiable para la predicción del futuro. Para tipos de riesgos únicos, es posible que los datos históricos no estén disponibles o las distintas partes interesadas puedan tener diferentes interpretaciones de los datos disponibles. La apreciación del riesgo llevada a cabo debe comprender el tipo y la naturaleza de la incertidumbre y apreciar las implicaciones de la fiabilidad de los resultados de la apreciación del riesgo. Estos resultados se deberían comunicar siempre a las personas que han de tomar decisiones.

6.5 Complejidad

Los riesgos pueden ser complejos por sí mismos, como por ejemplo, en sistemas complejos donde se necesita disponer de la apreciación del riesgo en todo el sistema, en vez de tratar cada componente por separado e ignorando las interacciones. En otros casos, el tratamiento de un riesgo único puede tener implicaciones por sí mismo y puede impactar en otras actividades. Los impactos resultantes y las dependencias del riesgo deben ser comprendidos para asegurar que la gestión de un riesgo, no crea por sí misma una situación intolerable. La comprensión de la complejidad de un riesgo único o de un conjunto de riesgos de una organización es crucial para la selección del método o de las técnicas apropiadas para la apreciación del riesgo.

6.6 Aplicación de la apreciación del riesgo durante las fases del ciclo de vida

Se puede considerar que muchas actividades, proyectos y productos tienen un ciclo de vida que comienza a partir del concepto y la definición iniciales y continúa con su realización hasta que se lleva a cabo su terminación final, que podría incluir la retirada de servicio y el desmontaje y enajenación del hardware.

La apreciación del riesgo se puede aplicar en todas las etapas del ciclo de vida, y normalmente se aplica muchas veces con diferentes niveles de detalle para ayudar en la toma de decisiones en cada fase.

Las fases del ciclo de vida tienen requisitos diferentes y necesitan técnicas diferentes. Por ejemplo, durante la fase de concepto y definición, cuando se identifica una oportunidad, la apreciación del riesgo se puede utilizar para decidir si se procede o no.

Cuando existen varias opciones disponibles, la apreciación del riesgo se puede utilizar en la evaluación de conceptos alternativos para ayudar a decidir cuál de ellos proporciona el mejor balance entre los riesgos positivos y negativos.

Durante la fase de diseño y desarrollo, la apreciación del riesgo contribuye a:

- asegurar que los riesgos del sistema son tolerables;
- el proceso de mejora del diseño;
- los estudios de eficacia de los costes;
- la identificación de los riesgos que impactan en las fases siguientes del ciclo de vida.

A medida que avanza la actividad, la apreciación del riesgo se puede utilizar para proporcionar información que ayude a desarrollar procedimientos para condiciones normales y de emergencia.

6.7 Tipos de técnicas de apreciación del riesgo

Las técnicas de apreciación del riesgo se pueden clasificar de varias maneras para ayudar a comprender sus cualidades relativas de solidez y de debilidad. A efectos ilustrativos, las tablas del anexo A relacionan algunas técnicas posibles y sus categorías.

Además, cada una de las técnicas se desarrolla en el anexo B según la naturaleza de la apreciación que proporcionan, y se dan directrices para su aplicabilidad para determinadas situaciones.

ANEXO A (Informativo)**COMPARACIÓN DE TÉCNICAS DE APRECIACIÓN DEL RIESGO****A.1 Tipos de técnicas**

La primera clasificación muestra cómo se aplican las técnicas en cada etapa del proceso de apreciación del riesgo, como sigue:

- identificación del riesgo;
- análisis del riesgo – análisis de las consecuencias;
- análisis del riesgo – estimación de la probabilidad cualitativa, semicuantitativa o cuantitativa;
- análisis del riesgo – evaluación de la eficacia de todos los controles existentes;
- análisis del riesgo – estimación del nivel de riesgo;
- evaluación del riesgo.

Para cada etapa del proceso de apreciación del riesgo, la aplicación del método se describe como muy aplicable, aplicable o no aplicable (véase la tabla A.1).

A.2 Factores que influyen en la selección de las técnicas de apreciación del riesgo

A continuación se describen los atributos de los métodos, en función de:

- la complejidad del problema y de los métodos que se necesitan para analizarlo;
- la naturaleza y el grado de incertidumbre de la apreciación del riesgo, basados en la cantidad de información disponible y que se requiere para satisfacer los objetivos;
- la amplitud de los recursos requeridos en función del tiempo y del nivel de conocimientos técnicos, de las necesidades de datos o de los costes;
- si el método puede proporcionar un resultado cuantitativo.

En la tabla A.2 se relacionan ejemplos de tipos de métodos de apreciación del riesgo disponibles, donde cada método se clasifica como alto, medio, o bajo en función de estos atributos.

Tabla A.1 – Aplicabilidad de las herramientas utilizadas para la apreciación del riesgo

Herramientas y técnicas	Proceso de apreciación del riesgo					Véase el capítulo
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Tormenta de ideas	MA ¹⁾	NA ²⁾	NA	NA	NA	B 01
Entrevistas estructuradas o semiestructuradas	MA	NA	NA	NA	NA	B 02
Delphi	MA	NA	NA	NA	NA	B 03
Listas de verificación	MA	NA	NA	NA	NA	B 04
Análisis preliminar de peligros	MA	NA	NA	NA	NA	B 05
Estudios de peligros y de operatividad (HAZOP)	MA	MA	A ³⁾	A	A	B 06
Análisis de peligros y puntos de control críticos (HACCP)	MA	MA	NA	NA	MA	B 07
Apreciación de riesgos ambientales	MA	MA	MA	MA	MA	B 08
Estructura «y si...» (SWIFT)	MA	MA	MA	MA	MA	B 09
Análisis de escenario	MA	MA	A	A	A	B 10
Análisis del impacto económico	A	MA	A	A	A	B 11
Análisis de la cauMA primordial	NA	MA	MA	MA	MA	B 12
Análisis de los modos de fallo y de los efectos	MA	MA	MA	MA	MA	B 13
Análisis del árbol de fallos	A	NA	MA	A	A	B 14
Análisis del árbol de sucesos	A	MA	A	A	NA	B 15
Análisis de cauMA-consecuencia	A	MA	MA	A	A	B 16
Análisis de cauMA-y-efecto	MA	MA	NA	NA	NA	B 17
Análisis de capas de protección (LOPA)	A	MA	A	A	NA	B 18
Diagrama de decisiones	NA	MA	MA	A	A	B 19
Análisis de fiabilidad humana	MA	MA	MA	MA	A	B 20
Análisis de pajarita	NA	A	MA	MA	A	B 21
Mantenimiento centrado en la fiabilidad	MA	MA	MA	MA	MA	B 22
Análisis del circuito de fuga	A	NA	NA	NA	NA	B 23
Análisis Markov	A	MA	NA	NA	NA	B 24
Simulación Monte-Carlo	NA	NA	NA	NA	MA	B 25
Estadísticas Bayesian y redes Bayes	NA	MA	NA	NA	MA	B 26
Curvas FN	A	MA	MA	A	MA	B 27
Índices de riesgo	A	MA	MA	A	MA	B 28
Matriz de consecuencia/probabilidad	MA	MA	MA	MA	A	B 29
Análisis de costes/beneficios	A	MA	A	A	A	B 30
Análisis de decisión multi-criterios (MCDA)	A	MA	A	MA	A	B 31

1) Muy aplicable.

2) No aplicable.

3) Aplicable.

Tabla A.2 – Atributos de una selección de herramientas para la apreciación del riesgo

Tipo de técnica de apreciación del riesgo	Descripción	Importancia de los factores que influyen			¿Puede proporcionar resultados cuantitativos?
		Recursos y capacidades	Naturaleza y grado de la incertidumbre	Complejidad	
MÉTODOS DE BÚSQUEDA					
Listas de verificación	Una forma sencilla de apreciación del riesgo. Una técnica que proporciona una lista de incertidumbres típicas que es necesario tener en consideración. Los usuarios pueden consultar listas, códigos o normas previamente desarrolladas.	Bajo	Bajo	Baja	No
Análisis preliminar de riesgos	Un método inductivo sencillo de análisis cuyo objetivo es identificar los riesgos y situaciones de riesgo y los sucesos que pueden causar daños en una determinada actividad, instalación o sistema.	Bajo	Alto	Media	No
MÉTODOS DE APOYO					
Entrevista estructurada y tormenta de ideas	Un medio de recopilación de un amplio conjunto de ideas y evaluación, que luego es clasificado por un equipo de personas. La tormenta de ideas se puede estimular mediante proposiciones o técnicas de entrevistas uno con uno o uno con varios.	Bajo	Bajo	Baja	No
Técnica Delphi	Un medio de combinar las opiniones de expertos que puede apoyar la identificación del origen y de la influencia, la estimación de la probabilidad y de la consecuencia, así como la evaluación del riesgo. Es una técnica de colaboración para crear el consenso entre expertos. Implica el análisis independiente y la votación de los expertos.	Medio	Medio	Media	No
SWIFT estructurado ("¿y si...?")	Un sistema para ayudar a un equipo de personas en la identificación de riesgos. Normalmente se utiliza dentro de un taller de trabajo dirigido. Por lo general está relacionado con una técnica de análisis y de evaluación del riesgo.	Medio	Medio	Alguna	No
Análisis de fiabilidad humana (HRA)	La apreciación de la fiabilidad humana (HRA) trata acerca del impacto del personal sobre el rendimiento del sistema, y se puede utilizar para evaluar la influencia de los errores humanos sobre el sistema.	Medio	Medio	Media	Sí
ANÁLISIS DE ESCENARIO					
Análisis de la causa primordial (análisis de daño único)	Un daño único que ha ocurrido, se analiza con objeto de comprender las causas que han contribuido a que se produzca, y cómo se puede mejorar el sistema o el proceso para evitar estos daños futuros. El análisis debe considerar los controles que estaban establecidos en el momento de producirse el daño, así como la manera en que se podrían mejorar los controles.	Medio	Bajo	Media	No

Tipo de técnica de apreciación del riesgo	Descripción	Importancia de los factores que influyen			¿Puede proporcionar resultados cuantitativos?
		Recursos y capacidades	Naturaleza y grado de la incertidumbre	Complejidad	
Análisis de escenario	Los posibles escenarios futuros se identifican por imaginación o por extrapolación a partir de riesgos presentes y diferentes, considerados asumiéndose que se podrían presentar en cada uno de estos escenarios. Esto se puede hacer formal o informalmente, cualitativa o cuantitativamente.	Medio	Alto	Media	No
Apreciación de riesgo toxicológico	Los peligros se identifican y analizan, y también se identifican los posibles caminos por los que el modelo especificado se podría exponer al peligro. La información sobre el nivel de exposición y la naturaleza del daño causado para un nivel dado de exposición se combinan para dar una medida de la probabilidad de que ocurra el daño especificado.	Alto	Alto	Media	Sí
Análisis del impacto en el negocio	Proporciona un análisis de cómo los riesgos de disrupción clave podrían afectar a las operaciones de una organización, e identifica y cuantifica las capacidades que se necesitarían para gestionarlos.	Medio	Medio	Media	No
Análisis del árbol de fallos	Una técnica que comienza con un suceso no deseado (suceso superior) y determina todos los caminos por los que podría ocurrir. Estos se representan gráficamente en un diagrama lógico. Una vez desarrollado el árbol de fallos, se deben tener en consideración los caminos para reducir o eliminar las posibles causas u orígenes del suceso.	Alto	Alto	Media	Sí
Análisis del árbol de sucesos	Se aplican razonamientos inductivos para determinar las probabilidades de que se inicien diferentes sucesos con sus posibles efectos.	Medio	Medio	Media	Sí
Análisis de causa y consecuencia	Una combinación de los análisis del árbol de fallos y del árbol de sucesos que permite la inclusión de demoras de tiempo. Se consideran tanto las causas como las consecuencias de la iniciación de un suceso.	Alto	Medio	Alta	Sí
Análisis de causa-y-efecto	Los diversos factores que contribuyen a que se produzca un efecto se pueden agrupar en diferentes categorías. Con frecuencia, estos factores contributivos se identifican a través de la tormenta de ideas y se representa mediante una estructura en árbol o de espina de pescado "Fishbone"	Bajo	Bajo	Media	No

Ejemplo del tipo de método y técnica de apreciación del riesgo	Descripción	Importancia de los factores que influyen			¿Posibles resultados cuantitativos?
ANÁLISIS FUNCIONAL					
FMEA y FMECA	<p>FMEA (Failure Mode and Effect Análisis - Análisis del modo de fallo y de los efectos) es una técnica que identifica los modos y mecanismos de fallo, y sus efectos.</p> <p>Existen varios tipos de análisis FMEA: FMEA del Diseño (o del producto), que se aplica a componentes y a productos; FMEA del Sistema, que se aplica a sistemas; FMEA del Proceso, que se aplica a procesos de fabricación y de montaje; FMEA del Servicio y FMEA del Software.</p> <p>El FMEA puede ir seguido por un análisis de criticidad que defina la importancia de cada modo de fallo de forma cualitativa, semicuantitativa o cuantitativa (FMECA). El análisis de criticidad se puede basar en la probabilidad de que el modo de fallo provocará el fallo del sistema, o en el nivel de riesgo asociado al modo de fallo, o en un número de prioridad del riesgo.</p>	Medio	Medio	Media	Sí
Mantenimiento centrado en la fiabilidad	Un método para identificar las políticas que se deberían implantar para gestionar los fallos, a fin de conseguir eficaz y acertadamente la seguridad, la disponibilidad y la economía de funcionamiento requeridas en todos los tipos de equipos.	Medio	Medio	Media	Sí
Análisis de fugas "sneak" (Análisis del circuito de fugas)	Una metodología para identificar errores de diseño. Una condición de fuga es una condición latente en el hardware o en el software o una condición integrada que puede originar un suceso no deseado o que puede inhibir un suceso deseado que no es causado por fallo de un componente. Estas condiciones se caracterizan por su naturaleza aleatoria y por la facilidad de evadir la detección durante los ensayos más rigurosos de sistemas normalizados. Las condiciones de fuga puedan causar un funcionamiento inadecuado, la pérdida de disponibilidad del sistema, demoras en el programa, o incluso lesiones o la muerte de personas.	Medio	Medio	Media	No
HAZOP Análisis de riesgos y de operatividad	<p>Un proceso general de identificación del riesgo para definir posibles desviaciones con respecto al rendimiento esperado o previsto. Este proceso utiliza una palabra guía basada en el sistema.</p> <p>Se evalúan las criticidades de las desviaciones.</p>	Medio	Alto	Alta	No
HACCP Análisis de peligros y puntos de control críticos	Un sistema metódico, pro-activo y preventivo para asegurar la calidad del producto, y la fiabilidad y seguridad de los procesos, mediante la medición y seguimiento de las características específicas que se requieren que estén dentro de unos límites definidos.	Medio	Medio	Media	No

Ejemplo del tipo de método y técnica de apreciación del riesgo	Descripción	Importancia de los factores que influyen			¿Posibles resultados cuantitativos?
APRECIACIÓN DE LOS CONTROLES					
LOPA (Análisis de niveles de protección)	(También se puede denominar análisis de barrera). Permite evaluar los controles y la eficacia de éstos.	Medio	Medio	Media	Si
Análisis pajarita	Un medio diagramático sencillo para describir y analizar los caminos de un riesgo, desde los peligros hasta los efectos, incluyendo la revisión de los controles. Se puede considerar que es una combinación de la lógica de un árbol de fallos que analiza las causas de un suceso (representado por el nudo de una corbata de pajarita) y de un árbol de sucesos que analiza las consecuencias.	Medio	Alto	Media	Si
MÉTODOS ESTADÍSTICOS					
Análisis Markov	El análisis Markov, a veces llamado análisis <i>estado-espacio</i> , se utiliza comúnmente para analizar sistemas complejos reparables que pueden existir en múltiples estados, incluidos distintos estados degradados.	Alto	Bajo	Alta	Si
Simulación Monte-Carlo	La simulación Monte-Carlo se utiliza para establecer la variación agregada en un sistema, resultante de diversas variaciones del sistema, para un determinado número de entradas de datos, donde cada entrada tiene una distribución definida y las entradas están relacionadas con las salidas de datos a través de relaciones definidas. La simulación se puede aplicar para un modelo específico donde las interacciones de las diversas entradas se pueden definir matemáticamente. Las entradas se pueden basar en una variedad de tipos de distribución de acuerdo con la naturaleza de la incertidumbre que tales entradas están destinadas a representar. Para la apreciación del riesgo, se utilizan normalmente distribuciones triangulares o distribuciones beta.	Alto	Bajo	Alta	Si
Análisis Bayesian	Un procedimiento estadístico que utiliza datos de la distribución previa para determinar la probabilidad del resultado. El análisis Bayesian depende de la precisión de la distribución previa para deducir un resultado exacto. El modelo causa-y-efecto de las redes Bayesian establece una variedad de dominios mediante la captura de relaciones probabilísticas de entradas de datos variables para obtener un resultado.	Alto	Bajo	Alta	Si

ANEXO B (Informativo)**TÉCNICAS DE APRECIACIÓN DEL RIESGO****B.1 Tormenta de ideas****B.1.1 Presentación**

La tormenta de ideas implica el estímulo y el fomento de conversaciones fluidas entre un grupo de personas competentes, con objeto de identificar los posibles modos de fallo y los peligros asociados, los riesgos, los criterios para la toma de decisiones, y/o las opciones de tratamiento. El término "tormenta de ideas" se utiliza frecuentemente de forma muy imprecisa cuando se aplica a cualquier tipo de debate en grupo. Sin embargo, la tormenta de ideas verdadera implica técnicas particulares para tratar de garantizar que se fuerza la imaginación de las personas mediante las ideas y declaraciones de otras personas del grupo.

En esta técnica es muy importante la facilitación eficaz e incluye la estimulación del debate desde el principio, las indicaciones periódicas del grupo sobre otras áreas importantes, y la aceptación de los resultados obtenidos en el debate (que normalmente suele ser bastante animado).

B.1.2 Utilización

La tormenta de ideas se puede utilizar conjuntamente con otros métodos de apreciación del riesgo que se describen más adelante, o se puede utilizar como una técnica independiente para estimular pensamientos imaginativos en cualquier etapa del proceso de gestión del riesgo y en cualquier etapa del ciclo de vida de un sistema. Se puede utilizar para discusiones de alto nivel cuando las salidas están identificadas, para una revisión más detallada o para un nivel detallado de problemas particulares.

La tormenta de ideas obliga a poner un énfasis especial sobre la imaginación. Por ello, es particularmente útil cuando se identifican riesgos de una nueva tecnología, cuando no existen datos, o cuando se necesitan soluciones nuevas para los problemas.

B.1.3 Elementos de entrada

Un grupo de personas con conocimientos de la organización, del sistema, del proceso o de la aplicación que se está sometiendo a apreciación.

B.1.4 Proceso

La tormenta de ideas puede ser formal o informal. La tormenta de ideas formal está más estructurada con participantes preparados con antelación, y la sesión tiene una finalidad y unos resultados definidos con un medio de evaluar ideas avanzadas. La tormenta de ideas informal es menos estructurada y con frecuencia está más destinada a un caso específico.

En un proceso formal:

- el coordinador prepara las propuestas de las opiniones e inicia las acciones apropiadas al contexto antes de la sesión;
- se definen los objetivos de la sesión y se explican las reglas a seguir;
- el coordinador expone una serie de ideas y todas las personas las examinan y las identifican con todos los asuntos posibles. En este punto no se discute si los proyectos deberían estar o no en una lista, o con respecto a lo que significan las declaraciones particulares debido a que esto tiende a inhibir lo que se considera una idea fluida de la sesión. Se aceptan todas las entradas y ninguna se censura, y el grupo decide rápidamente para permitir opiniones laterales;

- el coordinador puede exponer a los asistentes una nueva pista cuando se agota la idea en una dirección, o el debate se desvía demasiado de su objetivo. No obstante, la idea se recoge al igual que muchas otras para un posterior análisis.

B.1.5 Resultados

Los resultados dependen de la etapa del proceso de gestión del riesgo en la que se aplica. Por ejemplo, en la etapa de identificación, las salidas pueden ser una lista de riesgos y de controles actuales.

B.1.6 Fortalezas y limitaciones

Las fortalezas de la tormenta de ideas incluyen:

- estimular la imaginación, lo cual ayuda a identificar nuevos riesgos y soluciones novedosas;
- implica a las principales partes interesadas, y por tanto ayuda a la comunicación global;
- es relativamente rápida y fácil de establecer.

Las limitaciones incluyen:

- los participantes pueden carecer de los conocimientos técnicos y de otros tipos necesarios para ser colaboradores eficaces;
- dado que está relativamente poco estructurada, es difícil demostrar que se ha completado el proceso, por ejemplo, que se han identificado todos los riesgos potenciales;
- puede suceder que un grupo particular, en el que haya algunas personas con ideas valiosas permanezca tranquilo, mientras otras personas dominan el debate. Esto se puede superar mediante tormenta de ideas informáticas, utilizando un foro de charla a través de ordenadores o una técnica de grupo nominal. La tormenta de ideas por ordenador se puede establecer de manera que sea anónima, con lo cual se evitan los temas personales y políticos que pueden impedir el libre intercambio de ideas. En la técnica de grupo nominal, las ideas se envían de forma anónima a un moderador y después son discutidas por el grupo.

B.2 Entrevistas estructuradas o semiestructuradas

B.2.1 Presentación

En una entrevista estructurada, los entrevistados son sometidos a un conjunto de preguntas preparadas a partir de una hoja de indicaciones, que estimulan al entrevistado a ver la situación desde una perspectiva diferente y por tanto a identificar los riesgos desde esta perspectiva. Una entrevista semiestructurada es similar, pero permite más libertad para mantener una conversación con objeto de examinar los temas a tratar.

B.2.2 Utilización

Las entrevistas estructuradas y semiestructuradas son útiles cuando es difícil reunir a las personas para una sesión de tormenta de ideas o cuando un debate fluido en grupo no es apropiada para la situación o para las personas implicadas. Estas entrevistas se utilizan frecuentemente para identificar riesgos o para apreciar la eficacia de los controles existentes como parte del análisis del riesgo. Se pueden realizar en cualquier etapa de un proyecto o proceso. Constituyen un medio de proporcionar una entrada para la apreciación del riesgo a las partes interesadas.

B.2.3 Elementos de entrada

Las entradas incluyen:

- una definición clara de los objetivos de las entrevistas;
- una lista de entrevistados que se seleccionan de las partes interesadas pertinentes;
- un conjunto de preguntas preparadas.

B.2.4 Proceso

Se establece un conjunto de preguntas pertinentes para que sirva de guía al entrevistador. Siempre que sea posible, las preguntas deberían ser abiertas y concretas, sencillas, formuladas en un lenguaje apropiado al entrevistado, y relacionadas únicamente con un asunto. También se deben preparar las posibles preguntas de seguimiento para obtener aclaraciones.

Las preguntas se formulan entonces a la persona que está siendo entrevistada. Cuando se elaboran las preguntas de seguimiento, éstas deberían ser abiertas y concretas. Se debería tener cuidado con no "influnciar" al entrevistado.

Las respuestas se deberían considerar con cierto grado de flexibilidad, a fin de dar la oportunidad de que se exploren áreas en las que el entrevistado quiera entrar.

B.2.5 Resultados

Los resultados son las opiniones de las partes interesadas sobre los asuntos que se han debatido.

B.2.6 Fortalezas y limitaciones

Las fortalezas de las entrevistas estructuradas son los siguientes:

- las entrevistas estructuradas dan tiempo a las personas para que consideren la idea sobre un asunto;
- las comunicaciones uno a uno pueden permitir una consideración más profunda de los asuntos;
- las entrevistas estructuradas permiten la implicación de un mayor número de partes interesadas que la técnica de tormenta de ideas, que solo utiliza un grupo relativamente pequeño.

Las limitaciones son las siguientes:

- el tiempo que emplea el coordinador para obtener las múltiples opiniones de los entrevistados;
- la desviación se tolera y no se elimina a través del debate en grupo;
- es posible que no se consiga la provocación de la imaginación, que es una característica de la técnica de tormenta de ideas.

B.3 Técnica Delphi

B.3.1 Presentación

La técnica Delphi es un procedimiento para obtener un consenso fiable de la opinión de un grupo de expertos. Aunque el término se utiliza ahora ampliamente para significar alguna forma de tormenta de ideas, una característica esencial de la técnica Delphi, formulada originalmente, fue que los expertos expresaron sus opiniones de forma individual y anónima, mientras que el acceso a las opiniones de los otros expertos lo tenían a medida que el proceso avanzaba.

B.3.2 Utilización

La técnica Delphi se puede aplicar en cualquier etapa del proceso de gestión del riesgo o en cualquier fase del ciclo de vida de un sistema, dondequiera se necesite el consenso de las opiniones de los expertos.

B.3.3 Elemento de entrada

Un conjunto de opciones para el que se necesita el consenso.

B.3.4 Proceso

Mediante un cuestionario semiestructurado se realizan preguntas a un grupo de expertos. Los expertos no se reúnen con objeto de que sus opiniones sean independientes.

Este procedimiento consiste en lo siguiente:

- la formación de un grupo de trabajo para llevar a cabo y realizar el seguimiento el proceso Delphi;
- la selección de un grupo de expertos (puede haber uno o varios paneles de expertos);
- el desarrollo de la primera ronda del cuestionario;
- el ensayo del cuestionario;
- el envío del cuestionario individualmente a cada uno de los miembros del grupo;
- la información de la primera ronda de respuestas se analiza y combina y se redistribuye a los miembros del grupo;
- los miembros del grupo responden y se repite el proceso hasta que se consigue el consenso.

B.3.5 Resultados

La convergencia hacia el consenso sobre el asunto que se está tratando.

B.3.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- como los puntos de vista son anónimos, las opiniones impopulares se expresan con más libertad;
- todos los puntos de vista tienen la misma importancia, lo que evita el problema de personalidades dominantes;
- se consigue la posesión de los resultados;
- no es necesario que las personas se reúnan en un lugar y a una hora determinada.

Las limitaciones incluyen:

- es una labor intensa y que consume tiempo;
- los participantes necesitan ser capaces de expresarse por sí mismos por escrito y de forma clara.

B.4 Listas de verificación

B.4.1 Presentación

Las listas de verificación son listas de peligros, riesgos o fallos de control que se han desarrollado generalmente a partir de la experiencia como resultado de una apreciación previa del riesgo o como resultado de fallos ocurridos en el pasado.

B.4.2 Utilización

Las listas de verificación se pueden utilizar para identificar peligros y riesgos o para valorar la eficacia de los controles. Se pueden utilizar en cualquier etapa del ciclo de vida de un producto, proceso o sistema. También se pueden utilizar como parte de otras técnicas de apreciación del riesgo, pero son más útiles cuando se aplican para comprobar que se ha cubierto todo el sistema después de que se haya aplicado una técnica más imaginativa que identifique problemas nuevos.

B.4.3 Elementos de entrada

Se puede seleccionar o desarrollar la información previa y los conocimientos técnicos del asunto, tal como una lista de verificación aplicable y validada preferentemente.

B.4.4 Proceso

El proceso es el siguiente:

- se define el campo de aplicación de la actividad;
- se selecciona una lista de verificación que cubra adecuadamente el campo de aplicación. Las listas de verificación se deben seleccionar cuidadosamente para el fin al que van destinadas. Por ejemplo, una lista de verificación de controles normalizados no se puede utilizar para identificar peligros o riesgos nuevos;
- la persona o el grupo de trabajo va siguiendo los pasos de la lista de verificación a través de cada elemento del proceso o sistema y revisa si los puntos de la lista de verificación son correctos.

B.4.5 Resultados

Los resultados dependen de la etapa del proceso de gestión del riesgo en que se apliquen. Por ejemplo, el resultado puede ser una lista de controles que son inadecuados o una lista de riesgos.

B.4.6 Fortalezas y limitaciones

Las fortalezas de las listas de verificación incluyen:

- pueden ser utilizadas por personas no expertas;
- cuando están bien diseñadas combinan una amplia gama de conocimientos técnicos que son fáciles de utilizar;
- pueden ayudar a asegurar que no se olvidan problemas comunes.

Las limitaciones incluyen:

- tienden a inhibir la imaginación en la identificación de riesgos;
- se dirigen hacia lo "conocido de lo conocido", y no hacia lo "desconocido de lo conocido" o a lo "desconocido de lo desconocido";
- estimulan el comportamiento de tipo "marcar lo comprobado";
- tienden a estar basadas en la observación, por lo que se pasan por alto problemas que se han visto rápidamente.

B.5 Análisis preliminar de peligros (PHA)

B.5.1 Presentación

El PHA es un método sencillo e inductivo de análisis cuyo objetivo consiste en identificar los peligros y las situaciones peligrosas, así como los sucesos que pueden causar daño a una actividad, instalación o sistema dados.

B.5.2 Utilización

Es el análisis que más se utiliza normalmente al comienzo del desarrollo de un proyecto, cuando se dispone de poca información sobre los detalles del diseño o sobre los procedimientos de funcionamiento, y con frecuencia puede ser un precursor de estudios adicionales o proporcionar información para la especificación del diseño de un sistema. También puede ser útil cuando se analizan sistemas existentes, a fin de priorizar peligros y riesgos para análisis posteriores o cuando las circunstancias impiden aplicar una técnica más extensiva que la que se está utilizando.

B.5.3 Elementos de entrada

Los elementos de entrada incluyen:

- la información sobre el sistema que se va a apreciar;
- detalles del diseño del sistema que estén disponibles y sean pertinentes.

B.5.4 Proceso

Se formula una lista de peligros y situaciones peligrosas genéricas y de riesgos, teniendo en consideración características tales como:

- los materiales utilizados o producidos y la reactividad de los mismos;
- los equipos utilizados;
- el entorno ambiental de funcionamiento;
- la disposición de conjunto;
- las interfaces entre componentes del sistema, etc.

Con objeto de identificar riesgos para la posterior apreciación de los mismos, se puede realizar un análisis cualitativo de las consecuencias de un suceso no deseado y de sus probabilidades de que ocurra.

El PHA se debería actualizar durante las fases de diseño, fabricación y ensayo, con objeto de detectar cualquier nuevo peligro y poder realizar correcciones, si fuese necesario. Los resultados obtenidos se pueden presentar en diferentes formas, tales como tablas y diagramas en árbol.

B.5.5 Resultados

Los resultados incluyen:

- una lista de peligros y riesgos;
- recomendaciones acerca de la forma de aceptación, de los controles recomendados, de las especificaciones o requisitos de diseño para una apreciación más detallada.

B.5.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- que se puede utilizar cuando la información existente es limitada;
- permite considerar los riesgos con mucha antelación en el ciclo de vida del sistema.

Las limitaciones incluyen:

- un PHA solo proporciona información preliminar; no es completa ni proporciona información detallada sobre los riesgos ni de cómo se pueden prevenir de la mejor manera posible.

B.6 HAZOP (Análisis de riesgos y de operatividad)

B.6.1 Presentación

HAZOP es el acrónimo del análisis de riesgos (**HAZ**ard) y de operatividad (**OP**erability), que consiste en un examen estructurado y sistemático de un producto, proceso, procedimiento o sistema existente o planificado. El HAZOP es una técnica para identificar riesgos para las personas, los equipos, el entorno y/o los objetivos de la organización. También se espera que, cuando sea posible, el grupo de trabajo proporcione una solución para el tratamiento del riesgo.

El proceso HAZOP es una técnica cualitativa basada en la utilización de palabras guía que cuestionan cómo la intención del diseño o las condiciones de funcionamiento podrían no alcanzarse en cada paso del diseño, proceso, procedimiento o sistema. Normalmente lo realiza un grupo de trabajo multidisciplinar durante una serie de reuniones.

El HAZOP es similar al FMEA (análisis del modo de fallo y del efecto) en cuanto a que identifica los modos de fallo de un proceso, sistema o procedimiento, sus causas y sus consecuencias. Difiere en cuanto a que el grupo de trabajo tiene en consideración los resultados no deseados y las desviaciones con respecto a los resultados previstos, y las condiciones y los trabajos se repiten para localizar las causas posibles y los modos de fallo, mientras que el FMEA comienza identificando los modos de fallo.

B.6.2 Utilización

La técnica HAZOP se desarrolló inicialmente para analizar sistemas de procesos químicos, pero después se ha ampliado a otros tipos de sistemas y operaciones complejas. En estos se incluyen sistemas y procedimientos mecánicos y electrónicos, y sistemas de software, e incluso cambios organizacionales y modelos y revisiones de los contratos legales.

El proceso HAZOP puede tratar todas las formas de desviación respecto al diseño previsto debidas a deficiencias en el diseño, en los componentes, en los procedimientos planificados y en las acciones humanas.

Este proceso es muy utilizado para revisar los diseños de software. Cuando se aplica al control de instrumentos críticos de seguridad y a sistemas informáticos se puede conocer como CHAZOP (*Control **HAZ**ards and **OP**erability Analysis* o *computer hazard and operability analysis*) (análisis para control de riesgos y de operatividad o análisis de riesgos y operatividad informática).

Normalmente, un estudio HAZOP se realiza en la etapa de diseño en detalle, cuando se dispone de un diagrama completo del proceso previsto, pero mientras los cambios de diseño aún son practicables. No obstante, el estudio se puede realizar con un enfoque por fases con diferentes palabras guía para cada etapa, a medida que el diseño se desarrolla en detalle. Un estudio HAZOP también se puede realizar durante la fase de funcionamiento, pero los cambios que se requieren en esta etapa pueden ser muy costosos.

B.6.3 Elementos de entrada

Los elementos de entrada esenciales para un estudio HAZOP incluyen la información real sobre el sistema, el proceso o procedimiento a revisar, y las intenciones y las especificaciones de funcionamiento del diseño. Los elementos de entrada pueden incluir: planos, hojas de especificaciones, diagramas de flujo, diagramas lógicos y de control de proceso, planos de implantación, procedimientos de funcionamiento y de mantenimiento, y procedimientos de respuestas de emergencia. Para los estudios HAZOP que no estén relacionados con software, los elementos de entrada pueden ser cualquier documento que describa las funciones y los elementos del sistema o procedimiento que se está estudiando. Por ejemplo, los elementos de entrada pueden ser diagramas organizacionales y descripciones de funciones, un proyecto de contrato e incluso un proyecto de procedimiento.

B.6.4 Proceso

Un estudio HAZOP toma el "diseño" y las especificaciones del proceso, procedimiento o sistema que se está estudiando y revisa cada una de sus partes para descubrir las desviaciones que se pueden producir con respecto al funcionamiento previsto, cuales son las causas potenciales y cuales las consecuencias probables de una desviación. Esto se consigue mediante el examen sistemático de cómo cada parte del sistema, proceso o procedimiento responderá a los cambios en los parámetros claves utilizando palabras guía adecuadas. Las palabras guía se pueden personalizar para un sistema, proceso o procedimiento particular, o se pueden utilizar palabras guía genéricas que sirvan para todos los tipos de desviaciones. La tabla B.1 proporciona ejemplos de palabras guía que se utilizan normalmente en sistemas técnicos. Para identificar modos de errores humanos se pueden utilizar palabras guía similares, tales como "demasiado pronto", "demasiado tarde", "demasiado", "demasiado pequeño", "demasiado grande", "demasiado corto", "dirección errónea", "objeto erróneo" y "acción errónea".

Los pasos normales de un estudio HAZOP incluyen:

- el nombramiento de una persona que tenga la responsabilidad y la autoridad necesarias para dirigir el estudio HAZOP y para garantizar que se completarán todas las acciones que se deriven del estudio;
- la definición de los objetivos y del campo de aplicación del estudio;
- el establecimiento de un conjunto de claves o palabras guía para el estudio;
- la definición de un grupo de trabajo para el estudio HAZOP; generalmente, este grupo de trabajo es multidisciplinar y debería incluir personal de diseño y de operaciones que tengan los conocimientos técnicos apropiados para evaluar los efectos de las desviaciones con respecto al diseño previsto o real. Se recomienda que el grupo de trabajo incluya personas que no estén implicadas directamente en el diseño del sistema, proceso o procedimiento que se somete a revisión;
- la recopilación de la documentación que se requiere.

Dentro de una reunión de trabajo facilitada con el grupo de trabajo para el estudio:

- dividir el sistema, proceso o procedimiento en elementos, subsistemas, subprocesos o subelementos más pequeños para hacer posible la revisión;
- acordar el diseño previsto para cada subsistema, subproceso o subelemento y después para cada artículo en este subsistema o elemento aplicando las palabras guía una a continuación de la otra para postular las posibles desviaciones que tendrán resultados indeseables;
- cuando se identifique un resultado indeseable, acordar la causa y las consecuencias en cada caso y sugerir la forma en que se podría tratar para impedir que ocurra o para mitigar las consecuencias si se produce;
- documentar el debate y el acuerdo de las acciones específicas para tratar los riesgos identificados.

Tabla B.1 – Ejemplos de posibles palabras guía HAZOP

Términos	Definiciones
No o ninguna	No se consigue ninguna parte del resultado previsto o la condición prevista no existe
Más (más alta)	Aumento cuantitativo en la salida o en la condición de funcionamiento
Menos (más baja)	Disminución cuantitativa
Así como	Aumento cuantitativo (por ejemplo, material adicional)
Parte de	Disminución cuantitativa (por ejemplo, solo uno o dos componentes en una mezcla)
Inverso/opuesto	Opuesto (por ejemplo, reflujo)
Distinta de	No se consigue ninguna parte de la intención, algunas veces ocurre algo completamente diferente (por ejemplo, flujo o material erróneo)
Compatibilidad	Material, entorno ambiental
Se aplican palabras guía a parámetros tales como:	
	Propiedades físicas de un material o proceso
	Condiciones físicas tales como temperatura, velocidad
	Una intención especificada de un componente de un sistema o diseño (por ejemplo, transferencia de información)
	Aspectos operacionales

B.6.5 Resultados

Las actas de las reuniones HAZOP con los elementos de cada punto de revisión registrado. Esto debería incluir: la palabra guía utilizada, la desviación o desviaciones ocurridas, las causas posibles, las acciones encaminadas a los problemas identificados y la persona responsable de cada acción.

Para cualquier desviación que no se pueda corregir, se debería someter a apreciación el riesgo debido a la desviación.

B.6.6 Fortalezas y limitaciones

El análisis HAZOP ofrece las siguientes ventajas:

- proporciona el medio para examinar de manera sistemática y total un sistema, proceso o procedimiento;
- implica la existencia de un grupo de trabajo multidisciplinar que incluya personas con experiencia operacional en el ciclo de vida real y personas que pueden tener que realizar acciones de tratamiento;
- genera soluciones y acciones para el tratamiento del riesgo;
- es aplicable a una amplia gama de sistemas, procesos y procedimientos;
- permite la consideración explícita de las causas y de las consecuencias de errores humanos;
- crea un registro escrito del proceso que se puede utilizar para demostrar la diligencia necesaria.

Las limitaciones incluyen:

- un análisis detallado puede consumir mucho tiempo y, por tanto, puede resultar muy costoso económicamente;
- un análisis detallado requiere un alto nivel de documentación o de especificaciones del sistema/proceso y del procedimiento;
- se puede centrar en la búsqueda de soluciones detalladas en vez de hacer frente a suposiciones fundamentales (sin embargo, esto se puede mitigar mediante un enfoque por fases);
- el debate se puede centrar sobre asuntos detallados de diseño y no sobre asuntos más amplios o externos;
- está limitado por el diseño (proyecto) y el propósito del diseño, y por el campo de aplicación y los objetivos dados al grupo de trabajo;
- el proceso confía plenamente en los conocimientos técnicos de los diseñadores, que pueden encontrar dificultades para ser suficientemente objetivos para encontrar problemas en sus diseños.

B.6.7 Normas para consulta

IEC 61882, *Estudios de peligros y de operatividad (estudios HAZOP). Guía de aplicación.*

B.7 Análisis de riesgos y puntos de control críticos (HACCP)

B.7.1 Presentación

El análisis de riesgos y puntos de control críticos (HACCP) proporciona una estructura para la identificación de los riesgos y para establecer controles en todas las partes importantes de un proceso, a fin de protegerlo contra los riesgos y de mantener la fiabilidad y la seguridad de la calidad de un producto. El HACCP tiene por objeto asegurar que los riesgos se minimizan mediante controles a lo largo de todo el proceso, mejor que con una inspección del producto final.

B.7.2 Utilización

El HACCP se desarrolló para asegurar la calidad de los alimentos para los programas espaciales de la NASA. Ahora lo utilizan las organizaciones que funcionan dentro de la cadena alimenticia para controlar los riesgos debidos a los contaminantes físicos, químicos o biológicos de los alimentos. También se ha extendido su utilización en la fabricación de productos farmacéuticos y de productos sanitarios. Los principios para identificar artículos que pueden influir en la calidad del producto, y para definir puntos en un proceso donde puede realizarse el seguimiento de los parámetros críticos y los peligros se pueden controlar, se pueden generalizar para otros sistemas técnicos.

B.7.3 Elementos de entrada

El análisis HACCP se inicia a partir de un organigrama básico o un diagrama de proceso y de la información sobre los peligros que podrían afectar a la calidad, seguridad o fiabilidad de los resultados del producto o proceso. La información sobre los peligros y sus riesgos, así como de las maneras en que estos se pueden controlar constituye un elemento de entrada al análisis HACCP.

B.7.4 Proceso

El análisis HACCP está constituido por los siete principios siguientes:

- identificar los peligros y las medidas preventivas relativas a tales peligros;
- determinar los puntos del proceso donde los peligros se pueden controlar o eliminar (los puntos de control críticos o CCP);

- establecer los límites críticos necesarios para controlar los peligros, es decir, cada CCP debería funcionar dentro de parámetros específicos para asegurar que el peligro está controlado;
- hacer seguimiento de los límites críticos de cada CCP a intervalos definidos;
- establecer las acciones correctoras si el proceso se sale de los límites establecidos;
- establecer los procedimientos de verificación;
- implantar la preparación de registros y los procedimientos de documentación para cada etapa.

B.7.5 Resultados

Registros documentados que incluyan una ficha de trabajo del análisis del peligro y un plan HACCP.

La ficha de análisis del peligro registra para cada etapa del proceso:

- los peligros que se podrían introducir, controlar o empeorar en cada etapa;
- si los peligros presentan un riesgo importante (en base a la consideración de las consecuencias y de la probabilidad a partir de una combinación de experiencia, datos y documentación técnica);
- la justificación de la importancia;
- las posibles medidas preventivas para cada peligro;
- si las medidas de seguimiento y de control se pueden aplicar en esta etapa (es decir, ¿es un CCP?).

El plan HACCP delinea los procedimientos a seguir para asegurar el control de un diseño, producto, proceso o procedimiento específicos. El plan incluye una relación de todos los CCP, y para cada uno de ellos debe indicar:

- los límites críticos de las medidas preventivas;
- las actividades de seguimiento y de control (incluyendo porqué, cómo y cuándo se realizará el seguimiento y quién lo llevará a cabo);
- las acciones correctoras que se requieren si se detectan desviaciones con respecto a los límites críticos;
- las actividades de verificación y de conservación de registros.

B.7.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- un proceso estructurado que proporciona evidencias documentadas del control de calidad así como la identificación y reducción de riesgos;
- un enfoque sobre las posibilidades de cómo y cuando, en un proceso, se pueden prevenir los peligros y controlar los riesgos;
- la evidencia de que es mejor controlar el riesgo a lo largo de todo el proceso que dejarlo para la inspección del producto final;
- una aptitud para identificar los peligros introducidos a causa de acciones humanas y de cómo estas se pueden controlar en el punto de introducción o posteriormente.

Las limitaciones incluyen:

- el análisis HACCP requiere que se identifiquen los peligros, que se definan los riesgos que ellos representan, y que la importancia de los mismos se consideren como entradas al proceso. También es necesario definir los controles apropiados. Estos controles se requieren con objeto de especificar los puntos de control críticos y los parámetros de control durante el análisis HACCP, y puede ser necesario combinarlos con otras herramientas para conseguirlo;
- la toma de acciones cuando los parámetros de control exceden los límites definidos puede suponer la pérdida de la introducción de cambios graduales en los parámetros de control que son estadísticamente importantes y que por tanto se deberían actualizar.

B.7.7 Normas para consulta

ISO 22000, *Sistemas de gestión de la inocuidad de los alimentos. Requisitos para cualquier organización en la cadena alimentaria*

B.8 Apreciación de la toxicidad

B.8.1 Presentación

La apreciación de los riesgos ambientales se utiliza aquí para cubrir el proceso que se sigue en la apreciación de los riesgos a que se exponen las plantas, los animales y las personas como consecuencia de la exposición a una gama de peligros ambientales. La gestión del riesgo hace referencia a los pasos de toma de decisiones que incluyen la evaluación del riesgo y el tratamiento del riesgo.

El método a seguir implica analizar el peligro o el origen del daño, y en cómo este afecta a un modelo de población, así como los caminos por los cuales el peligro puede alcanzar a un modelo de población vulnerable. Esta información se combina entonces para dar una estimación de la probable amplitud y naturaleza del daño.

B.8.2 Utilización

Este proceso se utiliza para apreciar los riesgos en plantas, animales y personas, como consecuencia de la exposición a peligros tales como los originados por productos químicos, microorganismos u otras especies.

Los aspectos de la metodología, tales como el análisis de los caminos que exploran las diferentes rutas por las que un modelo de referencia se podría exponer a un origen de riesgo, se pueden adaptar y utilizar a través de una gama muy amplia de áreas de riesgo diferentes, fuera del contexto de la salud humana y del entorno ambiental, y es útil para identificar los tratamientos a seguir para reducir el riesgo.

B.8.3 Elementos de entrada

Este método requiere datos fiables sobre la naturaleza y las características de los peligros, la susceptibilidad del modelo de población (o de poblaciones), y la forma en que las dos reaccionan entre sí. Estos datos se basan normalmente en investigaciones que se realizan en laboratorio o se obtienen de estadísticas epidemiológicas.

B.8.4 Proceso

El procedimiento es el siguiente:

- a) Formulación del problema – esto incluye establecer el campo de aplicación de la apreciación mediante la definición de la variedad de modelos de población y los tipos de peligro de interés.
- b) Identificación del peligro – esto implica la identificación de todos los posibles orígenes de daño para el modelo de población a partir de los peligros incluidos dentro del campo de aplicación del estudio. La identificación del peligro depende normalmente de los conocimientos técnicos del experto y de la revisión de la documentación técnica.

- c) **Análisis del peligro** – esto implica la comprensión de la naturaleza del peligro y de cómo reacciona con el modelo de población. Por ejemplo, al considerar la exposición de personas a productos químicos, el peligro podría incluir una toxicidad aguda y crónica, el potencial de daños ADN, o la posibilidad de producir cáncer o taras de nacimiento. Para cada efecto peligroso, se compara la magnitud del efecto (la respuesta) con la cantidad de peligro al que se expone el modelo de población (la dosis) y, cuando sea posible, se determina el mecanismo por el que se produce el efecto. Se anotan los niveles en los que existen Efecto No Observable (NOEL) y Efectos Adversos No Observables (NOAEL). Dichos niveles se utilizan algunas veces como criterios de aceptabilidad del riesgo.

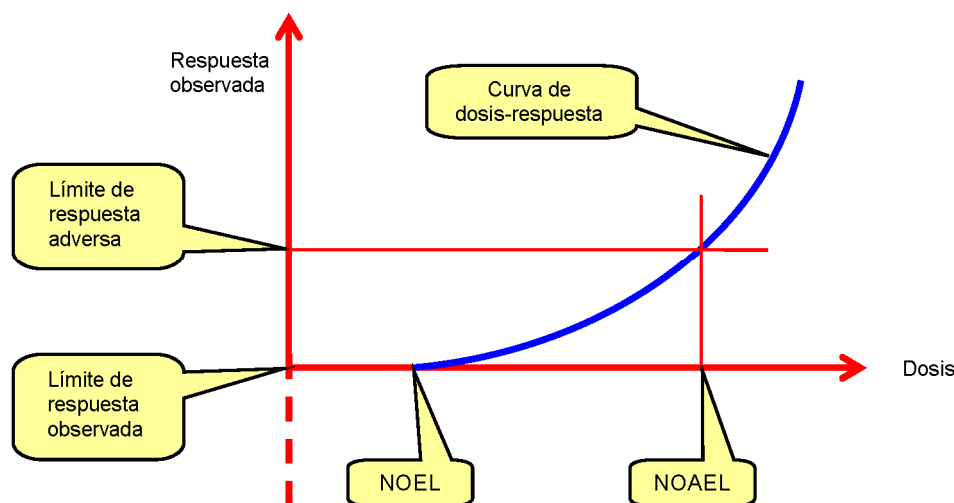


Figura B.1 – Curva de dosis-respuesta

Para la exposición a productos químicos, los resultados de los ensayos se utilizan para obtener las curvas de dosis-respuesta, tal como la mostrada esquemáticamente en la figura B.1. Normalmente, estas curvas se obtienen de ensayos sobre animales o a partir de sistemas experimentales, tales como cultivos de tejidos o de células.

Los efectos de otros peligros, tales como microorganismos o especies inoculadas, se pueden determinar a partir de los datos obtenidos de estudios de campo o epidemiológicos. Seguidamente se determina la naturaleza de la interacción de enfermedades o de plagas con el modelo de población y se estima la probabilidad de que se produzca un determinado nivel de daño como consecuencia de una exposición particular al peligro.

- d) **Análisis de la exposición** – en esta etapa se determina la manera y la cantidad en que una sustancia peligrosa o sus residuos podrían alcanzar a un modelo de población sensible. Con frecuencia, esto implica un análisis de vías de acceso que considere las diferentes rutas por las cuales el peligro podría aparecer, las barreras que podrían impedir que alcance al modelo de población y los factores que podrían influir en el nivel de exposición. Por ejemplo, considerando el riesgo debido a la pulverización de productos químicos, el análisis de la exposición consideraría la cantidad que se pulverizó, la forma y las condiciones en que se hizo, si hubo exposición directa de personas o animales, la cantidad que podría quedar como residuo en la vida de las plantas, el destino ambiental de los pesticidas que llegan al suelo, si se puede acumular en los animales y si entra en las aguas freáticas. En lo referente a la seguridad biológica, el análisis de las vías de acceso podría considerar la forma en que una plaga que entre en el país se podría transmitir al medio ambiente, establecerse y propagarse.
- e) **Caracterización del riesgo** – en esta etapa las informaciones obtenidas del análisis de los peligros y del análisis de la exposición se agrupan para estimar las probabilidades de que se produzcan consecuencias particulares cuando se combinan los efectos procedentes de todas las vías de acceso. Cuando existe un gran número de peligros o de vías de acceso, se puede realizar una selección inicial y después los análisis detallados de los peligros y de la exposición, y a continuación se lleva a cabo la caracterización del riesgo sobre los escenarios de alto riesgo.

B.8.5 Resultados

Por lo general, el resultado consiste en una indicación del nivel de riesgo debido a la exposición de un modelo de población determinado a un peligro particular en el contexto que corresponda. El riesgo se puede expresar de manera cuantitativa, semicuantitativa o cualitativa. Por ejemplo, el riesgo de cáncer con frecuencia se expresa de manera cuantitativa como la probabilidad de que una persona desarrolle cáncer en un periodo de tiempo dado, al estar sometido a una exposición especificada de un contaminante. El análisis semicuantitativo se puede aplicar para obtener un índice de riesgo para un contaminante o plaga particular y la salida cualitativa puede ser un nivel de riesgo (por ejemplo, alto, medio o bajo) o una descripción con datos prácticos de los probables efectos.

B.8.6 Fortalezas y limitaciones

La fortaleza de este análisis es que proporciona una comprensión muy detallada de la naturaleza del problema y de los factores que aumentan el riesgo.

El análisis de las vías de acceso por lo general es una herramienta útil para todas las áreas de riesgo y permite la identificación de cómo y dónde puede ser posible mejorar los controles o introducir otros nuevos.

No obstante, este análisis necesita datos fiables que con frecuencia no están disponibles o tienen un elevado nivel de incertidumbre asociado a ellos. Por ejemplo, las curvas de dosis-respuesta obtenidas de la exposición de animales a niveles elevados de un peligro se deberían extrapolar para estimar los efectos de niveles muy bajos de contaminantes aplicados a las personas, y existen muchos modelos mediante los cuales se consigue esto. Cuando el modelo es el medio ambiente en vez de personas y el peligro no es químico, se pueden limitar los datos que son directamente aplicables a las condiciones particulares del estudio.

B.9 Técnica estructurada "y si..." (SWIFT)

B.9.1 Presentación

La técnica SWIFT se desarrolló inicialmente como una alternativa más sencilla al estudio de riesgos y de operatividad (HAZOP). Esta técnica consiste en un estudio sistemático basado en el grupo de trabajo, donde se utiliza un conjunto de palabras o frases de "efecto inmediato" que utiliza el coordinador dentro de una reunión de trabajo para estimular a los participantes a que identifiquen riesgos. El coordinador y el grupo de trabajo utilizan frases normalizadas del tipo "¿y si....?" combinadas con las indicaciones, para investigar cómo un sistema, un elemento de planta, una organización o un procedimiento resultará afectado por las desviaciones con respecto a las operaciones y al comportamiento normales. La técnica SWIFT se aplica normalmente a más de un nivel de sistemas con un nivel de detalle más bajo que en el estudio HAZOP.

B.9.2 Utilización

Aunque la técnica SWIFT se diseñó inicialmente para ser aplicada al estudio de peligros en plantas químicas y petroquímicas, ahora su aplicación se ha extendido ampliamente a sistemas, artículos de plantas, procedimientos, y organizaciones. En particular, se utiliza para examinar las consecuencias de los cambios y de los riesgos alterados o creados.

B.9.3 Elementos de entrada

El sistema, procedimiento, artículo de planta, y/o cambio se tiene que definir cuidadosamente antes de que el estudio pueda comenzar. Los contextos externo e interno los establece el coordinador a través de entrevistas y por medio del estudio de documentos, planes y planos. Normalmente, el artículo, la situación o el sistema que se somete a estudio, se divide en nódulos o en elementos claves para facilitar el proceso de análisis, pero esto raramente ocurre al nivel de definición que requiere el HAZOP.

Otra entrada importante la constituyen los conocimientos técnicos y la experiencia del grupo de trabajo que realiza el estudio, el cual debería ser cuidadosamente seleccionado. Todas las partes interesadas deberían estar representadas, si es posible junto con aquellas personas que tienen experiencia en artículos, sistemas, modificaciones o situaciones similares.

B.9.4 Proceso

El proceso general es el siguiente:

- a) Antes de comenzar el estudio, el coordinador prepara una lista de palabras o frases de indicación que se puede basar en un conjunto normalizado o se puede crear para que permita una revisión completa de peligros o riesgos.
- b) En la reunión de trabajo se discute y acuerda el contexto externo y el contexto interno del artículo, sistema, modificación o situación, y el campo de aplicación del estudio.
- c) El coordinador realiza preguntas a los participantes para provocar y discutir sobre:
 - riesgos y peligros conocidos;
 - experiencias e incidentes previos;
 - controles y protecciones conocidos y existentes;
 - requisitos y restricciones de carácter reglamentario.
- d) Se favorece el debate realizando una pregunta donde se utilice la frase "¿y si....?" y una palabra o punto de indicación. Las frases "¿y si....?" son "¿y si...?", "¿que pasaría si....?", "¿podría algo o alguien....?", "¿tiene alguien o algo sobre....?". Lo que se pretende es estimular al grupo de estudio a que explore posibles escenarios, así como sus causas, consecuencias e impactos.
- e) Se hace un resumen de los riesgos y se consideran los controles a introducir.
- f) El equipo de trabajo confirma y registra la descripción del riesgo, sus causas, consecuencias y los controles previstos.
- g) El grupo de trabajo considera si los controles son adecuados y eficaces y acuerda una declaración de la eficacia del control del riesgo. Si éste no llega a ser satisfactorio, el equipo de trabajo considera tareas adicionales de tratamiento del riesgo y define los posibles controles.
- h) Durante este debate se realizan otras preguntas adicionales del tipo "¿y si....?" para identificar otros riesgos.
- i) El coordinador utiliza la lista de indicaciones para monitorizar el debate y para sugerir asuntos y escenarios adicionales para que el grupo de trabajo los discuta.
- j) Es normal aplicar un método cualitativo o semicuantitativo de apreciación del riesgo para clasificar en términos de prioridad las acciones creadas. Esta apreciación se dirige normalmente teniendo en cuenta los controles existentes y la eficacia de los mismos.

B.9.5 Resultados

Los resultados incluyen un registro del riesgo con las acciones o tareas jerarquizadas en función del riesgo. Estas tareas pueden constituir después la base para un plan de tratamiento del riesgo.

B.9.6 Fortalezas y limitaciones

Fortalezas de la técnica SWIFT:

- es ampliamente aplicable a todos los casos de plantas o sistemas físicos, situaciones o circunstancias, organizaciones o actividades;
- necesita una preparación mínima por el equipo de trabajo;

- es relativamente rápida y los peligros y riesgos principales se descubren rápidamente en las reuniones de trabajo;
- el estudio está 'orientado a sistemas' y permite a los participantes observar las respuestas del sistema a las desviaciones, mejor que examinar las consecuencias del fallo del componente;
- se puede utilizar para identificar las oportunidades de mejorar procesos y sistemas, y normalmente se puede utilizar para identificar acciones que conduzcan a mejorar sus probabilidades de éxito;
- en la reunión de trabajo se implica a aquellas personas que son responsables de los controles existentes y de acciones adicionales de apreciación del riesgo, a que refuercen sus responsabilidades;
- crea un registro del riesgo y un plan de tratamiento del riesgo con un poco más de esfuerzo,
- aunque con frecuencia se utiliza una forma cualitativa o semicuantitativa de clasificación del riesgo para la apreciación de éste y para priorizar la atención sobre las acciones resultantes, la técnica SWIFT se puede utilizar para identificar riesgos y peligros que se puedan encaminar a un estudio cuantitativo.

Limitaciones de la técnica SWIFT:

- necesita un coordinador experto y capacitado que sea eficiente;
- se necesita una preparación cuidadosa a fin de no malgastar el tiempo que el grupo de trabajo dedica a las reuniones de trabajo;
- si el grupo de las reuniones de trabajo no tiene una base de experiencia suficientemente amplia o si el sistema de indicaciones no es completo, es posible que algunos riesgos no se identifiquen;
- la aplicación a alto nivel de la técnica puede no revelar causas complejas, detalladas o correlacionadas.

B.10 Análisis de escenario

B.10.1 Presentación

El análisis de escenario es el nombre dado al desarrollo de modelos descriptivos de lo que podría ocurrir en el futuro. Se puede utilizar para identificar riesgos mediante la consideración de posibles desarrollos futuros y la exploración de sus implicaciones. Cuando se analiza el riesgo se pueden utilizar conjuntos de escenarios que reflejen (por ejemplo) 'el mejor caso', 'el peor caso' y 'el caso previsto' para analizar las posibles consecuencias y sus probabilidades de cada escenario, como una forma de análisis de sensibilidad.

La importancia de análisis de escenario se ilustra considerando los cambios importantes que se han producido en los últimos 50 años en la tecnología, en las preferencias de los consumidores, en las actitudes sociales, etc. El análisis de escenario no puede predecir las probabilidades de tales cambios, pero puede considerar las consecuencias y ayudar a las organizaciones a desarrollar fortalezas y a disponer de la elasticidad necesaria para adaptarse a los cambios previsibles.

B.10.2 Utilización

El análisis de escenario se puede utilizar para ayudar en la preparación de decisiones y en la planificación de estrategias futuras así como para considerar las actividades existentes. Puede jugar un papel importante en los tres componentes de la apreciación del riesgo. Para la identificación y el análisis, se pueden utilizar conjuntos de escenarios que reflejen (por ejemplo) el mejor caso, el peor caso y el caso 'previsto' con objeto de identificar lo que podría suceder bajo circunstancias particulares y analizar las posibles consecuencias y sus probabilidades en cada escenario.

El análisis de escenario se puede utilizar para anticipar la manera en que se podrían desarrollar tanto las amenazas como las oportunidades, y también se puede utilizar para todos los tipos de riesgo con planteamientos a corto y a largo plazo. Con un planteamiento a corto plazo y con datos fiables, los posibles escenarios se pueden extrapolar a partir del momento presente. Para un planteamiento a largo plazo o con datos poco fiables, el análisis de escenario pasa a ser más imaginativo y se puede mencionar como análisis futuros.

El análisis de escenario puede ser útil cuando existen importantes diferencias de distribución entre consecuencias positivas y consecuencias negativas en cuanto a espacio, tiempo y grupos en la comunidad o en la organización.

B.10.3 Elementos de entrada

El requisito previo para realizar un análisis de escenario es la disponibilidad de un grupo de personas que tengan entre ellos una comprensión de la naturaleza de los cambios importantes (por ejemplo, los posibles avances de la tecnología) y con imaginación para pensar en el futuro sin necesidad de realizar extrapolaciones desde el pasado. También es útil disponer de acceso a la documentación y a los datos sobre cambios que ya se hayan producido.

B.10.4 Proceso

La estructura del análisis de escenario puede ser informal o formal.

Una vez establecido el grupo de trabajo y los correspondientes canales de comunicación, así como definido el contexto del problema y los asuntos a considerar, el paso siguiente consiste en identificar la naturaleza de los cambios que podrían ocurrir. Para esto será necesario investigar las tendencias principales y la probable cronología en tiempo de los cambios en las tendencias, así como tener pensamientos imaginativos acerca del futuro.

Los cambios a considerar pueden incluir:

- cambios externos (tales como cambios tecnológicos);
- las decisiones que será necesario tomar en un futuro próximo, pero que pueden tener una variedad de resultados;
- las necesidades de las partes interesadas y la forma en que estas necesidades podrían cambiar;
- los cambios macro-ambientales (reglamentos, demográficos, etc.). Algunos serán inevitables y algunos serán inciertos.

Algunas veces, un cambio puede ser debido a las consecuencias de otro riesgo. Por ejemplo, el riesgo del cambio climático es consecuencia de los cambios en la demanda de los consumidores con respecto a los alimentos existentes. Esto influirá en los alimentos que se puedan exportar ventajosamente, así como en los alimentos que se puedan cultivar localmente.

Los factores o tendencias locales y macro se pueden ahora listar y jerarquizar por importancia (1) y por incertidumbre (2). Se presta especial atención a los factores que son más importantes y más inciertos. Los factores o tendencias clave se delimitan unos con otros sobre un plano para mostrar las zonas donde se pueden desarrollar los escenarios.

Se propone una serie de escenarios con cada uno enfocado a un cambio verosímil de parámetros.

A continuación se escribe una "historia" de cada escenario que indique cómo uno se podría mover hasta el escenario objeto. Las historias pueden incluir detalles admisibles que aporten valor a los escenarios.

Los escenarios se pueden utilizar entonces para ensayar o evaluar la cuestión original. El ensayo tiene en cuenta todos los factores importantes que sean predecibles (por ejemplo, el uso de modelos), y luego explora cual sería el 'éxito' de la política (actividad) en este nuevo escenario, y 'preensaya' resultados mediante la utilización de preguntas "¿y si....?" basadas en las hipótesis del modelo.

Cuando la pregunta o la propuesta se ha evaluado con respecto a cada escenario, puede ser obvio que sea necesario modificarla para hacerla más consistente o menos arriesgada. También debería ser posible identificar algunos de los indicadores principales que muestran cuando se ha producido el cambio. El seguimiento y las respuestas de los indicadores principales pueden proporcionar la oportunidad de cambiar las estrategias planificadas.

Dado que los escenarios se definen solo como 'módulos' de futuros posibles, es importante tener la seguridad de que se tiene en cuenta la probabilidad de que se produzca un resultado particular (escenario), es decir, adoptar un marco de riesgo. Por ejemplo, cuando se utilicen escenarios que correspondan al mejor caso, al peor caso y al caso previsto, se debería realizar alguna prueba para cualificar o expresar la probabilidad de que cada escenario se produzca.

B.10.5 Resultados

Es posible que no exista el escenario mejor ajustado, pero debería existir uno que muestre una percepción más clara de la gama de opciones y de cómo modificar el curso de la acción elegida a medida que se mueven los indicadores.

B.10.6 Fortalezas y limitaciones

El análisis de escenario tiene en cuenta una gama de futuros posibles que pueden ser preferibles al enfoque tradicional de depender de pronósticos altos-medios-bajos que se asumen mediante la utilización de datos históricos, aunque los sucesos futuros probablemente continuarán siguiendo las tendencias del pasado. Esto es importante para situaciones en las que existen pocos conocimientos reales en los que basar las predicciones o donde los riesgos se están considerando para un futuro a largo plazo.

Sin embargo, esta fortaleza tiene una falta de solidez asociada, que consiste en que cuando existe una incertidumbre elevada algunos de los escenarios pueden no ser realistas.

Las principales dificultades de la utilización del análisis de escenario están relacionadas con la disponibilidad de datos, y la aptitud del análisis y de las personas que han de tomar decisiones de poder desarrollar escenarios realistas que sean flexibles para probar los posibles resultados.

Los peligros de utilizar el análisis de escenario como una herramienta para tomar decisiones son que los escenarios utilizados pueden no tener una base adecuada, que los datos pueden ser especulativos, y que los resultados no realistas no se pueden reconocer como tales.

B.11 Análisis de impacto en el negocio (BIA)

B.11.1 Presentación

El análisis de impacto en el negocio, también conocido como evaluación de impacto en el negocio, analiza la forma en que los riesgos de siniestro importantes podrían afectar a las operaciones de la organización, e identifica y cuantifica los recursos que serían necesarios para gestionar tales riesgos. Específicamente, un análisis BIA proporciona una comprensión acordada de:

- la identificación y criticidad de los procesos que son económicamente fundamentales, de las funciones y recursos asociados y de las interdependencias clave que existen para una organización;
- la forma en que los sucesos de siniestro afectarán a la aptitud y a la capacidad para conseguir los objetivos que son críticos económicamente;
- la aptitud y la capacidad necesarias para gestionar el impacto de un siniestro y recuperar la organización hasta los niveles de funcionamiento acordados.

B.11.2 Utilización

El análisis BIA se utiliza para determinar la criticidad y los marcos de tiempo de recuperación de los procesos y de los recursos asociados (personas, equipo, tecnología de la información), a fin de asegurar la consecución continuada de los objetivos. Adicionalmente, el análisis BIA ayuda a determinar las interdependencias y las interrelaciones entre procesos, las partes internas y externas, y cualquier conexión de la cadena de suministro.

B.11.3 Elementos de entrada

Los elementos de entrada incluyen:

- un grupo de trabajo para realizar el análisis y el desarrollo de la planificación;
- la información relativa a los objetivos, el entorno, las operaciones y las interdependencias de la organización;
- los detalles de las actividades y operaciones de la organización, incluyendo procesos, recursos de apoyo, relaciones con otras organizaciones, disposiciones de fuentes externas, y partes interesadas;
- las consecuencias financieras y operacionales de la pérdida de procesos críticos;
- un cuestionario preparado;
- la lista de personas a entrevistar de las áreas pertinentes de la organización y/o de las partes interesadas con las que hay que contactar.

B.11.4 Proceso

Un análisis BIA se puede comprender utilizando cuestionarios, entrevistas, reuniones de trabajo estructuradas o combinaciones de las tres, para obtener un conocimiento de los procesos críticos, los efectos de la pérdida de estos procesos, así como los marcos de tiempo de recuperación y los recursos de apoyo que se requieren.

Las etapas clave incluyen:

- en base a la apreciación del riesgo y de la vulnerabilidad, la confirmación de los procesos fundamentales y de los resultados de la organización para determinar la criticidad de los procesos;
- la determinación de las consecuencias de una interrupción sobre los procesos críticos identificados, en lo referente a los aspectos financieros y/u operacionales, sobre periodos de tiempo definidos;
- la identificación de las interdependencias con las principales partes interesadas internas y externas. Esto incluiría la delimitación de la naturaleza de las interdependencias a lo largo de la cadena de suministro;
- la determinación de los recursos reales disponibles y el nivel esencial de recursos necesario para continuar el funcionamiento hasta un nivel mínimo aceptable después de un siniestro;
- la identificación de los trabajos y procesos alternativos relacionados con el trabajo actualmente en uso o planificados que se deben desarrollar. Cuando los recursos o las capacidades no estén disponibles o sean insuficientes durante el siniestro, puede ser necesario aplicar trabajos y procesos alternativos;
- la determinación del tiempo máximo de interrupción aceptable (MAO) para cada proceso, basado en las consecuencias identificadas y en los factores críticos de éxito de la función. El MAO representa el periodo máximo de tiempo que la organización puede tolerar la pérdida de capacidad;
- la determinación del/de los objetivo(s) del tiempo de recuperación (RTO) de cualquier equipo especializado o tecnología de información. El RTO representa el tiempo dentro del cual la organización intenta recuperar el equipo especializado o la capacidad de tecnología de información;
- la confirmación del nivel actual de preparación de los procesos críticos para gestionar un siniestro. Esto puede incluir la evaluación del nivel de redundancia dentro del proceso (por ejemplo, equipo de repuesto) o la existencia de proveedores alternativos.

B.11.5 Resultados

Los resultados son los siguientes:

- una lista de prioridades de procesos críticos e interdependencias asociadas;
- los impactos financieros y operacionales documentados debidos a una pérdida de los procesos críticos;
- los recursos de apoyo necesarios para los procesos críticos identificados;
- los calendarios de interrupción de los procesos críticos y los cuadros de tiempo de recuperación de la tecnología de información asociada.

B.11.6 Fortalezas y limitaciones

Las fortalezas del BIA incluyen:

- la comprensión de los procesos críticos que proporciona la organización con la aptitud de continuar hasta alcanzar sus objetivos previstos;
- la comprensión de los recursos que se requieren;
- una oportunidad para redefinir el proceso operacional de una organización para ayudar en la flexibilidad de la organización.

Las limitaciones incluyen:

- la falta de conocimiento por parte de los participantes implicados en cumplimentar los cuestionarios, en la realización de entrevistas o en las reuniones de trabajo;
- la dinámica del grupo puede afectar al análisis completo de un proceso crítico;
- expectativas simplistas o muy optimistas de los requisitos de recuperación;
- dificultad para obtener un nivel adecuado de comprensión de las operaciones y actividades de la organización.

B.12 Análisis de la causa raíz (RCA)

B.12.1 Presentación

El análisis de una pérdida principal para impedir que vuelva a ocurrir se menciona como Análisis de la Causa Primordial (RCA), Análisis de fallo de la causa raíz (RCFA) o análisis de pérdida. El análisis RCA se centran en las pérdidas de activos debidas a diversos tipos de fallos, mientras que el análisis de pérdidas se aplica principalmente a las pérdidas financieras o económicas debidas a factores externos o a catástrofes. Este análisis intenta identificar las causas raíz u originales en vez de tratar únicamente los síntomas inmediatamente obvios. Se reconoce que la acción correctora no siempre puede ser totalmente eficaz y que puede ser necesaria una mejora continua. El análisis RCA se aplica con bastante frecuencia para la evaluación de una pérdida principal, pero también se puede utilizar para analizar pérdidas sobre una base más global para determinar donde se pueden realizar mejoras.

B.12.2 Utilización

El análisis RCA se aplica en varios contextos con las siguientes amplias áreas de utilización:

- el RCA basado en la seguridad se utiliza en las investigaciones de accidentes y en las áreas de salud y seguridad ocupacional;
- el análisis de fallo se utiliza en sistemas tecnológicos relacionados con la fiabilidad y el mantenimiento;

- el RCA basado en la producción se aplica en el campo del control de la calidad dentro de la fabricación industrial;
- el RCA basado en el proceso está enfocado a procesos del negocio;
- el RCA basado en el sistema se ha desarrollado como una combinación de las áreas anteriores para tratar sistemas complejos con aplicación en la gestión de cambios, la gestión del riesgo y el análisis de sistemas.

B.12.3 Elementos de entrada

La entrada básica para un RCA la constituye la totalidad de las evidencias recopiladas del fallo o de la pérdida. En el análisis también se pueden considerar los datos procedentes de otros fallos similares. Otras entradas pueden ser los resultados obtenidos ensayando hipótesis específicas.

B.12.4 Proceso

Cuando se identifica la necesidad de realizar un análisis RCA, se nombra un grupo de expertos para llevar a cabo el análisis y hacer recomendaciones. El tipo de experto dependerá principalmente de los conocimientos técnicos específicos necesarios para analizar el fallo.

Aunque se pueden utilizar diferentes métodos para realizar el análisis, los pasos básicos de un RCA son similares e incluyen:

- la constitución del grupo de trabajo;
- el establecimiento del campo de aplicación y de los objetivos del RCA;
- la recopilación de datos y evidencias del fallo o de la pérdida;
- la realización de un análisis estructurado para determinar la causa raíz;
- desarrollar soluciones y hacer recomendaciones;
- implantar las recomendaciones;
- verificar el éxito de las recomendaciones implantadas.

Las técnicas de análisis estructurado pueden ser una de las siguientes:

- técnica de "5 porqués", es decir, preguntar repetidamente '¿porqué?' para eliminar opciones de causa y subcausa;
- análisis del modo de fallo y de los efectos;
- análisis de árbol de fallos;
- diagramas de espina de pescado "fishbone" o de Ishikawa;
- análisis Pareto;
- delimitación de la causa raíz.

Con frecuencia, la evaluación de las causas avanza desde causas físicas inicialmente evidentes hasta causas relacionadas con las personas, y finalmente hasta la gestión subyacente o causas fundamentales. Las partes implicadas deben poder controlar o eliminar los factores causales con objeto de que la acción correctiva sea efectiva y que merezca la pena.

B.12.5 Resultados

Los resultados de un análisis RCA incluyen:

- la documentación recopilada de los datos y las evidencias;
- las hipótesis consideradas;
- las conclusiones sobre las causas primordiales más probables del fallo o de la pérdida;
- las recomendaciones de la acción correctiva.

B.12.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- la implicación de los expertos correspondientes trabajando en equipo;
- el análisis estructurado;
- la consideración de todas las hipótesis probables;
- la documentación de los resultados;
- la necesidad de exponer las recomendaciones finales.

Limitaciones de un RCA:

- es posible que no se dispongan de los expertos que se requieren;
- las evidencias críticas se pueden destruir durante el fallo o quedar eliminadas durante la rectificación;
- es posible que el grupo de trabajo no disponga de tiempo o de recursos suficientes para evaluar totalmente la situación;
- es posible que las recomendaciones no se puedan implantar adecuadamente.

B.13 Análisis de los modos de fallo y de los efectos (FMEA) y análisis de los modos de fallos y de los efectos y de la criticidad (FMECA)**B.13.1 Presentación**

El análisis de los modos de fallos y de los efectos (FMEA) es una técnica que se utiliza para identificar las vías por las que los componentes, sistemas o procesos pueden fallar en cuanto a cumplir los objetivos de su diseño.

El análisis FMEA identifica:

- todos los posibles modos de fallo de las diversas partes de un sistema (un modo de fallo es lo que se observa que falla o que funciona incorrectamente);
- los efectos que estos fallos pueden tener sobre el sistema;
- los mecanismos del fallo;
- cómo evitar los fallos, y/o mitigar los efectos de los fallos sobre el sistema.

El análisis FMECA supera al FMEA en que a cada modo de fallo identificado le asigna una jerarquía en función de su importancia o criticidad.

Normalmente, el análisis de criticidad es de tipo cualitativo o semicuantitativo, pero se puede cuantificar mediante la aplicación de estimaciones de fallo reales.

B.13.2 Utilización

Existen varias aplicaciones del análisis FMEA: FMEA de diseño (o de producto) que se utiliza para componentes y productos, FMEA de sistema que se utiliza para sistemas, FMEA de proceso que se utiliza para procesos de fabricación y de montaje, FMEA de servicios y FMEA de software.

El análisis FMEA/FMECA se pueden aplicar durante el diseño, la fabricación o el funcionamiento de un sistema físico.

No obstante, para mejorar la confiabilidad, normalmente los cambios son más fáciles de implantar en la etapa de diseño. Los análisis FMEA y FMECA también se pueden aplicar a procesos y procedimientos. Por ejemplo, se utilizan para identificar el potencial de error médico en sistemas de atención médica, y fallos en los procedimientos de mantenimiento.

El análisis FMEA/FMECA se puede utilizar para:

- ayudar en la selección de alternativas de diseño con una alta confiabilidad;
- asegurar que se han considerado todos los modos de fallo de sistemas y procesos, y sus efectos sobre el éxito operacional;
- identificar los modos de errores humanos y sus efectos;
- disponer de una base para planificar los ensayos y el mantenimiento de sistemas físicos;
- mejorar el diseño de los procedimientos y procesos;
- proporcionar información cualitativa o cuantitativa de técnicas de análisis tales como el análisis de árbol de fallos.

Los análisis FMEA y FMECA pueden proporcionar entradas para otras técnicas de análisis tales como el análisis de árbol de fallos a nivel cualitativo o cuantitativo.

B.13.3 Elementos de entrada

Los análisis FMEA y FMECA necesitan información acerca de los elementos del sistema con detalle suficiente para el análisis significativo de las vías en que cada elemento puede fallar. Para un FMEA de diseño detallado, el elemento puede estar a nivel de componente individual detallado, mientras que para un FMEA de diseño de nivel más alto, los elementos se pueden definir a un nivel más elevado.

La información puede incluir:

- planos o un diagrama de flujo del sistema que se está analizando y de sus componentes, o los pasos de un proceso;
- una comprensión de la función de cada paso de un proceso o componente de un sistema;
- detalles de los parámetros ambientales y de otros tipos, que puedan afectar al funcionamiento;
- una comprensión de los resultados de fallos particulares;
- información histórica de los fallos, incluyendo los datos de las tasas de fallo, cuando estén disponibles.

B.13.4 Proceso

El proceso FMEA consiste en lo siguiente:

- a) definición del campo de aplicación y de los objetivos del estudio;
- b) composición del equipo de trabajo;
- c) comprensión del sistema/proceso que se va a someter al FMECA;
- d) descomposición del sistema en sus componentes o pasos;
- e) definición de la función de cada paso o componente,
- f) para cada componente o paso listado, identifica:
 - ¿cómo puede fallar cada parte de una forma concebible?
 - ¿qué mecanismos podrían producir estos modos de fallo?
 - ¿cuáles serían los efectos si se produjese el fallo?
 - ¿es el fallo inofensivo o dañino?
 - ¿cómo se detecta el fallo?
- g) identificación de las disposiciones inherentes al diseño para compensar el fallo.

Para el análisis FMECA, el grupo de trabajo clasifica cada uno de los modos de fallo identificados en función de su criticidad.

Existen diversas formas de hacerlo. Los métodos más comunes incluyen:

- el índice de criticidad del modo de fallo,
- el nivel de riesgo,
- el número de la prioridad del riesgo.

La criticidad modelo es una medida de la probabilidad de que el modo de fallo que se está considerando produzca un fallo en el sistema considerado en su conjunto; se define como:

Probabilidad del efecto del fallo * Régimen del modo de fallo * Tiempo de funcionamiento del sistema

Se aplica con más frecuencia a modos de fallo del equipo en los que cada uno de estos términos se puede definir cuantitativamente y todos los modos de fallo tienen las mismas consecuencias.

El nivel de riesgo se obtiene combinando las consecuencias de un modo de fallo que ocurre, con la probabilidad del fallo. Se utiliza cuando las consecuencias de modos de fallo diferentes son distintas y se pueden aplicar a sistemas o procesos de equipos. El nivel de riesgo se puede expresar de forma cualitativa, semicuantitativa o cuantitativa.

El número de prioridad del riesgo (RPN) es una medida semicuantitativa de la criticidad, que se obtiene multiplicando números de las escalas de clasificación (normalmente entre 1 y 10) por la consecuencia del fallo, la probabilidad de fallo y la aptitud para detectar el problema. (A un fallo se le da una prioridad más alta si es difícil de detectar.). Este método se utiliza con mucha frecuencia en aplicaciones de aseguramiento de la calidad.

Una vez que los modos y los mecanismos de fallo han sido identificados, las acciones correctivas se pueden definir e implantar para los modos de fallo más importantes.

El FMEA se documenta en un informe que contiene:

- los detalles del sistema que se ha analizado;
- la forma en que se realizó el análisis;
- las suposiciones efectuadas en el análisis;
- los orígenes de los datos;
- los resultados, incluyendo las fichas de trabajo cumplimentadas;
- la criticidad (si se ha completado) y la metodología aplicada para definirla;
- todas las recomendaciones para análisis adicionales, los cambios o características de diseño a incorporar en los planes de ensayo, etc.

El sistema se puede volver a someter a apreciación para otro ciclo de análisis FMEA, una vez que se hayan completado las acciones.

B.13.5 Resultados

El resultado principal del análisis FMEA consiste en una lista de modos de fallo y de los mecanismos y efectos de fallo para cada componente o paso de un sistema o proceso (que puede incluir información sobre la probabilidad del fallo). También proporciona información sobre las causas del fallo y las consecuencias para el sistema considerado en su totalidad. La salida del análisis FMECA incluye una clasificación de la importancia basada en la probabilidad de que el sistema falle, en el nivel de riesgo resultante del modo de fallo o en una combinación del nivel de riesgo y la 'detectabilidad' del modo de fallo.

El FMECA puede dar una salida cuantitativa si se utilizan datos adecuados de la tasa de fallos y consecuencias cuantitativas.

B.13.6 Fortalezas y limitaciones

Las fortalezas de los análisis FMEA/FMECA son las siguientes:

- son ampliamente aplicable a modos de fallo de personas, equipos y sistemas y para hardware, software y procedimientos;
- identifican los modos de fallo de los componentes, sus causas y sus efectos sobre el sistema, y los presentan en un formato fácilmente legible;
- evitan la necesidad de costosas modificaciones del equipo en servicio, mediante la identificación temprana en el proceso de diseño;
- identifican modos de fallo de un solo punto y los requisitos, por redundancia o mediante sistemas de seguridad;
- proporcionan la entrada para el desarrollo de programas de seguimiento, realzando las características importantes a realizar el seguimiento.

Las limitaciones incluyen:

- estos análisis únicamente se pueden utilizar para identificar modos de fallo únicos, y no combinaciones de modos de fallo;
- salvo que se controlen y enfoquen adecuadamente, los estudios pueden ocupar mucho tiempo y ser costosos;
- pueden ser difíciles y tediosos para sistemas complejos de muchas etapas.

B.13.7 Normas para consulta

IEC 60812, *Técnicas de análisis de la fiabilidad de sistemas. Procedimiento de análisis de los modos de fallo y de sus efectos (AMFE)*

B.14 Análisis del árbol de fallos (FTA)

B.14.1 Presentación

El FTA es una técnica para identificar y analizar factores que pueden contribuir a un suceso especificado no deseado (denominado el "suceso superior o principal"). Los efectos causales se identifican deductivamente, se organizan de una manera lógica y se representan gráficamente mediante un diagrama de árbol que describe los factores causales y sus relaciones lógicas con respecto al suceso superior.

Los factores identificados en el árbol pueden ser sucesos que están asociados con fallos materiales de componentes, con errores humanos o con cualquier otro suceso pertinente que conduce al suceso no deseado.

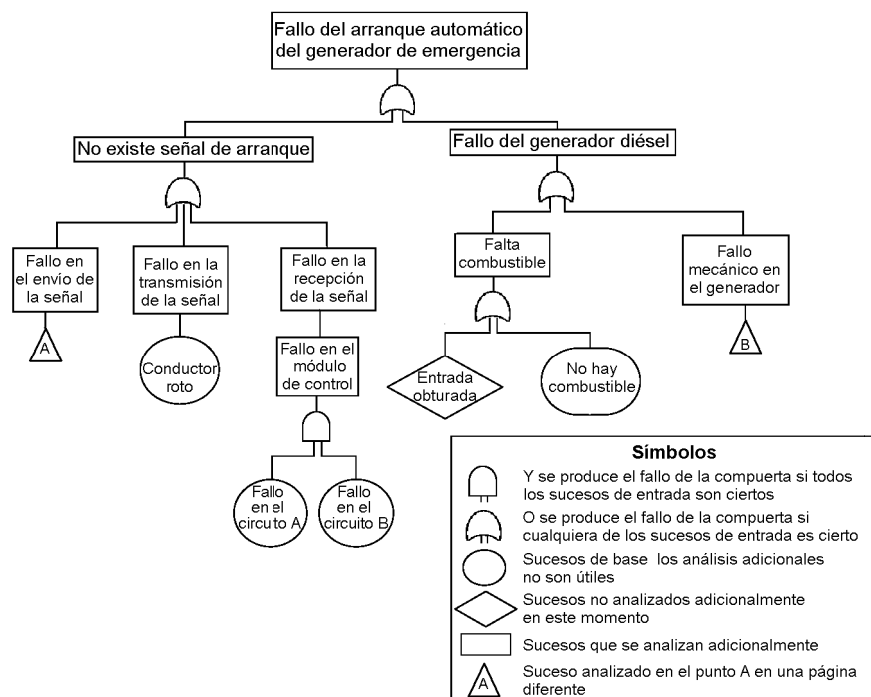


Figura B.2 – Ejemplo de un FTA según la Norma IEC 60300-3-9

B.14.2 Utilización

Un árbol de fallos se puede utilizar cualitativamente para identificar las causas potenciales y los caminos por los que se produce un fallo (el suceso superior), o cuantitativamente para calcular la probabilidad del suceso superior, proporcionando conocimiento de las probabilidades de los sucesos causales.

Se puede utilizar en la etapa de diseño de un sistema para identificar las causas potenciales del fallo y, por tanto, para seleccionar entre opciones de diseño diferentes. Se puede utilizar en la fase de funcionamiento para identificar cómo se pueden producir los fallos principales, y la importancia relativa de los diferentes caminos que llevan al suceso superior. Un árbol de fallos también se puede utilizar para analizar un fallo que ha ocurrido, con objeto de representar mediante un diagrama la forma en que sucesos diferentes se unieron para causar el fallo.

B.14.3 Elementos de entrada

Para el análisis cualitativo se requiere conocer el sistema y las causas del fallo, así como el conocimiento técnico de cómo el sistema puede fallar. Los diagramas detallados son útiles como ayuda para el análisis.

Para el análisis cuantitativo, se requieren datos sobre las frecuencias de fallo o sobre la probabilidad de que exista un estado de fallo para todos los sucesos básicos del árbol de fallos.

B.14.4 Proceso

Las etapas para desarrollar un árbol de fallos son las siguientes:

- Se define el suceso superior a analizar. Éste puede ser un fallo o puede ser una consecuencia más amplia de este fallo. Cuando se analiza la consecuencia, el árbol puede contener una sección relacionada con la mitigación del fallo real.
- Comenzando con el suceso superior, las causas inmediatas posibles de los modos de fallo conducen a que el suceso superior sea identificado.
- Cada una de estas causas/modos de fallo se analiza para identificar cómo se podrían producir sus fallos.
- Progresivamente se siguen las etapas de identificación del funcionamiento no deseable del sistema para los niveles sucesivamente más bajos hasta que los análisis adicionales ya no sean procedentes. En un sistema de hardware, este fallo puede surgir a nivel de fallo de componente. Los sucesos y factores causales del nivel más bajo del sistema analizado se conocen como sucesos de base.
- Cuando se puedan asignar probabilidades a los sucesos de base, se puede calcular la probabilidad del suceso superior. Para que la cuantificación sea válida, debe ser posible demostrar que para cada salida, todas las entradas son necesarias y suficientes para provocar el suceso de salida. Cuando no sea este el caso, el árbol de fallos no es válido para el análisis de la probabilidad, pero puede ser una herramienta útil para mostrar las relaciones causales.

Como parte de la cuantificación, puede ser necesario simplificar el árbol de fallos utilizando álgebra de Boole para contabilizar los modos de fallo duplicados.

El árbol de fallos proporciona también una estimación de la probabilidad de que se pueda identificar el suceso principal y los ajustes de corte mínimos que formarían caminos individuales separados hacia el suceso principal, así como que se pueda calcular las influencias de estos sobre el suceso superior.

Salvo para los árboles de fallo simples, es necesario disponer de programas informáticos para realizar los cálculos adecuadamente cuando existen sucesos repetidos en varios lugares del árbol de fallos, y para calcular los ajustes de corte mínimos. Los programas informáticos ayudan a confirmar la consistencia, la exactitud y la posibilidad de verificación de los datos.

B.14.5 Resultados

Los resultados del análisis del árbol de fallos son las siguientes:

- una representación gráfica de cómo puede ocurrir el suceso superior que muestra la interacción de los caminos donde dos o más sucesos pueden ocurrir simultáneamente;
- una lista de los ajustes de corte mínimos (camino individuales hacia el fallo) con (cuando los datos están disponibles) la probabilidad de que ocurra cada uno de ellos;
- la probabilidad del suceso superior.

B.14.6 Fortalezas y limitaciones

Fortalezas del análisis FTA:

- Este análisis ofrece un enfoque disciplinado que es altamente sistemático, pero que al mismo tiempo es suficientemente flexible para permitir el análisis de una variedad de factores, incluyendo las interacciones humanas y los fenómenos físicos.
- La aplicación del enfoque "de arriba hacia abajo", implícito en la técnica, centra la atención sobre aquellos efectos de fallo que están relacionados directamente con el suceso superior.
- El FTA es especialmente útil para analizar sistemas que tengan muchas interfaces e interacciones.
- La representación gráfica permite una fácil comprensión del comportamiento del sistema y de los factores que incluye, pero como los árboles suelen ser grandes, el procesamiento de los árboles de fallos puede requerir sistemas informáticos. Esta característica permite la inclusión de relaciones lógicas más complejas (por ejemplo, NAND y NOR), pero también hace que la verificación del árbol de fallos sea más difícil.
- El análisis lógico de los árboles de fallos y la identificación de los ajustes de corte, es útil para la identificación de caminos de fallo simples en un sistema muy complejo en el que se podrían pasar por alto combinaciones particulares de sucesos que conducen al suceso superior.

Las limitaciones incluyen:

- Las incertidumbres en las probabilidades de los sucesos de base se incluyen en los cálculos de la probabilidad del suceso superior. Esto puede originar altos niveles de incertidumbre cuando las probabilidades de fallo del suceso de base no se conocen con exactitud; no obstante, en sistemas bien conocidos es posible un alto grado de confianza.
- En algunas situaciones, los sucesos causales no están ligados unos a otros y puede ser difícil averiguar si están incluidos todos los caminos importantes hacia el suceso superior. Por ejemplo, la inclusión de todos los orígenes de ignición como suceso superior en el análisis de un fuego. En esta situación, no es posible el análisis de probabilidad.
- El árbol de fallos es un modelo estático; las interdependencias del tiempo no se consideran.
- Los árboles de fallos solamente se pueden tratar con estados binarios (fallado/no fallo).
- Aunque los modos de error humano se pueden incluir en un árbol de fallos cualitativo, en general los fallos de grado o calidad que con frecuencia caracteriza a los errores humanos no se pueden incluir fácilmente.
- Un árbol de fallos no permite que los efectos dominó o los fallos condicionales se puedan incluir fácilmente.

B.14.7 Normas para consulta

IEC 61025, *Análisis por árbol de fallos (AAF)*.

IEC 60300-3-9, *Gestión de la confiabilidad. Parte 3-9, Guía de aplicación. Análisis de riesgos de sistemas tecnológicos.*

B.15 Análisis del árbol de sucesos (ETA)

B.15.1 Presentación

El análisis ETA es una técnica gráfica para la representación de secuencias mutuamente exclusivas de sucesos que siguen a un suceso iniciador de acuerdo con el funcionamiento/no funcionamiento de los diversos sistemas diseñados para mitigar sus consecuencias (véase la figura B.3). Este análisis se puede aplicar cualitativa y cuantitativamente.

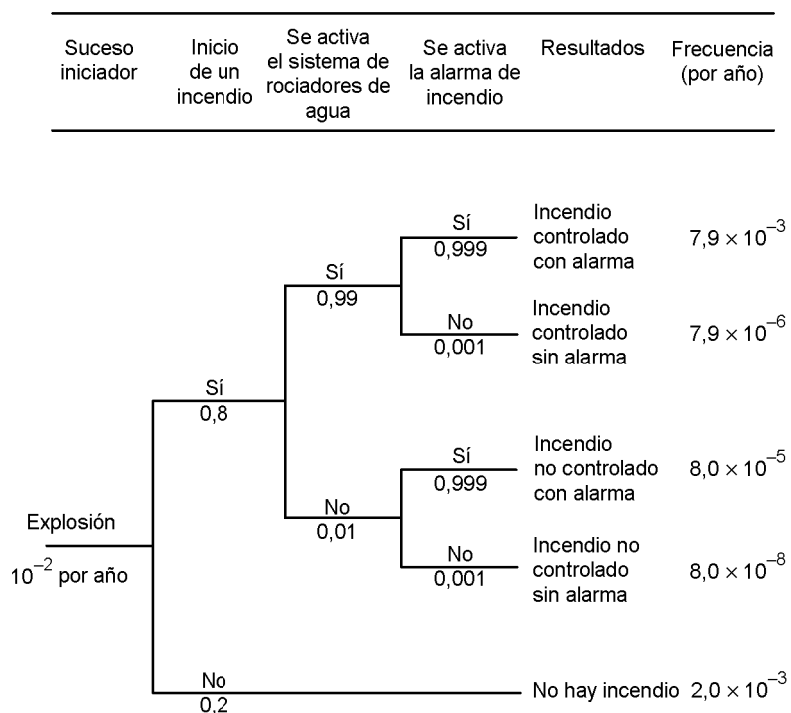


Figura B.3 – Ejemplo de un árbol de sucesos

La figura B.3 muestra los cálculos simples para un ejemplo de árbol de sucesos, cuando las ramas son totalmente independientes.

Mediante el despliegue en forma de árbol, el análisis ETA puede representar sucesos de agravamiento o de mitigación en respuesta al suceso iniciador, teniendo en cuenta sistemas, funciones o barreras adicionales.

B.15.2 Utilización

El análisis ETA se puede utilizar para modelar, calcular y clasificar jerárquicamente (desde un punto de vista del riesgo) los diferentes escenarios de accidente que siguen al suceso iniciador.

El análisis ETA se puede utilizar en cualquier etapa del ciclo de vida de un producto o proceso. Se puede utilizar cualitativamente para ayudar en la tormenta de ideas de escenarios potenciales y secuencias de sucesos que siguen a un suceso iniciador y para ver cómo los resultados son afectados por los diversos tratamientos, barreras o controles previstos para mitigar resultados no deseados.

El análisis cuantitativo tiende a considerar por sí mismo la aceptabilidad de los controles. Se utiliza con frecuencia para modelar fallos en los que hay múltiples protecciones.

El análisis ETA también se puede utilizar para modelar sucesos iniciadores que podrían proporcionar pérdidas o ganancias. No obstante, las circunstancias en las que se buscan caminos para optimizar las ganancias, se modelan más frecuentemente utilizando un árbol de decisión.

B.15.3 Elementos de entrada

Los elementos de entrada incluyen:

- una lista de sucesos iniciadores apropiados;
- información sobre los tratamientos, barreras y controles, y sus probabilidades de fallo (para análisis cuantitativos);
- la comprensión de los procesos en los cuales un fallo inicial se intensifica.

B.15.4 Proceso

Un árbol de sucesos comienza con la selección de un suceso iniciador. Este suceso puede ser un incidente, tal como una explosión de polvo, o un suceso causal tal como un fallo de potencia. A continuación se listan las funciones o sistemas disponibles para mitigar los resultados. Para cada función o sistema se traza una línea para representar su éxito o su fallo. A cada línea se puede asignar una probabilidad particular de fallo con esta probabilidad condicional estimada, por ejemplo, mediante un criterio experto o un análisis de árbol de fallos. De esta forma, se modelan diferentes caminos a partir del suceso iniciador.

Se hace constar que las probabilidades en el árbol de sucesos son probabilidades condicionales, por ejemplo, la probabilidad de que funcione un rociador de agua no es la probabilidad obtenida mediante ensayos realizados bajo condiciones normales, sino la probabilidad de que funcione bajo condiciones de incendio causado por una explosión.

Cada camino a través del árbol representa la probabilidad de que todos los sucesos ocurrirán en ese camino. Por ello, la frecuencia del resultado se representa por el producto de las probabilidades condicionales individuales y la frecuencia de la iniciación del suceso, dado que los diferentes sucesos son independientes.

B.15.5 Resultados

Los resultados del análisis ETA incluyen lo siguiente:

- descripciones cualitativas de los posibles problemas, considerados como combinaciones de sucesos que producen diversos tipos de problemas (gama de resultados) a partir de los sucesos iniciadores;
- estimaciones cuantitativas de las frecuencias o probabilidades del suceso y de la importancia relativa de las diversas secuencias de fallo y de los sucesos que contribuyen al fallo;
- lista de recomendaciones para reducir los riesgos;
- evaluaciones cuantitativas de la eficacia de las recomendaciones.

B.15.6 Fortalezas y limitaciones

Las fortalezas del análisis ETA incluyen lo siguiente:

- se analizan los posibles escenarios que el análisis ETA presenta gráficamente después de un suceso iniciador, y en un diagrama se representa de forma clara la influencia del éxito o del fallo de los sistemas o de las funciones de mitigación;
- contabiliza en función del tiempo los efectos de dependencia y de dominó que son incómodos para la modelización del árbol de fallos;

- representa gráficamente las secuencias de los sucesos que no es posible representar cuando se utilizan árboles de fallos.

Las limitaciones incluyen:

- con objeto de utilizar el análisis ETA como parte de una apreciación completa, es necesario identificar todos los sucesos iniciadores. Esto se puede hacer aplicando otro método de análisis (por ejemplo, HAZOP, PHA), sin embargo, siempre existe la posibilidad de que desaparezca algún suceso iniciador importante;
- con los árboles de sucesos, solo se tratan estados de éxito y de fallo, y es difícil incorporar éxitos atrasados o la recuperación de sucesos;
- cualquier camino es condicional en cuanto a los sucesos que han ocurrido en los puntos de bifurcación previos a lo largo del camino. Por ello, muchas dependencias son dirigidas a lo largo de los posibles caminos. No obstante, algunas dependencias, tales como componentes comunes, sistemas de utilidad y operadores se pueden pasar por alto si no se manejan cuidadosamente y pueden conducir a estimaciones optimistas del riesgo.

B.16 Análisis de causa-consecuencia

B.16.1 Generalidades

El análisis de causa-consecuencia es una combinación del análisis de árbol de fallos y del análisis de árbol de sucesos. Comienza a partir de un suceso crítico y analiza las consecuencias por medio de una combinación de salidas lógicas SI/NO que representan las condiciones que pueden ocurrir, o los fallos de los sistemas que se han diseñado para mitigar las consecuencias del suceso iniciador. Las causas de las condiciones o los fallos se analizan mediante árboles de fallos (véase el capítulo B.15).

B.16.2 Utilización

El análisis de causa-consecuencia se desarrolló inicialmente como una herramienta de fiabilidad para sistemas críticos de seguridad, lo que proporcionaba una comprensión más completa de los fallos del sistema. Como análisis de árbol de fallos, se utiliza para representar la lógica del fallo que conduce a un suceso crítico, pero aumenta la funcionalidad de un árbol de fallos al permitir que se analicen los fallos secuenciales en el tiempo. Este método también permite que las demoras de tiempo se incorporen al análisis de las consecuencias, lo que no es posible con los árboles de sucesos.

Este método se utiliza para analizar los diversos caminos que un sistema podría tomar después de un suceso crítico, dependiendo del comportamiento de los subsistemas particulares (tales como sistemas de respuestas de emergencia). Si se cuantifican, proporcionarán una estimación de la probabilidad de las diferentes consecuencias posibles que siguen a un suceso crítico.

Como en un diagrama de causa-consecuencia, cada secuencia es una combinación de árboles de subfallos, el análisis de causa-consecuencia se puede utilizar como una herramienta para preparar árboles de fallo mayores.

Los diagramas son complejos de preparar y de utilizar, y por ello solo se tiende a utilizarlos cuando la magnitud de las potenciales consecuencias del fallo justifica un esfuerzo intenso.

B.16.3 Elementos de entrada

Se requiere el conocimiento del sistema, así como de sus modos de fallo y de los escenarios de fallo.

B.16.4 Proceso

La figura B.4 muestra un diagrama conceptual de un análisis de causa-consecuencia típico.

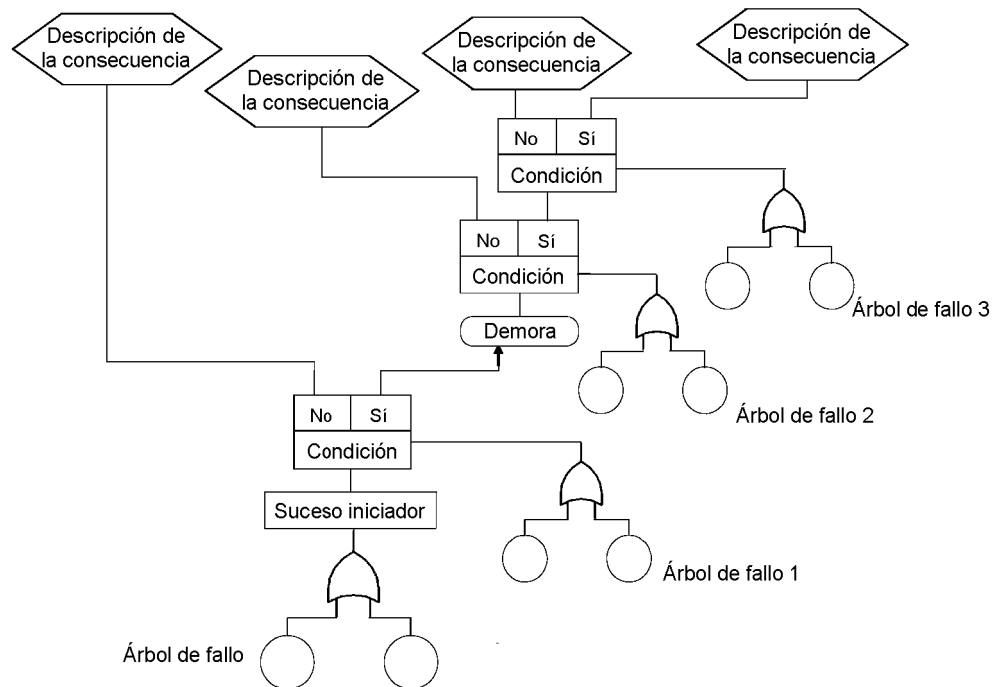


Figura B.4 – Ejemplo de análisis de causa-consecuencia

El procedimiento es el siguiente:

- Se identifica el suceso crítico (o iniciador) (equivalente al suceso superior de un árbol de fallos y al suceso iniciador de un árbol de sucesos).
- Se desarrolla y valida el árbol de fallos para las causas del suceso iniciador como se describe en el capítulo B.14. Se utilizan los mismos símbolos que en un análisis de árbol de fallos convencional.
- Se decide el orden en que se consideran las condiciones. Esta debería ser una secuencia lógica tal como la secuencia temporal en que las condiciones se producen.
- Se construyen los vectores para las consecuencias en función de las distintas condiciones. Es similar a un árbol de sucesos, pero las bifurcaciones en los caminos del árbol de sucesos se muestran como cajas etiquetadas con la condición particular que se aplica.
- La probabilidad de cada consecuencia se puede calcular, siempre que los fallos de cada caja de condición sean independientes. Esto se consigue asignando primero probabilidades a cada salida de la caja de condición (utilizando los árboles de fallo aplicables que sean apropiados). La probabilidad de que una secuencia cualquiera conduzca a una secuencia particular se obtiene multiplicando las probabilidades de cada secuencia por las condiciones que terminan en esta secuencia particular. Si más de una secuencia termina con la misma secuencia, se suman las probabilidades de cada secuencia. Si existen dependencias entre fallos de condiciones en una secuencia (por ejemplo, un fallo de la energía puede dar lugar a varias condiciones de fallo), entonces las dependencias se deberían tratar antes de los cálculos.

B.16.5 Resultado

El resultado del análisis de causa-consecuencia es una representación en diagrama de cómo puede fallar un sistema, mostrando las causas y las consecuencias. La salida es una estimación de la probabilidad de ocurrencia de cada posible consecuencia basada en el análisis de las probabilidades de ocurrencia de condiciones particulares que siguen al suceso crítico.

B.16.6 Fortalezas y limitaciones

Las fortalezas del análisis de causa-consecuencia son las mismas que las de los análisis de árboles de sucesos y de árboles de fallos combinadas. Además, supera algunas de las limitaciones de estas técnicas pudiendo analizar sucesos que se desarrollan en el tiempo. El análisis de causa-consecuencia proporciona una visión global del sistema.

Las limitaciones son que éste análisis es más complejo que los análisis de árbol de fallos y de árbol de sucesos, así como la forma de realizarlo y la manera en que las dependencias se tratan durante la cuantificación.

B.17 Análisis de causa-y-efecto

B.17.1 Presentación

El análisis de causa-y-efecto es un método estructurado para identificar las posibles causas de un suceso o problema indeseable. Este análisis organiza los posibles factores contributivos en categorías, de manera que se pueden considerar todas las posibles hipótesis. No obstante, no apunta por sí mismo a las causas reales, ya que estas solo se pueden determinar por medio de evidencias reales y de ensayos empíricos de las hipótesis. La información se organiza en un diagrama de espina de pescado "Fishbone" (también llamado diagrama de Ishikawa) o algunas veces en diagrama en árbol (véase B.17.4).

B.17.2 Utilización

El análisis de causa-y-efecto proporciona una presentación gráfica estructurada de una lista de causas de un efecto específico. El efecto puede ser positivo (un objetivo) o negativo (un problema) dependiendo del contexto.

Este análisis se utiliza para permitir la consideración de todos los escenarios y causas posibles identificadas por un grupo de expertos, y que se establezca el consenso de las causas más probables que se pueden ensayar empíricamente o por evaluación de los datos disponibles. Es más útil al comienzo de un análisis para pensar en las causas posibles y después establecer las posibles hipótesis que se puedan considerar de la manera más formal.

La elaboración de un diagrama de causa-y-efecto se puede llevar a cabo cuando existe la necesidad de:

- identificar las causas raíz posibles, las razones básicas, de un efecto, problema o condición específicos;
- clasificar y relacionar algunas de las interacciones entre los factores que afectan a un proceso particular;
- analizar los problemas existentes para que se aplique la acción correctiva;

Los beneficios de la elaboración de un diagrama de causa-y-efecto incluyen:

- que la atención de los miembros de la revisión se concentre sobre un problema específico;
- ayudar a determinar las causas raíz de un problema utilizando un enfoque estructurado;
- alentar la participación del grupo de expertos y utilizar el conocimiento de este grupo sobre el producto o proceso;
- utilizar un formato ordenado y fácil de leer para las relaciones del diagrama de causa-y-efecto;
- indicar las causas posibles de variación en un proceso;
- identificar las áreas donde se deberían recopilar datos para estudios adicionales.

El análisis de causa-y-efecto se puede utilizar como un método que realiza el análisis de la causa raíz (véase el capítulo B.12).

B.17.3 Elementos de entrada

Los elementos de entrada para un análisis de causa-y-efecto puede proceder de los conocimientos técnicos y de la experiencia de los participantes o de un modelo desarrollado previamente que se haya utilizado en el pasado.

B.17.4 Proceso

El análisis de causa-y-efecto debería ser realizado por un grupo de expertos entendido en el problema que requiere solución.

Los pasos básicos para realizar el análisis de causa-y-efecto son los siguientes:

- establecer el efecto a analizar y situarlo en una caja. El efecto puede ser positivo (un objetivo) o negativo (un problema) dependiendo de las circunstancias;
- determinar las categorías principales de las causas representadas por cajas en el diagrama de espina de pescado "Fishbone". Típicamente, para un problema del sistema, las categorías pueden ser personas, equipos, entorno ambiental, procesos, etc. No obstante, estas categorías se eligen para fijar el contexto particular;
- llenar cada categoría principal con ramales y subramales de las causas posibles para describir la relación entre ellas;
- preguntar "¿porqué?" o "¿a causa de qué?" para conectar las causas;
- revisar todas los ramales para verificar la coherencia y plenitud y asegurar que las causas se aplican al efecto principal;
- identificar la mayoría de las causas probables en base a la opinión del grupo de expertos y a la evidencia disponible.

Los resultados se representan normalmente como un diagrama de espina de pescado "Fishbone" o diagrama de Ishikawa o un diagrama en árbol. El diagrama de espina de pescado "Fishbone" se estructura separando las causas en categorías principales (representadas por las líneas situadas fuera de la espina central del pescado) con ramales y subramales que describen más causas específicas en esas categorías.

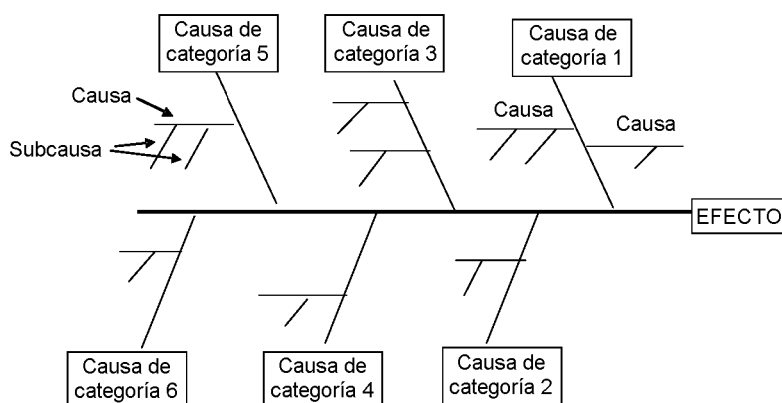


Figura B.5 – Ejemplo de diagrama de espina de pescado "Fishbone" o de Ishikawa

En apariencia, la representación en árbol es similar a un árbol de fallos, aunque con frecuencia se representa con el árbol desarrollándose de izquierda a derecha en vez de hacia la parte de abajo de la página. No obstante, no se puede cuantificar para producir una probabilidad del suceso principal dado que las causas son posibles factores que contribuyen, en vez de fallos, con una probabilidad de ocurrencia conocida.

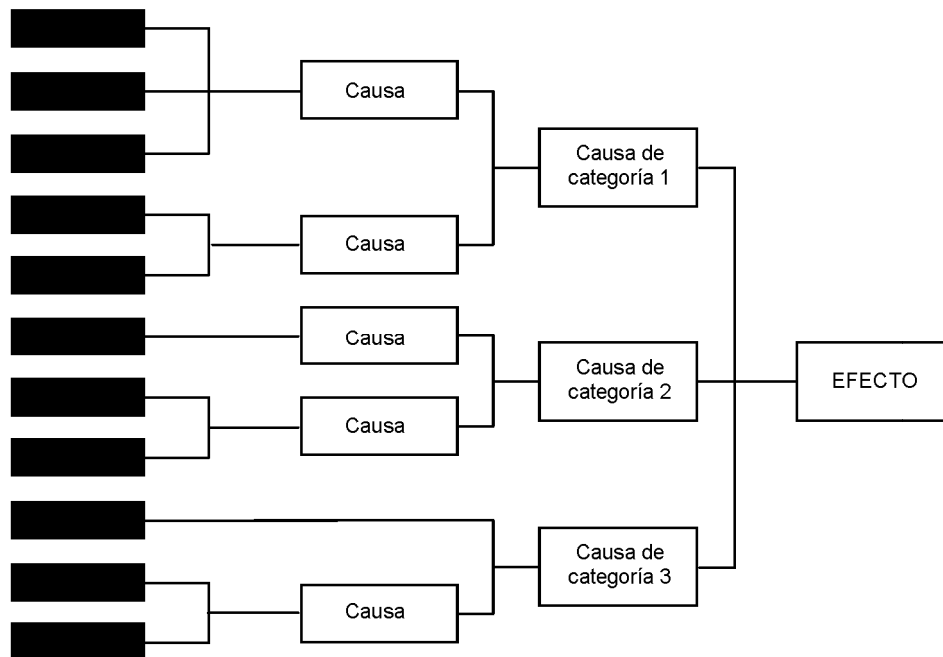


Figura B.6 – Ejemplo de formulación en árbol del análisis de causa-y-efecto

Por lo general, los diagramas de causa-y-efecto se utilizan en forma cualitativa. Es posible asumir que la probabilidad del problema es 1 y asignar probabilidades a causas genéricas, y posteriormente a las subcausas, sobre la base del grado de creencia acerca de su relevancia. Sin embargo, con frecuencia los factores contributivos interactúan y contribuyen al efecto por caminos complejos que invalidan la cuantificación.

B.17.5 Resultados

El resultado de un análisis de causa-y-efecto es un diagrama de espina de pescado "Fishbone" o un diagrama en árbol que muestra las causas posibles y probables. Después esto se tiene que verificar y ensayar empíricamente antes de poder hacer recomendaciones.

B.17.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- la implicación de los expertos que trabajan en equipo;
- el análisis estructurado;
- la consideración de todas las hipótesis probables;
- una ilustración gráfica de los resultados que sea fácil de leer;
- áreas identificadas donde se necesitan datos adicionales;

- se puede utilizar para identificar los factores que contribuyen a los efectos deseados así como a los no deseados. El hacer un enfoque positivo sobre una consecuencia puede fomentar un mayor dominio y participación.

Las limitaciones incluyen:

- el equipo puede no tener los conocimientos técnicos necesarios;
- éste no es un proceso completo por sí mismo y necesita ser una parte de un análisis de la causa primordial para poder generar recomendaciones;
- es más una técnica de presentación de tormenta de ideas que una técnica de análisis independiente;
- la separación de los factores causales en categorías principales al comienzo del análisis significa que las interacciones entre las categorías no se pueden considerar adecuadamente, por ejemplo, cuando el fallo del equipo es debido a errores humanos, o los problemas humanos son causados por un diseño deficiente.

B.18 Análisis de capas de protección (LOPA)

B.18.1 Presentación

El LOPA es un método semicuantitativo para estimar los riesgos asociados con un suceso o escenario no deseado. Sirva para analizar si existen suficientes medidas para controlar o mitigar el riesgo.

Se selecciona un par causa-consecuencia y se identifican las capas de protección que impiden que la causa conduzca a una consecuencia no deseada. Se realiza un cálculo de magnitudes para determinar si la protección es adecuada para reducir el riesgo hasta un nivel tolerable.

B.18.2 Utilización

El LOPA se puede utilizar en forma cualitativa simplemente para revisar las capas de protección entre un peligro o suceso causal y una consecuencia. Normalmente se aplicaría un enfoque semicuantitativo para añadir más rigor al proceso de filtrado, por ejemplo a continuación de un HAZOP o PHA.

El LOPA proporciona una base para la especificación de capas de protección independientes (IPLs) y niveles de integridad y seguridad (niveles SIL) para sistemas instrumentados, como se describen en la serie de Normas IEC 61508 o en la Norma IEC 61511, y para la determinación de los requisitos del nivel de integridad y seguridad (SIL) para sistemas instrumentados de seguridad. El LOPA se puede utilizar para ayudar a asignar de forma efectiva los recursos para la reducción del riesgo, analizando la reducción del riesgo producida por cada capa de protección.

B.18.3 Elementos de entrada

Los elementos de entrada al LOPA incluyen:

- la información básica sobre riesgos, incluyendo peligros, causas y consecuencias tales como las facilitadas por un PHA;
- la información sobre los controles instalados o propuestos;
- las frecuencias de un suceso causal, y las probabilidades de fallo de la capa de protección, las medidas de la consecuencia y una definición de riesgo tolerable;
- las frecuencias de causas iniciadoras, las probabilidades de fallo de la capa de protección, las medidas de la consecuencia y una definición de riesgo tolerable.

B.18.4 Proceso

El LOPA lo realiza un grupo de expertos aplicando el siguiente procedimiento:

- se identifican las causas iniciadoras de una consecuencia no deseada y se buscan datos sobre sus frecuencias y consecuencias;
- se selecciona un par de causa-consecuencia;
- se identifican y analizan en cuanto a su eficacia las capas de protección que impiden la causa que da lugar a la consecuencia no deseada;
- se identifican las capas de protección independientes (IPLs) (no todas las capas de protección son IPLs);
- se estima la probabilidad de fallo de cada IPL;
- se combina la frecuencia de la causa iniciadora con las probabilidades de fallo de cada IPL, y las probabilidades de todos los modificadores condicionales (un modificador condicional es, por ejemplo si una persona estará presente y será impactada) para determinar la frecuencia de ocurrencia de la consecuencia no deseada. Para las frecuencias y las probabilidades se utilizan órdenes de magnitud;
- se compara el nivel de riesgo calculado con los niveles de tolerancia del riesgo para determinar si se requiere protección adicional.

Un IPL es un dispositivo, sistema o acción que es capaz de impedir que un escenario preceda a su consecuencia no deseada, con independencia del suceso causal o de cualquier otra capa de protección asociada al escenario.

Un IPL incluye:

- características de diseño;
- dispositivos de protección física;
- sistemas de enclavamiento y de parada;
- alarmas críticas e intervención manual;
- protección física posterior al suceso;
- sistemas de respuesta de emergencia (los procedimientos y las inspecciones no son IPLs).

B.18.5 Resultados

Se deben dar recomendaciones sobre todos los controles adicionales y la eficacia de estos controles en la reducción del riesgo.

El LOPA es una de las técnicas utilizada para la apreciación del SIL cuando se tratan sistemas relacionados con la seguridad o dotados de medios para medir la seguridad.

B.18.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- requiere menos tiempo y recursos que un análisis de árbol de fallos o una apreciación del riesgo totalmente cuantitativa, pero es más riguroso que los juicios subjetivos cualitativos;
- ayuda a identificar y dirigir recursos sobre las capas de protección más críticas;

- identifica operaciones, sistemas y procesos para los que no existe protección suficiente;
- está enfocado a las consecuencias más serias.

Las limitaciones incluyen:

- El LOPA se enfoca sobre un par causa-consecuencia y un escenario en un momento dado. Las interacciones complejas entre riesgos o entre controles no están cubiertas;
- los riesgos cuantificados pueden no contabilizar para los fallos en modo común;
- el LOPA no se aplica a escenarios muy complejos donde existen muchos pares de causa-consecuencia o donde existe una variedad de consecuencias que afectan a partes interesadas diferentes.

B.18.7 Normas para consulta

IEC 61508 (todas las partes), *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad*.

IEC 61511, *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de la industria de procesos*.

B.19 Análisis del árbol de decisiones

B.19.1 Presentación

Un árbol de decisiones presenta decisiones alternativas y resultados de una manera secuencial que tiene en cuenta resultados inciertos. Es similar a un árbol de sucesos en que comienza a partir de un suceso iniciador o de una decisión inicial, en que se pueden hacer modelos de caminos y consecuencias diferentes como un resultado de sucesos que pueden ocurrir, y en que se pueden tomar diferentes decisiones.

B.19.2 Utilización

Un árbol de decisiones se utiliza para gestionar los riesgos del proyecto y en otras circunstancias para ayudar a seleccionar la mejor línea de conducta cuando existe incertidumbre. La presentación gráfica también puede ayudar a comunicar razones para tomar las decisiones.

B.19.3 Elementos de entrada

Un plan de proyecto con puntos de decisión. La información sobre posibles resultados de las decisiones y sobre la probabilidad de sucesos que pudiesen afectar a las decisiones.

B.19.4 Proceso

Un árbol de decisiones comienza con una decisión inicial, por ejemplo proceder con el proyecto A en vez de con el proyecto B. Como los dos proyectos anteriores son hipotéticos, se producirán sucesos diferentes y será necesario tomar diferentes decisiones previsibles. Estas se presentan en formato de árbol, similar al árbol de sucesos. La probabilidad de los sucesos se puede estimar junto con los costes o la utilidad del resultado final del camino seguido.

La información concerniente al mejor camino de decisión es lógicamente la que produce el valor previsto más alto, calculado como el producto de todas las probabilidades condicionales a lo largo del camino y el valor de la consecuencia.

B.19.5 Resultados

Los resultados incluyen:

- un análisis lógico del riesgo, presentando las diferentes opciones que se pueden tomar;
- un cálculo del valor esperado de cada posible camino a seguir.

B.19.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- proporcionan una presentación gráfica clara de los detalles de un problema de decisión;
- permiten calcular el mejor camino a seguir en una situación.

Las limitaciones incluyen:

- los árboles de decisiones muy grandes pueden llegar a ser demasiado complejos para una comunicación fácil con otras partes;
- puede existir una tendencia a simplificar en exceso la situación, de manera que se pueda presentar como un diagrama en árbol.

B.20 Análisis de la fiabilidad humana (HRA)

B.20.1 Presentación

El análisis de la fiabilidad humana (HRA) se ocupa del impacto de las personas sobre el rendimiento del sistema, y se puede utilizar para evaluar la influencia de los errores humanos en el sistema.

Muchos procesos pueden ser objeto de errores humanos, especialmente cuando el tiempo disponible para que el operador tome decisiones es muy corto. La probabilidad de que los problemas se desarrollen suficientemente para convertirse en problemas serios puede ser pequeña. Sin embargo, a veces las acciones humanas serán la única defensa para impedir que un fallo inicial progrese hasta convertirse en un accidente.

La importancia de la HRA ha sido ilustrada por varios accidentes en los que errores humanos críticos han contribuido a una secuencia catastrófica de sucesos. Tales accidentes eran avisos contra apreciaciones del riesgo que estaban enfocadas únicamente a los elementos materiales y lógicos de un sistema. Estos accidentes ilustran los peligros de ignorar la posibilidad de la contribución de los errores humanos. Además, las HRAs son útiles para resaltar errores que pueden dificultar la productividad y para revelar caminos donde estos errores y otros fallos (hardware y software) pueden ser "recuperados" por los operadores humanos y por el personal de mantenimiento.

B.20.2 Utilización

La HRA se puede utilizar cualitativa o cuantitativamente. De manera cualitativa se utiliza para identificar el potencial de errores humanos y sus causas, de forma que se pueda reducir la probabilidad de error. La HRA cuantitativa se utiliza para proporcionar datos sobre fallos humanos en el FTA o en otras técnicas.

B.20.3 Elementos de entrada

Los elementos de entrada a la HRA incluyen:

- información para definir tareas que deberían ser realizadas por personas;
- experiencia de los tipos de error que se producen en la práctica y el potencial de error;
- conocimientos técnicos sobre errores humanos y la cuantificación de los mismos.

B.20.4 Proceso

El proceso de la HRA es el siguiente:

- **Definición del problema**, ¿qué tipos de implicaciones humanas se han de investigar/evaluar?
- **Análisis de la tarea**, ¿cómo se realizará la tarea y qué tipo de ayudas serán necesarias para apoyar el rendimiento?
- **Análisis de errores humanos**, ¿cómo puede fallar el rendimiento de la tarea: qué errores pueden ocurrir y cómo se pueden recuperar?
- **Representación**, ¿cómo estos errores o fallos en el rendimiento de la tarea se pueden integrar con otros sucesos, materiales, lógicos o ambientales para permitir que se puedan calcular las probabilidades de fallo del sistema general?
- **Filtrado**, ¿existen algunos errores o tareas que no requieran una cuantificación detallada?
- **Cuantificación**, ¿cuál es la probabilidad de errores y de fallos individuales de las tareas?
- **Evaluación del impacto**, ¿qué errores o tareas son más importantes, es decir, cuales son las que tienen la mayor contribución a la fiabilidad o al riesgo?
- **Reducción de errores**, ¿cómo se puede conseguir la fiabilidad humana más alta?
- **Documentación**, ¿qué detalles de la HRA es necesario documentar?

En la práctica, el proceso de la HRA se realiza escalonadamente, aunque algunas veces con partes (por ejemplo, análisis de tareas e identificación de errores) que se realizan en paralelo con alguna otra.

B.20.5 Resultados

Los resultados incluyen:

- una lista de los errores que pueden ocurrir y los métodos con los que se pueden reducir – preferiblemente mediante rediseño del sistema;
- los modos de error, los tipos de error, las causas y las consecuencias;
- una apreciación cualitativa o cuantitativa del riesgo planteada por los errores;

B.20.6 Fortalezas y limitaciones

Las fortalezas de la HRA incluyen:

- la HRA proporciona un mecanismo formal para incluir los errores humanos en consideración de los riesgos asociados con sistemas en los que con frecuencia las personas juegan un papel importante;
- la consideración formal de los modos y mecanismos de los errores humanos pueden ayudar a reducir la probabilidad de fallos debidos a errores.

Las limitaciones incluyen:

- la complejidad y variabilidad de las personas, que hacen la definición de los modos de fallo simples y dificultan la probabilidad;
- muchas actividades de las personas no tienen un modo de pasa/no pasa simple. La HRA tiene dificultades al tratar fallos parciales o fallos de calidad o de toma de decisiones deficiente.

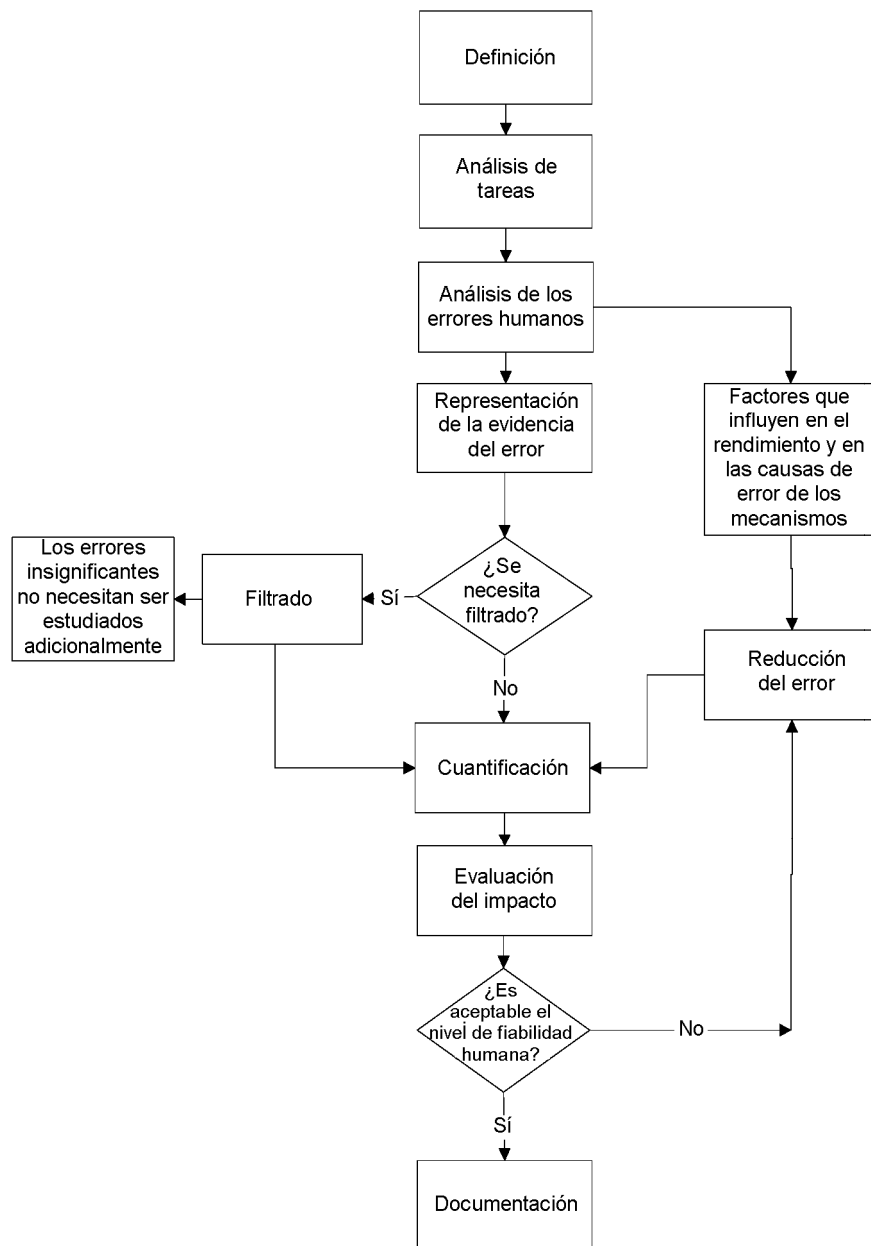


Figura B.7 – Ejemplo de evaluación de la fiabilidad humana

B.21 Análisis de pajarita

B.21.1 Presentación

El análisis de pajarita es un método esquemático sencillo para describir y analizar los caminos de un riesgo desde las causas hasta las consecuencias. Se puede considerar que es una combinación del pensamiento de un árbol de fallos que analiza la causa de un suceso (representado por el nudo de una corbata de pajarita) y un árbol de sucesos que analiza las consecuencias. No obstante, el enfoque del diagrama de pajarita se centra en las barreras entre las causas y el riesgo, y el riesgo y las consecuencias. Los diagramas de pajarita se pueden elaborar a partir del árbol de fallos y del árbol de sucesos, pero con más frecuencia se obtienen directamente de una sesión de tormenta de ideas.

B.21.2 Utilización

El análisis de pajarita se utiliza para presentar un riesgo mostrando una gama de causas y consecuencias posibles. Se utiliza cuando la situación no justifica la complejidad de un análisis de árbol de fallos completo o cuando se trata más de asegurar que existe una barrera o control para cada camino de fallo. Este análisis es útil cuando existen caminos independientes y claros que tratan el fallo.

Con frecuencia, el análisis de pajarita es más fácil de entender que los árboles de fallos y de sucesos, y por ello puede ser una herramienta de comunicación útil cuando el análisis se obtiene mediante la utilización de técnicas más complejas.

B.21.3 Elementos de entrada

Se requiere la comprensión de la información sobre las causas y consecuencias de un riesgo y de las barreras y controles que pueden impedir, mitigar o estimular el riesgo.

B.21.4 Proceso

El análisis de pajarita se elabora de la manera siguiente:

- a) Mediante análisis se identifica un riesgo particular y se representa como el nudo central de una corbata de pajarita.
- b) Se listan las causas del suceso considerando los orígenes del riesgo (o peligros en un contexto de seguridad).
- c) Se identifica el mecanismo mediante el cual el origen del riesgo conduce al suceso crítico.
- d) Se trazan las líneas entre cada causa y el suceso, formando el lado izquierdo del diagrama de pajarita. Los factores que podrían llevar a una intensificación se pueden identificar e incluir en el diagrama.
- e) Las barreras que deberían impedir que cada causa conduzca a consecuencias no deseadas se pueden representar como barras verticales a través de la línea. Cuando existan factores que pudiesen dar lugar a que se produzca una intensificación, también se pueden representar las barreras contra la intensificación. El enfoque se puede aplicar para consecuencias positivas cuando las barras reflejen 'controles' que estimulen la generación del suceso.
- f) En el lado derecho del diagrama de pajarita se identifican las diferentes consecuencias posibles del riesgo y se trazan las líneas radiales que unen el suceso del riesgo con cada consecuencia posible.
- g) Las barreras a las consecuencias se representan como barras que cruzan las líneas radiales. El enfoque se puede aplicar para consecuencias positivas cuando las barras reflejen 'controles' que soportan la generación de consecuencias.
- h) Las funciones de gestión que soportan controles (tales como formación e inspección) se pueden mostrar bajo el diagrama de pajarita y unidas a sus controles respectivos.

Algún nivel de cuantificación de un diagrama de pajarita puede ser posible cuando los caminos son independientes, la probabilidad de una consecuencia o resultado particular es conocida, y la eficacia de un control se puede estimar mediante un número. No obstante, en muchas situaciones, los caminos y las barreras no son independientes y los controles pueden ser de procedimiento y por tanto la efectividad no es clara. Con frecuencia, la cuantificación se consigue de forma más apropiada aplicando análisis FTA y ETA.

B.21.5 Resultados

El resultado es un diagrama sencillo que muestra los caminos del riesgo principal y las barreras colocadas para impedir o mitigar las consecuencias no deseadas o estimular y promover las consecuencias deseadas.

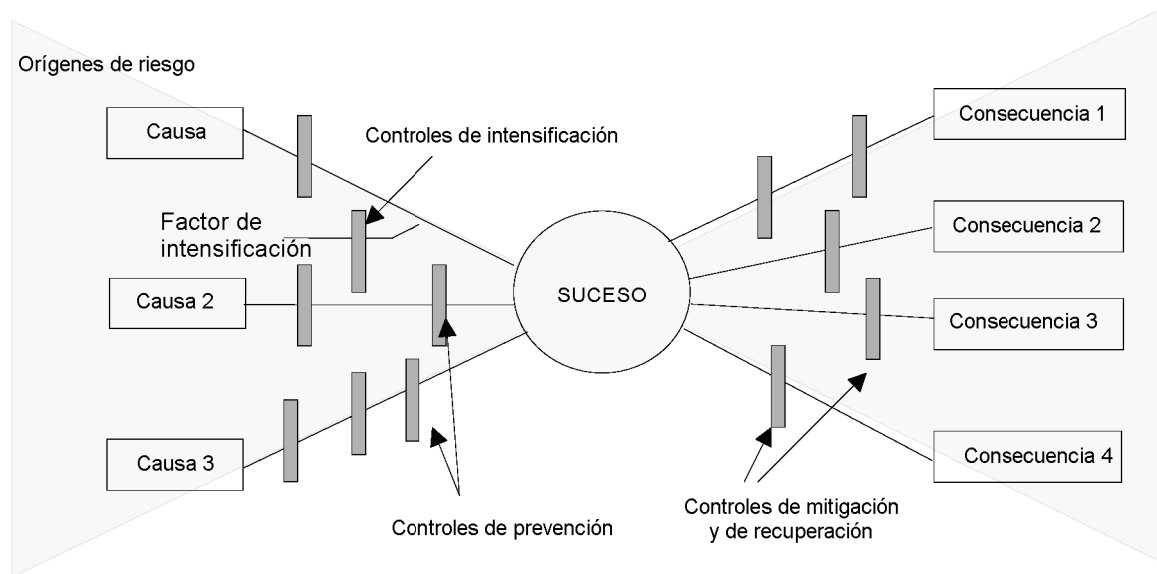


Figura B.8 – Ejemplo de diagrama de pajarita para consecuencias no deseadas

B.21.6 Fortalezas y limitaciones

Fortalezas del análisis de pajarita:

- es simple de comprender y proporciona una representación pictórica clara del problema;
- enfoca su atención sobre los controles que se supone que están colocados para prevención y mitigación y sobre sus consecuencias;
- se puede utilizar para consecuencias deseables;
- no es necesario un alto nivel de conocimientos técnicos para utilizarlo.

Las limitaciones incluyen:

- no se puede representar cuando se producen múltiples causas simultáneamente que originan consecuencias (es decir, cuando existen salidas "AND" ("Y") en un árbol de fallos situadas en el lado izquierdo del nudo);
- puede simplificar al máximo situaciones complejas, en particular cuando se trata de conseguir la cuantificación.

B.22 Mantenimiento centrado en la fiabilidad

B.22.1 Presentación

El mantenimiento centrado en la fiabilidad (RCM) es un método para identificar las políticas que se deberían implantar para gestionar los fallos de manera que se obtenga de forma eficiente y efectiva la seguridad requerida, la disponibilidad y economía de funcionamiento para todos los tipos de equipos.

El RCM es ahora una metodología probada y aceptada que se utiliza en una amplia gama de industrias.

El RCM proporciona un proceso de decisión para identificar requisitos de mantenimiento preventivo eficaces para los equipos, de acuerdo con las consecuencias de seguridad, operacionales y económicas de fallos identificables, y el mecanismo de degradación responsable de esos fallos. El resultado final de trabajar a lo largo de todo el proceso es un juicio sobre la necesidad de realizar una tarea de mantenimiento u otras acciones tales como cambios operacionales. La Norma IEC 60300-3-11 proporciona detalles relativos a la utilización y aplicación del RCM.

B.22.2 Utilización

Todas las tareas se basan en la seguridad de las personas y del medio ambiente, y en el interés operacional y económico. No obstante, se debería indicar que los criterios considerados dependerán de la naturaleza del producto y de su aplicación. Por ejemplo, un proceso de producción necesitará ser viable económicamente, y puede ser sensible a consideraciones ambientales estrictas, mientras que un artículo de un equipo de defensa debería ser útil operacionalmente, pero puede tener unos criterios de seguridad, económicos y ambientales menos rigurosos. Los beneficios más grandes se pueden conseguir mediante la elección de objetivos del análisis dirigidos hacia donde los fallos tuviesen efectos de seguridad, ambientales, económicos u operacionales más serios.

El RCM se utiliza para asegurar que se realiza un mantenimiento aplicable y efectivo, y que generalmente se aplica durante la fase de diseño y de desarrollo y después se implanta durante las fases de funcionamiento y mantenimiento.

B.22.3 Elementos de entrada

La aplicación con éxito del RCM exige un buen conocimiento del equipo y de la estructura, del entorno operacional y de los sistemas, subsistemas y artículos de equipo asociados, así como de los fallos posibles y de las consecuencias de estos fallos.

B.22.4 Proceso

Las etapas básicas de un programa RCM son las siguientes:

- iniciación y planificación;
- análisis de fallos funcionales;
- selección de la tarea;
- implantación;
- mejora continua.

El RCM se basa en el riesgo ya que sigue las etapas básicas de la apreciación del riesgo. El tipo de apreciación del riesgo es un análisis del modo de fallo, del efecto y de la criticidad (FMECA), pero requiere un enfoque específico de análisis cuando se utiliza en este contexto.

La identificación del riesgo está enfocada a situaciones en que los fallos potenciales se pueden eliminar o reducir en la frecuencia y/o en las consecuencias, mediante la realización de tareas de mantenimiento. Se realiza para identificar las funciones requeridas y las normas de funcionamiento y los fallos del equipo y de componentes que pueden interrumpir estas funciones.

El análisis de riesgo consiste en la estimación de la frecuencia de cada fallo sin que se haya realizado mantenimiento. Las consecuencias se establecen definiendo los efectos del fallo. Una matriz de riesgo que combine la frecuencia del fallo y sus consecuencias permite establecer categorías de niveles de riesgo.

Después se realiza la evaluación del riesgo seleccionando la política de gestión del fallo apropiada para cada modo de fallo.

El proceso RCM completo se documenta de forma extensiva para futuras consultas y revisiones. La recolección de los datos relativos al fallo y al mantenimiento permite el seguimiento de los resultados y la implantación de mejoras.

B.22.5 Resultados

El RCM proporciona una definición de tareas de mantenimiento tales como el seguimiento de la condición, la renovación programada, la sustitución programada, la localización de fallos o el mantenimiento no preventivo. Otras posibles acciones que pueden resultar del análisis son el rediseño, los cambios a incluir en los procedimientos de funcionamiento o de mantenimiento o de formación adicional. Después se identifican los intervalos de las tareas y los recursos que se necesitan.

B.22.6 Normas para consulta

IEC 60300-3-11, *Gestión de la confiabilidad. Parte 3-11: Guía de aplicación. Mantenimiento centrado en la fiabilidad.*

B.23 Análisis de fugas (SA) y análisis del circuito de fuga (SCA)

B.23.1 Presentación

El análisis de fugas (SA) es una metodología para identificar errores de diseño. Una condición de fuga es una condición de hardware, software o integrada latente, que puede hacer que se produzca un suceso no deseado o que puede inhibir un suceso deseado, y que no es causada por fallo de componentes. Estas condiciones se caracterizan por su naturaleza aleatoria y por la facilidad para escapar de la detección durante los ensayos más rigurosos del sistema normalizado. Las condiciones de fuga pueden dar lugar a un funcionamiento incorrecto, a la pérdida de disponibilidad del sistema, a retrasos del programa, o incluso a lesiones o la muerte de personas.

B.23.2 Utilización

El análisis del circuito de fuga (SCA) fue desarrollado por la NASA en los últimos años de la década de 1960 para verificar la integridad y la funcionalidad de sus diseños. Ha servido como una herramienta útil para descubrir caminos no intencionados en circuitos eléctricos, y para ayudar a imaginar soluciones para aislar cada función. No obstante, como la tecnología avanza, las herramientas para el análisis de los circuitos de fuga también han tenido que avanzar. El análisis de fugas incluye e incluso supera la cobertura del análisis del circuito de fuga. Puede localizar problemas de hardware y de software utilizando cualquier tecnología. Las herramientas de análisis de fugas pueden integrar diversos análisis tales como los de árboles de fallo, análisis del modo de fallo y de los efectos (FMEA), estimaciones de fiabilidad, etc., en un único análisis que ahorre tiempo y costes del proyecto.

B.23.3 Elementos de entrada

El análisis de fugas es único a partir del proceso de diseño, y por la razón de que utiliza diferentes herramientas (árboles de red, bosques, e indicios o preguntas para ayudar al analista a identificar las condiciones de fuga) para descubrir un tipo de problema específico. Los árboles de red y los bosques son agrupaciones topológicas del sistema actual. Cada árbol de red representa una subfunción y muestra todas las entradas que pueden afectar a la salida de la subfunción. Los bosques se forman combinando árboles de red que contribuyen a una salida particular del sistema. Un bosque correcto muestra una salida del sistema en función de todas sus entradas relacionadas. Estas, junto con otras, pasan a ser las entradas para el análisis.

B.23.4 Proceso

Las etapas básicas para realizar un análisis de fugas son:

- la preparación de datos;
- la construcción del árbol de red;

- la evaluación de los caminos de la red;
- las recomendaciones finales y el informe.

B.23.5 Resultados

Un circuito de fuga es un camino no previsto o un flujo lógico dentro de un sistema que, bajo determinadas condiciones, puede iniciar una función no deseada o inhibir una función deseada. El camino puede consistir en elementos materiales, lógicos, acciones del operador, o combinaciones de estos elementos. Los circuitos de fuga no son el resultado de fallos materiales, pero son condiciones latentes, diseñadas inadvertidamente en el sistema, codificadas en programas del software, o impelidas por un error humano. Existen cuatro categorías de circuitos de fuga:

- a) caminos de fuga: caminos no previstos a lo largo de los cuales la corriente, la energía, o una secuencia lógica discurre en una dirección imprevista;
- b) cadencia de fuga: sucesos que ocurren en una secuencia imprevista o conflictiva;
- c) indicaciones de fuga: presentaciones ambiguas o falsas del sistema funcionando en condiciones que pueden hacer que el sistema o un operador realice una acción no deseada;
- d) etiquetas de fuga: etiquetado incorrecto o impreciso de funciones del sistema, por ejemplo, entradas del sistema, controles, caminos principales para señales de presentación, que pueden hacer que un operador aplique un estímulo incorrecto al sistema.

B.23.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- el análisis de fugas es bueno para identificar errores de diseño;
- este análisis funciona mejor cuando se aplica conjuntamente con estudios de peligros y de operatividad (HAZOP);
- es muy bueno para tratar sistemas que tengan múltiples estados, tales como planta por lotes o por mitades de lotes.

Las limitaciones pueden incluir:

- que el proceso sea algo diferente dependiendo de si se aplica a circuitos eléctricos, plantas de proceso, equipo mecánico o software;
- el método es dependiente de que se establezcan árboles de red correctos.

B.24 Análisis Markov

B.24.1 Presentación

El análisis Markov se aplica cuando el estado futuro de un sistema depende únicamente de su estado actual. Por lo general, se aplica para analizar sistemas reparables que pueden existir en múltiples estados, y el empleo de un análisis en bloque de fiabilidad sería inapropiado para analizar adecuadamente el sistema. El método se puede ampliar a sistemas más complejos mediante la utilización de procesos Markov de nivel más elevado, y solo se restringe por modelos, cálculos matemáticos y supuestos.

El proceso de análisis Markov es una técnica cuantitativa, y puede ser discontinua (aplicando probabilidades de cambio entre los estados) o continua (aplicando tasas de cambio a través de los estados).

Mientras un análisis Markov se puede realizar manualmente, la naturaleza de las técnicas se presta por sí misma al empleo de programas informáticos, muchos de los cuales están disponibles en el mercado.

B.24.2 Utilización

La técnica del análisis Markov se puede aplicar sobre diversas estructuras de sistema, con o sin reparación, incluyendo:

- componentes independientes instalados en paralelo;
- componentes independientes instalados en serie;
- sistema de carga compartida;
- sistema en espera, incluyendo el caso en que se pueda producir un fallo de conmutación;
- sistemas degradados.

La técnica del análisis Markov también se puede aplicar para calcular la disponibilidad, incluyendo el tener en cuenta los componentes de repuesto para reparaciones.

B.24.3 Elementos de entrada

Los elementos de entrada esenciales para un análisis Markov son las siguientes:

- lista de los diversos estados en que el sistema, subsistema o componente se puede encontrar (por ejemplo, totalmente operativo, parcialmente operativo (es decir, en un estado degradado), estado de fallo, etc.);
- un conocimiento claro de las posibles transiciones que se necesitan para modelarlo. Por ejemplo, el fallo de un neumático de coche necesita tener en consideración el estado de la rueda de repuesto y por tanto la frecuencia de inspección de ésta);
- régimen de cambio de un estado a otro, representado normalmente por una tasa de cambio entre estados de sucesos discontinuos, o el régimen de fallo (λ) y/o el régimen de reparación (μ) para sucesos continuos.

B.24.4 Proceso

La técnica del análisis Markov se centra alrededor del concepto de "estados", por ejemplo "disponible" y "estado de fallo", así como en la transición entre estos dos estados en el tiempo basada en una probabilidad de cambio constante. Para describir la transición entre cada uno de los estados se utiliza una matriz de probabilidad de transición estocástica que permite el cálculo de los diversos resultados.

Para ilustrar la técnica del análisis Markov, se considera un sistema complejo que solo pueda estar en tres estados: de funcionamiento, degradado y de fallo, que se definen como estados S1, S2 y S3 respectivamente. Cada día, el sistema se encuentra en uno de estos tres estados. La tabla B.2 muestra la probabilidad de que mañana el sistema se encuentre en el estado S_i donde i puede ser 1, 2 ó 3.

Tabla B.2 – Matriz Markov

		Estado de hoy		
		S1	S2	S3
Estado de mañana	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Esta disposición de probabilidades se denomina matriz Markov o matriz de transición. Se debe resaltar que la suma de cada una de las columnas es 1 y que son la suma de todas las salidas posibles en cada caso. El sistema también se puede representar mediante un diagrama Markov, donde los círculos representan los estados, y las flechas representan la transición, junto a la probabilidad vinculada.

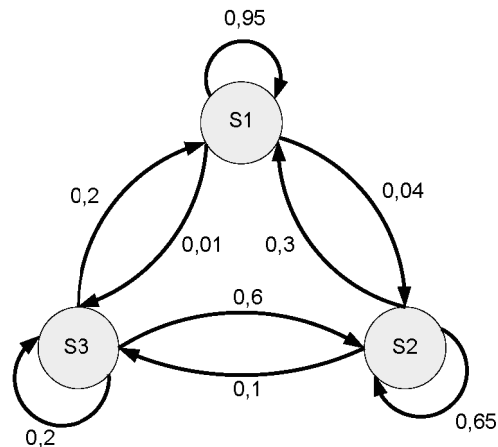


Figura B.9 – Ejemplo de diagrama Markov

Normalmente las flechas para pasar de un estado a éste mismo no se muestran, pero en estos ejemplos se muestran para que el diagrama se vea completo.

Si P_i representa la probabilidad de encontrar el sistema en el estado i para $i = 1, 2, 3$, entonces las ecuaciones simultáneas a resolver son:

$$P_1 = 0,95 P_1 + 0,30 P_2 + 0,20 P_3 \quad (\text{B.1})$$

$$P_2 = 0,04 P_1 + 0,65 P_2 + 0,60 P_3 \quad (\text{B.2})$$

$$P_3 = 0,01 P_1 + 0,05 P_2 + 0,20 P_3 \quad (\text{B.3})$$

Estas tres ecuaciones no son independientes y no resolverán las tres incógnitas. Se debería utilizar la ecuación siguiente y descartar una de las ecuaciones anteriores.

$$1 = P_1 + P_2 + P_3 \quad (\text{B.4})$$

La solución es 0,85, 0,13 y 0,02 para los respectivos estados 1, 2 y 3. El sistema está totalmente operativo durante el 85% del tiempo, en estado degradado durante el 13% del tiempo y en estado de fallo durante el 2% del tiempo.

Se consideran dos elementos que funcionen en paralelo y se requiere que estén operativos para que el sistema funcione. Los elementos pueden estar en estado operativo o de fallo y la disponibilidad del sistema depende del estado de los elementos.

Los estados se pueden considerar como:

Estado 1: Los dos elementos están funcionando correctamente.

Estado 2: Un elemento ha fallado y está siendo reparado, y el otro elemento está funcionando.

Estado 3: Los dos elementos han fallado y uno de ellos está siendo reparado.

Si se asume que el régimen de fallo continuo de cada elemento es λ y que el régimen de reparación es μ , el diagrama de transición de estado es el siguiente:

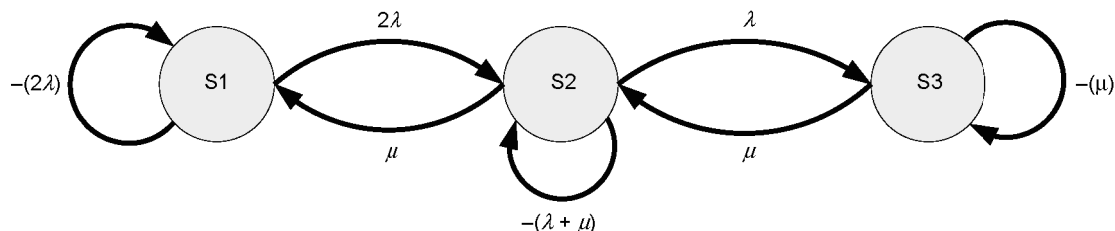


Figura B.10 – Ejemplo de diagrama de transición de estado

Se indica que la transición del estado 1 al estado 2 es 2λ como consecuencia del fallo de uno de los dos elementos y que el sistema pasará al estado 2.

Siendo $P_i(t)$ la probabilidad de estar en un estado inicial i en el momento t ; y

siendo $P_i(t + \delta t)$ la probabilidad de estar en un estado final en el momento $t + \delta t$.

La matriz de la probabilidad de transición pasaría a ser:

Tabla B.3 – Matriz Markov final

		Estado inicial		
		P1 (t)	P2 (t)	P3 (t)
Estado final	P1 (t + δt)	-2λ	μ	0
	P2 (t + δt)	2λ	-(λ + μ)	μ
	P3 (t + δt)	0	λ	-μ

Es necesario indicar que el valor cero se produce y no es posible pasar del estado 1 al estado 3 o del estado 3 al estado 1. También, que las columnas suman cero cuando se especifican tasas.

Las ecuaciones simultáneas pasan a ser:

$$dP1/dt = -2\lambda P1(t) + \mu P2(t) \quad (B.5)$$

$$dP2/dt = 2\lambda P1(t) + -(\lambda + \mu) P2(t) + \mu P3(t) \quad (B.6)$$

$$dP3/dt = \lambda P2(t) + -\mu P3(t) \quad (B.7)$$

Por simplicidad, se asumirá que la disponibilidad requerida es la disponibilidad en estado estable.

Cuando δt tiende a infinito, dP_i/dt tenderá a cero y las ecuaciones son más fáciles de resolver. También se debería utilizar la ecuación adicional mostrada anteriormente como ecuación (B.4):

Ahora la ecuación $A(t) = P1(t) + P2(t)$ se puede expresar como:

$$A = P1 + P2$$

$$\text{Por tanto, } A = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + \lambda^2)$$

B.24.5 Resultados

Los resultados de un análisis Markov son las diversas probabilidades de que el sistema esté en los diversos estados, y por tanto constituye una estimación de las probabilidades de fallo y/o de la disponibilidad, uno de los componentes esenciales de un sistema.

B.24.6 Fortalezas y limitaciones

Las fortalezas de un análisis Markov incluyen:

- la posibilidad de calcular las probabilidades de sistemas con una capacidad de reparación y diversos estados degradados.

Las limitaciones de un análisis Markov incluyen:

- el hecho de asumir probabilidades constantes de cambio de estado; de fallo o de reparaciones;
- todos los sucesos son independientes estadísticamente ya que los estados futuros son independientes de todos los estados pasados, excepto con el estado inmediatamente anterior;
- las necesidades de conocer todas las probabilidades de cambio de estado;
- el conocimiento de las operaciones matriciales;
- los resultados son difíciles de comunicar al personal no técnico.

B.24.7 Comparaciones

El análisis Markov es similar al análisis Petri-Net en cuanto a que puede realizar seguimiento y observar los estados del sistema, aunque difiere en que el análisis Petri-Net puede existir en múltiples estados al mismo tiempo.

B.24.8 Normas para consulta

IEC 61078, *Técnicas de análisis de la confiabilidad. Método del diagrama de bloques de la fiabilidad y métodos booleanos*.

IEC 61165, *Aplicación de las técnicas de Markov*.

ISO/IEC 15909 (todas las partes), *Ingeniería del software y de sistemas. Redes Petri de alto nivel*.

B.25 Simulación de Monte Carlo

B.25.1 Presentación

Muchos sistemas son demasiado complejos a causa de los efectos de incertidumbre, por lo que se deben modelar aplicando técnicas analíticas, pero se pueden evaluar considerando las entradas como variables aleatorias y realizando un número N de cálculos (también llamados simulaciones) mediante el muestreo de los elementos de entrada, con objeto de obtener N posibles consecuencias del resultado deseado.

Este método se puede aplicar a situaciones complejas que serían difíciles de entender y resolver mediante un método analítico. Se pueden desarrollar sistemas que utilicen hojas de cálculo y otras herramientas convencionales, aunque ya se encuentran disponibles herramientas más sofisticadas para aplicarlas a requisitos más complejos, muchas de las cuales son realmente económicas. Cuando la técnica se desarrolló en principio, el número de iteraciones requeridas para las simulaciones de Monte Carlo hacía que el proceso fuese lento y que consumiera mucho tiempo, pero los avances en la tecnología informática y en los desarrollos teóricos, tales como el muestreo del hipercubo Latino, han hecho que el tiempo de proceso sea casi insignificante para muchas aplicaciones.

B.25.2 Utilización

La simulación de Monte Carlo proporciona un medio para evaluar el efecto de la incertidumbre en una amplia gama de situaciones de los sistemas. Normalmente, se utiliza para evaluar la gama de posibles resultados y la frecuencia relativa de valores en esta gama de medidas cuantitativas de un sistema, tales como costes, duración, capacidad de tratamiento, demanda y medidas similares. La simulación de Monte Carlo se puede utilizar para dos fines diferentes:

- propagación de la incertidumbre sobre modelos analíticos convencionales;
- cálculo de probabilidades cuando no se puedan emplear técnicas analíticas.

B.25.3 Elementos de entrada

Los elementos de entrada a una simulación de Monte Carlo son un buen modelo del sistema, y la información sobre los tipos de elementos de entrada, las fuentes de incertidumbre que se han de representar, y los resultados que se requieren. Los datos de entrada con incertidumbre se representan como variables aleatorias con distribuciones que están más o menos dispersas según el nivel de incertidumbres. Para este fin se utilizan frecuentemente distribuciones uniformes, triangulares, normales y normales logarítmicas.

B.25.4 Proceso

El proceso es como sigue:

- a) Se define un modelo o algoritmo que represente de la forma más exacta posible el comportamiento del sistema que se está estudiando.
- b) El modelo se hace funcionar múltiples veces utilizando números aleatorios para producir salidas del modelo (simulaciones del sistema). Cuando la aplicación consista en modelar los efectos de la incertidumbre, el modelo tendrá la forma de una ecuación que proporcione la relación entre parámetros de entrada y una salida. Los valores seleccionados para los elementos de entrada se toman de distribuciones de probabilidad apropiadas que representen la naturaleza de la incertidumbre en esos parámetros.
- c) En uno u otro caso, con un ordenador se hacen múltiples iteraciones del modelo (con frecuencia hasta 10.000 veces) con entradas diferentes y se obtienen múltiples salidas. Estas se pueden procesar utilizando técnicas estadísticas convencionales para obtener informaciones tales como valores medios, desviación típica, intervalos de confianza.

A continuación se proporciona un ejemplo de una simulación.

Se considera el caso de dos elementos que funcionan en paralelo y el sistema solo necesita que funcione uno de ellos. El primer elemento tiene una fiabilidad de 0,9 y el otro de 0,8.

Se puede preparar una hoja de cálculo con las siguientes columnas.

Tabla B.4 – Ejemplo de simulación Monte Carlo

Número de simulación	Elemento 1		Elemento 2		Sistema
	Número aleatorio	¿Funciones?	Número aleatorio	¿Funciones?	
1	0,277 243	SÍ	0,059 355	SÍ	1
2	0,746 909	SÍ	0,311 324	SÍ	1
3	0,541 728	SÍ	0,919 765	NO	1
4	0,423 274	SÍ	0,643 514	SÍ	1
5	0,917 776	NO	0,539 349	SÍ	1
6	0,994 043	NO	0,972 506	NO	0
7	0,082 574	SÍ	0,950 241	NO	1
8	0,661 418	SÍ	0,919 868	NO	1
9	0,213 376	SÍ	0,367 555	SÍ	1
10	0,565 657	SÍ	0,119 215	SÍ	1

El generador aleatorio crea un número comprendido entre 0 y 1 que se utiliza para compararlo con la probabilidad de cada elemento, con objeto de determinar si el sistema es funcional. Justo con 10 iteraciones, no se debería esperar que el resultado de 0,9 sea un resultado preciso. El enfoque usual es trabajar con un baremo para comparar el resultado total a medida que avanza la simulación, hasta conseguir el nivel de seguridad que se requiere. En este ejemplo, después de 20 000 iteraciones se obtuvo un resultado de 0,979 9

El modelo anterior se puede ampliar de varias maneras. Por ejemplo:

- ampliando el propio modelo (considerando que el segundo elemento comienza a funcionar solo cuando el primer elemento falla);
- cambiando la probabilidad fijada a una variable (un buen ejemplo es la distribución triangular) cuando la probabilidad no se puede definir de forma precisa;
- utilizando regímenes de fallo combinados con la selección del número aleatorio para obtener un tiempo de fallo (con distribución exponencial, de Weibull, o de otro tipo adecuado) y transformarlo en tiempos de reparación.

Las aplicaciones incluyen, entre otras cosas, la evaluación de la incertidumbre en previsiones financieras, las características de las inversiones, los costes de proyecto y pronóstico del programa de fabricación, las interrupciones del proceso económico y los requisitos de dotación de personal.

Las técnicas analíticas no pueden proporcionar resultados relevantes o cuando hay incertidumbre en los datos de entrada y por tanto también en los resultados.

B.25.5 Resultados

Los resultados podrían ser un valor único, como se determinó en el ejemplo anterior, y también podría ser un resultado expresado como la distribución de probabilidad o de frecuencia, o podría ser la identificación de las funciones principales dentro del modelo que tiene el mayor impacto sobre el resultado.

Por lo general, se utilizará una simulación de Monte Carlo para evaluar la distribución completa de consecuencias que se producirían o las medidas claves de una distribución, tales como:

- la probabilidad de que se produzca una consecuencia definida;
- el valor de una consecuencia para el cual los responsables del problema tienen un determinado nivel de confianza que no se excederá o sobrepasará, unos costes que tienen menos de un 10% de posibilidad de que sean excedidos, o una duración que tiene un 80% de certeza de ser excedida.

Un análisis de las relaciones entre los elementos de entrada y los resultados puede arrojar luz sobre la importancia relativa de los factores en uso, e identificar objetivos útiles para los esfuerzos que influyen en la incertidumbre de los resultados.

B.25.6 Fortalezas y limitaciones

Las fortalezas del análisis de Monte Carlo son las siguientes:

- el método se puede acomodar, en principio, a cualquier distribución en una variable de entrada, incluyendo distribuciones empíricas obtenidas de observaciones de sistemas afines;
- los modelos son relativamente simples de desarrollar y se pueden ampliar a medida que se necesite;
- todas las influencias o relaciones que surjan en la realidad se pueden representar, incluyendo efectos sutiles tales como dependencias condicionales;
- se puede aplicar el análisis de sensibilidad con objeto de identificar influencias intensas y débiles;
- los modelos se pueden entender fácilmente dado que la relación entre los elementos de entrada y los resultados es transparente;
- hay disponibles modelos de comportamiento eficiente, tal como el Petri Nets (futura Norma IEC 62551) que han demostrado ser muy válidos para los fines de la simulación de Monte Carlo;
- proporciona una medida de la exactitud de un resultado;
- el software es fácil de obtener y relativamente económico.

Las limitaciones son las siguientes:

- la exactitud de las soluciones depende del número de simulaciones que se puedan realizar (esta limitación comienza a ser menos importante a causa de las velocidades crecientes de los ordenadores actuales);
- puede representar incertidumbres en parámetros para una distribución válida;
- los modelos grandes y complejos pueden desafiar al modelador y hacer difícil a las partes interesadas acoplarse con el proceso;
- la técnica puede no ponderar adecuadamente los sucesos de elevadas consecuencias/baja probabilidad y por tanto no permitir que en el análisis se refleje un deseo de riesgo de la organización.

B.25.7 Normas para consulta

IEC 61649, *Análisis de Weibull*.

IEC 62551, *Técnicas de análisis de la confiabilidad. Técnicas de red Petri* ¹⁾.

1) Actualmente sometida a consideración.

ISO/IEC Guide 98-3:2008, *Medición de la incertidumbre. Parte 3: Guía para la medición de la incertidumbre (GUM:1995)*.

B.26 Estadísticas y redes Bayesianas

B.26.1 Presentación

Las estadísticas Bayesianas se atribuyen al reverendo Thomas Bayes. Su premisa es que cualquier información ya conocida (la Previa) se puede combinar con mediciones ulteriores (la Posterior) para establecer una probabilidad global. El teorema de Bayes se puede expresar de una manera general como:

$$P(A|B) = \{P(A)P(B|A)\} / \sum_i P(B|E_i)P(E_i)$$

donde

la probabilidad de X se indica por $P(X)$;

la probabilidad de X sobre la condición de que Y ha ocurrido se indica por $P(X|Y)$; y

E_i es el suceso número i .

En su forma más simplificada se reduce a $P(A|B) = \{P(A)P(B|A)\} / P(B)$.

Las estadísticas Bayesianas difieren de las estadísticas clásicas en que no asumen que todos parámetros de distribución son fijos, sino que estos parámetros son variables aleatorias. Una probabilidad Bayesiana se puede comprender fácilmente si se considera como un grado de creencia personal en un determinado suceso, en oposición a la estadística clásica que se basa en la evidencia física. Como el enfoque Bayesiano se basa en la interpretación subjetiva de la probabilidad, proporciona una base fácil para pensar en decisiones y para el desarrollo de redes Bayesianas (o redes veraces, redes de opinión o redes Bayesianas).

Las redes Bayesianas utilizan un modelo gráfico para representar un conjunto de variables y sus relaciones de probabilidad. La red se compone de nudos que representan una variable aleatoria y de flechas que unen un nudo padre con un nudo hijo [cuando un nudo padre es una variable que influye directamente sobre otra variable (hijo)].

B.26.2 Utilización

En los últimos años ha aumentado y se ha extendido el empleo de la teoría y de las redes Bayesianas, en parte debido a su interés intuitivo y también a causa de la disponibilidad de programas de software para tratamiento informático. Las redes Bayesianas se utilizan en una amplia gama de temas: diagnóstico médica, modelación de imágenes, estudios genéticos, reconocimiento de la voz, estudios económicos, exploración espacial y en los motores de búsqueda de gran potencia en la red utilizados actualmente. Estas redes se pueden valorar en cualquier área donde exista el requisito de investigar sobre variables desconocidas mediante la utilización de relaciones estructurales y de datos. Las redes Bayesianas se pueden utilizar para aprender las relaciones causales que proporcionan la comprensión del ámbito de un problema y predecir las consecuencias de la intervención.

B.26.3 Elementos de entrada

Los elementos de entrada son similares a las de un modelo de Monte Carlo. Para una red Bayesiana, los ejemplos de los pasos a seguir incluyen lo siguiente:

- definir las variables del sistema;
- definir las uniones causales entre variables;

- especificar las probabilidades condicionales y las probabilidades previas;
- añadir la evidencia a la red;
- actualizar opiniones;
- sacar opiniones posteriores.

B.26.4 Proceso

La teoría de Bayes se puede aplicar en una amplia variedad de temas. Este ejemplo considerará la creación de una tabla Bayes en la que se utilizará un ensayo médico para determinar si el paciente tiene una enfermedad. Antes de realizar el ensayo la creencia es que el 99% de la población no tiene esa enfermedad y que el 1% si la padece, es decir, la información Previa. La precisión del ensayo ha mostrado que el paciente tiene la enfermedad, el resultado del ensayo es positivo el 98% de las veces. También existe una probabilidad de que si no tiene la enfermedad, el resultado del ensayo sea positivo el 10% de las veces. La tabla de Bayes proporciona la siguiente información:

Tabla B.5 – Datos de la tabla de Bayes

	PREVIA	PROBABILIDAD	PRODUCTO	POSTERIOR
Tiene enfermedad	0,01	0,98	0,009 8	0,090 1
No tiene enfermedad	0,99	0,10	0,099 0	0,909 9
TOTAL	1		0,108 8	1

Aplicando la regla de Bayes, se determina el producto combinando la información previa y la probabilidad. La información posterior se obtiene dividiendo el valor del producto por el total del producto. El resultado muestra que un resultado de ensayo positivo indica que la información previa ha aumentado del 1% al 9%. Más importante aún, es que existe una gran posibilidad de que incluso con un ensayo positivo, es improbable que el paciente tenga la enfermedad. El examen de la ecuación $(0,01 \times 0,98) / ((0,01 \times 0,98) + (0,99 \times 0,1))$ muestra que el valor 'no tiene enfermedad-resultado positivo' juega un importante papel en los valores posteriores.

Se considera la siguiente red de Bayes:

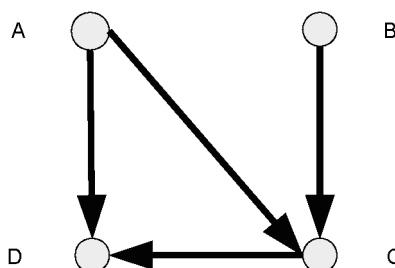


Figura B.11 – Muestra de red de Bayes

Con las probabilidades condicionales previas definidas en las tablas siguientes, y utilizando la anotación de que Y indica positivo y N indica negativo, el positivo debería ser "tener la enfermedad" como anteriormente, o sería Alta y N sería Baja.

Tabla B.6 – Probabilidades previas para los nudos A y B

$P(A = Y)$	$P(A = N)$	$P(B = Y)$	$P(B = N)$
0,9	0,1	0,6	0,4

Tabla B.7 – Probabilidades condicionales para el nudo C con el nudo A y el nudo B definidos

A	B	$P(C = Y)$	$P(C = N)$
Y	Y	0,5	0,5
Y	N	0,9	0,1
N	Y	0,2	0,8
N	N	0,7	0,3

Tabla B.8 – Probabilidades condicionales para el nudo D con el nudo A y el nudo C definidos

A	C	$P(D = Y)$	$P(D = N)$
Y	Y	0,6	0,4
Y	N	1,0	0,0
N	Y	0,2	0,8
N	N	0,6	0,4

Para determinar la probabilidad posterior de $P(A|D=N, C=Y)$, primero es necesario calcular $P(A,B|D=N, C=Y)$.

Aplicando la regla de Bayes, el valor $P(D|A,C)P(C|A,B)P(A)P(B)$ se determina como se indica a continuación, y la última columna muestra las probabilidades normalizadas cuyas sumas hasta 1 se obtienen en el ejemplo anterior (resultado redondeado).

Tabla B.9 – Probabilidad posterior para los nudos A y B con el nudo D y el nudo C definidos

A	B	$P(D A, C)P(C A,B)P(A)P(B)$	$P(A,B D=N, C=Y)$
Y	Y	$0,4 \times 0,5 \times 0,9 \times 0,6 = 0,110$	0,4
Y	N	$0,4 \times 0,9 \times 0,9 \times 0,4 = 0,130$	0,48
N	Y	$0,8 \times 0,2 \times 0,1 \times 0,6 = 0,010$	0,04
N	N	$0,8 \times 0,7 \times 0,1 \times 0,4 = 0,022$	0,08

Para obtener $P(A|D=N, C=Y)$, es necesario asumir todos los valores de B :

Tabla B.10 – Probabilidad posterior para el nudo A con el nudo D y el nudo C definidos

$P(A=Y D=N,C=Y)$	$P(A=N D=N,C=Y)$
0,88	0,12

Esto muestra que la probabilidad previa para $P(A=N)$ ha aumentado desde 0,1 hasta una probabilidad posterior de 0,12, lo que solo supone un cambio pequeño. Por otro lado, $P(B=N|D=N,C=Y)$ ha cambiado desde 0,4 a 0,56, lo que supone un cambio más importante.

B.26.5 Resultados

El enfoque Bayesiano se puede aplicar con la misma amplitud que las estadísticas clásicas con una amplia gama de resultados, por ejemplo, análisis de datos para obtener estimadores puntuales e intervalos de confianza. Su reciente popularidad está en relación con las redes de Bayes para obtener distribuciones posteriores. La representación gráfica de resultados proporciona un modelo fácil de comprender, y los datos se pueden modificar fácilmente para considerar las correlaciones y la sensibilidad de los parámetros.

B.26.6 Fortalezas y limitaciones

Fortalezas:

- todo lo que es necesario es conocido, es el conocimiento previo;
- los enunciados deductivos son fáciles de comprender;
- la regla de Bayes es todo lo que se requiere;
- proporciona un mecanismo para utilizar creencias subjetivas en un problema.

Limitaciones:

- el hecho de definir todas las interacciones en las redes Bayesianas para sistemas complejos es un asunto problemático;
- el enfoque Bayesiano necesita el conocimiento de una multitud de probabilidades condicionales que por lo general son proporcionadas por los juicios de expertos. Las herramientas de software solamente pueden proporcionar respuestas basadas en estas presunciones.

B.27 Curvas FN

B.27.1 Resumen

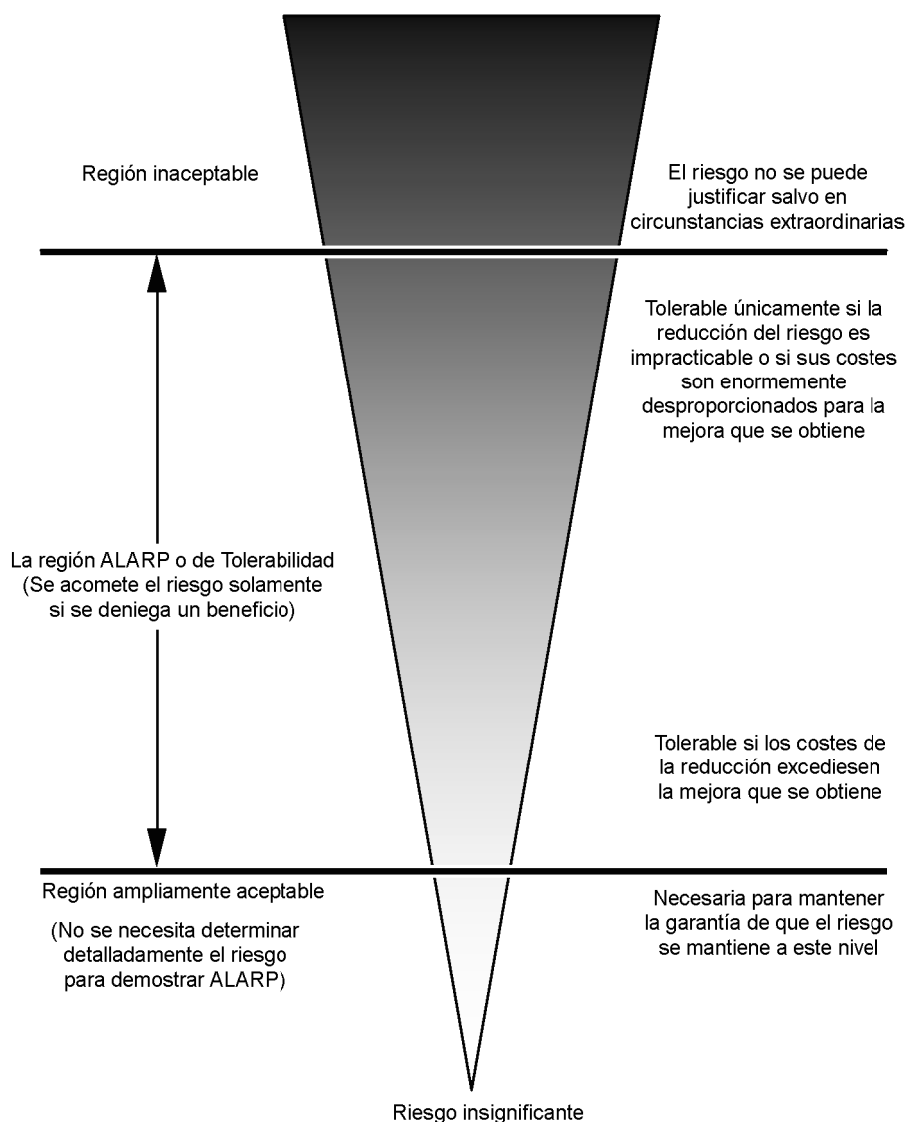


Figura B.12 – El concepto ALARP ("tan bajo como razonablemente sea posible")

Las curvas FN son una representación gráfica de la probabilidad de que los sucesos causen un nivel especificado de perjuicios a una población determinada. La mayoría de las veces se refieren a la frecuencia de que se produzca un número dado de pérdidas.

Las curvas FN muestran la frecuencia acumulativa (F) con la que N o más miembros de la población se verán afectados. Los valores elevados de N que se pueden dar con una frecuencia elevada F son de gran interés ya que social y políticamente pueden ser inaceptables.

B.27.2 Utilización

Las curvas FN son una manera de representar los resultados de un análisis de riesgo. Muchos sucesos tienen una alta probabilidad de dar un resultado de consecuencias limitadas, y una baja probabilidad de dar un resultado de consecuencias elevadas. Las curvas FN proporcionan una representación del nivel de riesgo, mediante una línea que describe esta gama, mejor que un punto único que represente un par de probabilidad-consecuencia.

Las curvas FN se pueden utilizar para comparar riesgos, por ejemplo, para comparar riesgos previsibles contra criterios definidos como una curva FN, o para comparar riesgos previsibles con datos procedentes de incidentes históricos, o con criterios de decisión (también expresados como una curva F/N).

Las curvas FN se pueden aplicar a diseños de sistemas o de procesos, o para la gestión de sistemas existentes.

B.27.3 Elementos de entrada

Los elementos de entrada son:

- conjuntos de pares de probabilidad-consecuencia durante un periodo de tiempo dado;
- los datos de un análisis de riesgo cuantitativo que proporciona las probabilidades estimadas para números de pérdidas especificados;
- datos procedentes de registros históricos y de un análisis de riesgo cuantitativo.

B.27.4 Proceso

Los datos disponibles se representan sobre un gráfico donde el número de pérdidas (hasta un nivel de perjuicio especificado, es decir, fallecimiento) ocupen el eje de abscisas y la probabilidad de N o más pérdidas ocupen el eje de ordenadas. Debido al amplio intervalo de valores, normalmente ambos ejes son escalas logarítmicas.

Las curvas FN se pueden generar estadísticamente utilizando números "reales" procedentes de pérdidas anteriores o se pueden calcular a partir de estimaciones de modelos simulados. Los datos utilizados y las suposiciones tomadas pueden significar que estos dos tipos de curvas FN proporcionen informaciones diferentes y se deberían utilizar por separado y para fines diferentes. En general, las curvas FN teóricas son más útiles para diseños de sistemas, y las curvas FN estadísticas son más útiles para la gestión de un sistema particular existente.

Ambos enfoques de derivación pueden consumir mucho tiempo por lo que es normal utilizar una mezcla de ambos. Los datos empíricos darán lugar a puntos fijos de pérdidas conocidas de manera precisa que se han producido en accidentes/incidentes conocidos durante un periodo de tiempo especificado, y el análisis de riesgo cuantitativo proporciona otros puntos por extrapolación o interpolación.

La necesidad de considerar accidentes de baja frecuencia y de elevadas consecuencias puede requerir la consideración de largos periodos de tiempo para recopilar datos suficientes para un análisis correcto. Esto, a su vez, puede hacer que los datos disponibles sean sospechosos, si los sucesos iniciadores ocurren a lo largo del tiempo.

B.27.5 Resultados

Una línea que representa el riesgo a través de una gama de valores de las consecuencias, que se pueden comparar con los criterios que son apropiados para la población que se está estudiando y para el nivel de perjuicio especificado.

B.27.6 Fortalezas y limitaciones

Las curvas FN son un medio útil de presentar la información del riesgo, que pueden ser utilizadas por los gestores y los diseñadores del sistema para ayudar a tomar decisiones sobre el riesgo y los niveles de seguridad. Estas curvas son un medio útil de presentar la información de la frecuencia y de las consecuencias en un formato accesible.

Las curvas FN son apropiadas para comparar riesgos procedentes de situaciones similares cuando se dispone de datos suficientes. Estas curvas no se deberían utilizar para comparar riesgos de tipos diferentes con características que varíen en circunstancias en que también varíe la cantidad y la calidad de los datos.

Una limitación de las curvas FN es que no dicen nada acerca de la gama de efectos o de las consecuencias de incidentes que no sea el número de personas impactadas, y no hay manera de identificar las diferentes formas en las que el nivel de perjuicios puede haber ocurrido. Estas curvas delimitan un tipo de consecuencia particular, normalmente perjuicios a las personas. Las curvas FN no son un método de apreciación del riesgo, sino una forma de presentar los resultados de la apreciación del riesgo.

Estas curvas son un método bien establecido para presentar los resultados de la apreciación del riesgo, pero requieren que sean preparadas por analistas muy cualificados, y con frecuencia son difíciles de interpretar y de evaluar por personas que no sean especialistas.

B.28 Índices de riesgo

B.28.1 Presentación

Un índice de riesgo es una medida semicuantitativa del riesgo consistente en una estimación que se obtiene utilizando un procedimiento de puntuación mediante la aplicación de escalas ordinales. Los índices de riesgo se pueden utilizar para clasificar una serie de riesgos aplicando criterios similares de manera que se puedan comparar. Las puntuaciones se aplican a cada componente de riesgo, por ejemplo a las características contaminantes (fuentes de contaminación), a la gama de posibles vías de exposición y al impacto sobre los receptores.

Los índices de riesgo son esencialmente un procedimiento cualitativo para clasificar y comparar riesgos. Aunque se utilicen números, esto es simplemente para tener en cuenta su manipulación. En muchos casos, cuando el modelo o sistema fundamental no es bien conocido o no se puede representar, es mejor utilizar un procedimiento cualitativo más abierto.

B.28.2 Utilización

Los índices se pueden utilizar para clasificar riesgos diferentes asociados a una actividad cuando el sistema se entiende bien. Los índices de riesgo permiten la integración de una gama de factores que tienen un impacto sobre el nivel de riesgo en una única puntuación numérica del nivel de riesgo.

Los índices se utilizan para muchos tipos diferentes de riesgo, normalmente como un medio de definir el alcance de la clasificación del riesgo de acuerdo con el nivel de riesgo. Esto se puede utilizar para determinar los riesgos que necesitan una apreciación adicional en profundidad y posiblemente de tipo cuantitativa.

B.28.3 Elementos de entrada

Los elementos de entrada se obtienen del análisis del sistema, o de una descripción general del contexto. Esto requiere una buena comprensión de todas las fuentes de riesgo, de las vías posibles, y de lo que podría verse afectado. Para soportar el desarrollo de los índices de riesgo se pueden utilizar herramientas tales como el análisis de árbol de fallos, el análisis de árbol de sucesos y el análisis de toma de decisiones generales.

Dado que la elección de escalas ordinales es, hasta cierto punto, arbitraria, se necesitan datos suficientes para validar el índice.

B.28.4 Proceso

El primer paso consiste en comprender y describir el sistema. Una vez que el sistema esté definido, se desarrollan puntuaciones para cada componente de manera que éstas se puedan combinar para obtener un índice mixto. Por ejemplo, en un contexto ambiental, se deben puntuar los orígenes, el camino y el/los receptores, teniendo en cuenta que en algunos casos puede haber múltiples caminos y receptores para cada origen. Las puntuaciones individuales se combinan de acuerdo con un esquema que tenga en cuenta la realidad física del sistema. Es importante que las puntuaciones de cada parte del sistema (orígenes, caminos y receptores) sean coherentes internamente y mantengan las relaciones correctas. Las puntuaciones se pueden dar para componentes de riesgo (por ejemplo, probabilidad, exposición, consecuencia) o para factores que aumenten el riesgo.

Las puntuaciones se pueden sumar, restar, multiplicar y/o dividir de acuerdo con este modelo de alto nivel. Los efectos acumulativos se pueden tener en cuenta mediante la adición de puntuaciones (por ejemplo, sumando puntuaciones de caminos diferentes). No es estrictamente válido aplicar fórmulas matemáticas a escalas ordinales. Por ello, una vez que el sistema de clasificación se ha desarrollado, el modelo se debería validar aplicándolo a un sistema conocido. El desarrollo de un índice es un procedimiento iterativo y puede ser necesario probar varios sistemas diferentes para combinar las puntuaciones antes de que el analista se encuentre a gusto con la validación.

La incertidumbre se puede estudiar mediante un análisis de sensibilidad, y variando las puntuaciones hasta encontrar los parámetros que sean más sensibles.

B.28.5 Resultados

Los resultados consisten en una serie de números (índices mixtos) relacionados con un origen particular, que se puede comparar con los índices desarrollados para otros orígenes procedentes del mismo sistema, o que se pueden modelizar de la misma manera.

B.28.6 Fortalezas y limitaciones

Fortalezas:

- los índices pueden constituir una buena herramienta para la clasificación jerárquica de riesgos diferentes;
- los índices permiten que múltiples factores que afectan al nivel de riesgo sean incorporados en una única puntuación numérica para el nivel de riesgo.

Limitaciones:

- si el proceso (modelo) y su resultado no están bien validados, los resultados pueden carecer de sentido. El hecho de que la salida sea un valor numérico del riesgo, puede ser mal interpretado y mal utilizado, por ejemplo, en los posteriores análisis de costes/beneficios;
- en muchas situaciones en las que se utilizan los índices, no existe un modelo fundamental para definir si las escalas individuales de los factores de riesgo son lineales, logarítmicas o de algún otro tipo, ni tampoco un modelo que defina los factores que se deberían combinar. En estas situaciones, la clasificación es por consiguiente de poca confianza y en consecuencia es particularmente importante realizar una validación contra datos reales.

B.29 Matriz de consecuencia/probabilidad

B.29.1 Presentación

La matriz de consecuencia/probabilidad es un medio de combinar clasificaciones cualitativas o semicuantitativas de consecuencia y probabilidad para producir un nivel de riesgo o una clasificación del riesgo.

El formato de la matriz y las definiciones que se apliquen dependen del contexto en el que se utiliza, y es importante que se utilice un diseño apropiado a las circunstancias.

B.29.2 Utilización

La matriz de consecuencia/probabilidad se utiliza para jerarquizar riesgos, orígenes de riesgo y tratamientos del riesgo sobre la base del nivel de riesgo. Normalmente, se utiliza como una herramienta de filtrado cuando se han identificado muchos riesgos, por ejemplo, para definir cuáles son los riesgos que necesitan análisis adicionales o más detallados, cuales son los que se han de tratar primero, o cuales se han referenciar a un nivel de gestión más elevado. También se puede utilizar para seleccionar los riesgos que no es necesario considerar en ese momento. El tipo de matriz de riesgo también se utiliza con mucha frecuencia para determinar si un riesgo dado es ampliamente aceptable o no aceptable (véase el apartado 5.4), en función de la zona donde se localice sobre la matriz.

La matriz de consecuencia/probabilidad también se puede utilizar para ayudar a que toda la organización participe en la comprensión común de los niveles cualitativos de riesgos. La forma en que se establecen los niveles de riesgo y se asignan las reglas de decisión a quienes se deberían alinear con el deseo de riesgo de la organización.

Una forma de la matriz de consecuencia/probabilidad se utiliza en el análisis de criticidad del FMECA (análisis del modo de fallo, del efecto y de la criticidad) o para ajustar las prioridades después del HAZOP (estudios de peligros y de operatividad). También se puede utilizar en aquellas situaciones en que los datos sean insuficientes para un análisis detallado o la situación no garantice el tiempo y el esfuerzo para un análisis más cuantitativo.

B.29.3 Elementos de entrada

Los elementos de entrada al proceso son escalas personalizadas de la consecuencia y de la probabilidad, y una matriz que combina las dos.

La escala (o escalas) de consecuencia debería cubrir la gama de diferentes tipos de consecuencia a considerar (por ejemplo, pérdidas financieras, parámetros de seguridad; parámetros ambientales o de otros tipos, dependiendo del contexto) y se debería extender desde la consecuencia máxima verosímil hasta la consecuencia más baja de interés. Un ejemplo parcial se muestra en la figura B.13.

La escala puede tener cualquier número de puntos. Las escalas más comunes son las de 3, 4 o 5 puntos.

La escala de probabilidad también puede tener cualquier número de puntos. Las definiciones de la probabilidad se deben seleccionar de manera que sean lo menos ambiguas posible. Si se utilizan guías numéricas para definir probabilidades diferentes, se deben indicar las unidades. La escala de probabilidad debe estar adaptada a la gama aplicable al estudio que se tiene entre manos, recordando que la probabilidad más baja debe ser aceptable para la consecuencia más alta definida, en caso contrario todas las actividades con la consecuencia más alta se definen como intolerables. Un ejemplo parcial se muestra en la figura B.14.

La matriz se dibuja con la consecuencia representada sobre un eje de coordenadas y la probabilidad sobre el otro eje. La figura B.15 muestra parte de una matriz de ejemplo con escalas de consecuencia de 6 puntos y con escala de probabilidad de 5 puntos.

Los niveles de riesgo asignados a las celdas dependerán de las definiciones de las escalas de probabilidad/consecuencia. La matriz se puede establecer de manera que realce el peso de las consecuencias (como se muestra) o el de la probabilidad, o puede ser simétrica dependiendo de la aplicación. Los niveles de riesgo pueden estar enlazados a reglas de toma de decisiones, tales como el nivel de atención de la gestión o de la escala de tiempo para la que se necesita la respuesta.

Rating	Financial impact AU\$ EBITDA	Investment Return AU\$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	\$100m+ loss or gain	\$300 + loss or gain	<ul style="list-style-type: none"> Multiple fatalities, or Significant irreversible effects to 10's of people 	<ul style="list-style-type: none"> Irreversible long term environmental harm. Community outrage- potential large-scale class action. 	<ul style="list-style-type: none"> International press reporting over several days. Total loss of shareholder support who act to dis-invest. CEO departs and board is restructured. 	<ul style="list-style-type: none"> Major litigation or prosecution with damages of \$50m+ plus significant costs. Custodial sentence for company Executive. Prolonged closure of operations by authorities.
5	\$10m - \$99m loss or gain	\$30m - \$299m loss or gain	<ul style="list-style-type: none"> Single fatality and/or Severe irreversible disability to one or more persons 	<ul style="list-style-type: none"> Prolonged environmental impact. High-profile community concerns raised - requiring significant remediation measures. 	<ul style="list-style-type: none"> National press reporting over several days. Sustained impact on the reputation of shareholders. Loss of shareholder support for growth. Pressure on management. 	<ul style="list-style-type: none"> Major litigation costing \$10m+ Investigation by regulatory body resulting in long interruption to operations.
4	\$1m - \$9m loss or gain	\$3m - \$29m loss or gain	<ul style="list-style-type: none"> Extensive injuries or irreversible damage to property 	<ul style="list-style-type: none"> Major spill or 		
3	\$100k - \$900k loss or gain					
2	\$10k - 100k loss or gain					
1	\$1k - 10k loss or gain					

Figura B.13 – Ejemplo parcial de una tabla de criterios de consecuencia

Rating	Criteria
Likely	<ul style="list-style-type: none"> - balance of probability will occur, or - could occur within "weeks to months"
Possible	<ul style="list-style-type: none"> - may occur shortly but a distinct possibility - could occur within "months"
Unlikely	<ul style="list-style-type: none"> - may occur but not for a foreseeable period - could occur in "years"
Rare	<ul style="list-style-type: none"> - occurrence requires exceptional circumstances - exceptional - only occurs once in a long time
Remote	<ul style="list-style-type: none"> - theoretical possibility - frequency of occurrence is very low

Figura B.14 – Ejemplo parcial de una matriz de clasificación jerárquica del riesgo

Clasificación de la probabilidad	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		Clasificación de la consecuencia					

Figura B.15 – Ejemplo parcial de una matriz de criterios de probabilidad

Las escalas de clasificación y la matriz se pueden establecer con escalas cuantitativas. Por ejemplo, en un contexto de fiabilidad, la escala de probabilidad podría representar los regímenes de fallos indicativos y la escala de consecuencia los costes del fallo en dólares.

Para la utilización de las herramientas se necesitan personas (preferiblemente un grupo) que tengan los conocimientos técnicos correspondientes, y que dispongan de datos para poder enjuiciar la consecuencia y la probabilidad.

B.29.4 Proceso

Para clasificar jerárquicamente los riesgos, el usuario en primer lugar localiza el descriptor de la consecuencia que mejor se adapta a la situación, y después define la probabilidad con la que ocurrirán estas consecuencias. A continuación, de la matriz deduce el nivel de riesgo.

Muchos sucesos de riesgo pueden tener una gama de consecuencias con diferentes probabilidades asociadas. Usualmente, los problemas menores son más comunes que las catástrofes. Por ello, existe una elección sobre si jerarquizar las consecuencias más comunes, o las más serias, o alguna otra combinación. En muchos casos, es adecuado enfocar las consecuencias verosímiles más serias ya que estas plantean las mayores amenazas y con frecuencia son las de mayor importancia. En algunos casos, puede ser apropiado jerarquizar como riesgos independientes los problemas comunes y las catástrofes improbables. Es importante que se utilice la probabilidad aplicable a la consecuencia seleccionada y no la probabilidad del suceso como un todo.

El nivel de riesgo definido por la matriz puede estar asociado a una regla de toma de decisiones, tal como la de tratar o no tratar el riesgo.

B.29.5 Resultados

Los resultados son una clasificación de cada riesgo o una lista jerarquizada de riesgos con niveles de importancia definidos.

B.29.6 Fortalezas y limitaciones

Fortalezas:

- es relativamente fácil de utilizar;
- proporciona una clasificación jerarquizada rápida de los riesgos con diferentes niveles de importancia.

Limitaciones:

- la matriz se debería diseñar de manera que sea apropiada a las circunstancias, por lo que en una organización puede ser difícil disponer de un sistema común que se aplique a una gama de circunstancias importantes;
- es difícil definir escalas que no sean ambiguas;
- su utilización es muy subjetiva, y por tanto pueden existir variaciones significativas entre los clasificadores;
- los riesgos no se pueden sumar (es decir, no se puede definir que un número particular de riesgos bajos o que un riesgo bajo identificado un número particular de veces sea equivalente a un riesgo de tipo medio);
- es difícil combinar o comparar el nivel de riesgo para categorías diferentes de consecuencias.

Los resultados dependerán del nivel de detalle del análisis, es decir, del análisis más detallado, del mayor número de escenarios, cada uno con la más baja probabilidad. Esto subestimaré el nivel de riesgo real. La forma de agrupar juntos los escenarios para la descripción del riesgo debería ser consistente y estar definida al comienzo del estudio.

B.30 Análisis de costes/beneficios (CBA)

B.30.1 Resumen

El análisis de costes/beneficios se puede utilizar para la evaluación del riesgo cuando los costes previstos totales se compensan con los beneficios totales previstos, a fin de elegir la mejor opción o la más ventajosa. Este análisis constituye una parte implícita de muchos sistemas de evaluación del riesgo. Puede ser cualitativo o cuantitativo, o implicar una combinación de elementos cuantitativos y cualitativos. El CBA cuantitativo añade el valor monetario de todos los costes y todos los beneficios para todas las partes interesadas que están incluidas en el campo de aplicación, y se ajusta para periodos de tiempo diferentes en los que los costes y beneficios se acumulan. El valor actual neto (NPV) que se obtiene, pasa a ser una entrada para la toma de decisiones sobre el riesgo. Un NPV positivo asociado con una acción, normalmente significaría que la acción debería realizarse. No obstante, para algunos riesgos negativos, en particular aquellos que implican riesgos para la vida de las personas o daños para el entorno ambiental, se puede aplicar el principio ALARP ("tan bajo como razonablemente sea posible"). Esto divide los riesgos en tres regiones: un nivel por encima del cual los riesgos negativos son intolerables y no se deberían aceptar excepto en circunstancias extraordinarias; un nivel por debajo del cual los riesgos son insignificantes y únicamente necesitan seguirse para asegurar que continúan siendo bajos; y una banda central donde se procura que los riesgos sean tan bajos como razonablemente sea posible (ALARP). Hacia el extremo de riesgo más bajo de esta región, se puede aplicar un estricto análisis de costes/beneficios, pero en la zona donde los riesgos están próximos a ser considerados como intolerables, la expectativa del principio ALARP es que el tratamiento se realizará salvo que los costes del tratamiento sean enormemente desproporcionados con respecto a los beneficios que obtienen.

B.30.2 Utilización

El análisis de costes/beneficios se puede utilizar para decidir entre opciones que implican riesgo.

Por ejemplo:

- como entrada en una decisión acerca de si un riesgo se debería tratar;
- para diferenciar entre, y decidir, la mejor manera de tratar el riesgo;
- decidir entre diferentes formas de acción.

B.30.3 Elementos de entrada

Los elementos de entrada incluyen la información sobre costes y beneficios para las principales partes interesadas y sobre las incertidumbres en estos costes y beneficios. Se deberían tener en consideración los costes y beneficios tangibles e intangibles. Los costes incluyen los recursos consumidos y las consecuencias negativas; los beneficios incluyen las consecuencias positivas, las consecuencias negativas que se han evitado y los recursos ahorrados.

B.30.4 Proceso

Se identifican las partes interesadas que pueden experimentar costes o recibir beneficios. En un análisis de costes/beneficios completo se incluyen todas las partes interesadas.

Se identifican los beneficios y costes directos e indirectos de todas las partes interesadas de las opciones que se están considerando. Los beneficios directos son aquellos que salen directamente de la acción tomada, mientras que los beneficios indirectos o subsidiarios son aquellos que son fortuitos pero que aún pueden contribuir significativamente a la decisión. Como ejemplos de beneficios indirectos se consideran la mejora de reputación, la satisfacción del personal de dirección y la "tranquilidad de ánimo". (Con frecuencia, estos se ponderan intensamente en la toma de decisiones).

Los costes directos son aquellos que están asociados directamente con la acción. Los costes indirectos son los costes adicionales, los subsidiarios y los inmovilizados, tales como la pérdida de utilidad, la confusión en el tiempo de gestión o la derivación de capital fuera de potenciales inversiones. Cuando se aplica un análisis de costes/beneficios a una decisión sobre si se debe tratar un riesgo, se deberían incluir los costes y los beneficios asociados al tratamiento del riesgo y con la aceptación del riesgo.

En el análisis de costes/beneficios cuantitativo, cuando se han identificado todos los costes y beneficios tangibles e intangibles se asigna un valor monetario a todos los costes y beneficios (incluidos los intangibles). Para hacer esto existe un número de maneras normalizadas, incluyendo el enfoque de "buena disposición para pagar" y utilizando maneras sustitutas. Si, como ocurre con frecuencia, los costes se estiman sobre un periodo de tiempo corto (por ejemplo, un año) y los beneficios corresponden a un periodo de tiempo grande a partir de entonces, normalmente es necesario descontar los beneficios para traerlos al "valor de hoy" de manera que se pueda obtener una comparación válida. Todos los costes y beneficios se expresan como valores actuales. Los valores actuales de todos los costes y de todos los beneficios para todas las partes interesadas se pueden combinar para obtener un valor actual neto (NPV). Un NPV positivo implica que la acción es beneficiosa. También se utiliza la relación beneficios-costes; véase el apartado B.30.5.

Si existe incertidumbre sobre el nivel de los costes o de los beneficios, uno o ambos términos se pueden ponderar de acuerdo con sus probabilidades.

En el análisis de costes/beneficios cualitativo no se intenta encontrar un valor monetario para los costes y beneficios intangibles y, en vez de proporcionar un número único que resuma los costes y beneficios, las relaciones y las concesiones mutuas entre costes y beneficios se consideran cualitativamente.

Una técnica relacionada es un análisis de costes-eficacia. En este análisis se asume que se desea un determinado beneficio o resultado, y que existen varios caminos alternativos para conseguirlo. El análisis estudia únicamente los costes y cuál es el camino más económico para conseguir el beneficio.

B.30.5 Resultados

El resultado de un análisis de costes/beneficios consiste en la información sobre costes y beneficios, relativa a diferentes opciones o acciones. Esto se puede expresar cuantitativamente como un valor actual neto (NPV), un porcentaje de retorno interno (IRR) o como la relación entre el valor actual de los beneficios y el valor actual de los costes. Los resultados expresados en forma cualitativa, por lo general, consisten en una tabla que compara los costes y los beneficios de diferentes tipos de costes y beneficios, prestando atención a las concesiones mutuas.

B.30.6 Fortalezas y limitaciones

Las fortalezas del análisis de costes/beneficios:

- permite la comparación entre costes y beneficios utilizando una métrica única (numeraria);
- proporciona transparencia para la toma de decisiones;
- requiere la recopilación de información detallada sobre todos los posibles aspectos de la decisión. Esto puede ser útil como revelador de ignorancia así como de comunicación de conocimientos.

Limitaciones

- un CBA cuantitativo puede producir números dramáticamente diferentes, dependiendo de los métodos utilizados para asignar valores económicos a beneficios no económicos;
- en algunas aplicaciones es difícil definir una tasa de descuento válida para costes y beneficios futuros;
- los beneficios que se acumulan para una población grande son difíciles de estimar, en particular aquellos que están relacionados con bienes públicos que no se cambian en los mercados;
- la práctica del descuento significa que los beneficios que se obtengan en un futuro a largo plazo tienen una influencia insignificante sobre las decisiones tomadas, dependiendo de la tasa de descuento elegida. El método comienza a ser inadecuado para la consideración de riesgos que afecten a generaciones futuras, salvo que se fijen regímenes de discontinuidad muy baja o cero.

B.31 Análisis de decisión multi-criterios (MCDA)

B.31.1 Presentación

El objetivo de este análisis es utilizar una gama de criterios para apreciar de forma objetiva y transparente el mérito de un conjunto de opciones. En general, la meta global es generar un orden de preferencia entre opciones disponibles. Este análisis implica el desarrollo de una matriz de opciones y de criterios que se jerarquizan y suman para proporcionar una puntuación global de cada opción.

B.31.2 Utilización

El MCDA se puede utilizar para:

- comparar múltiples opciones como un primer paso de análisis para determinar opciones preferentes y potenciales y opciones inapropiadas;
- comparar opciones cuando existen múltiples criterios, que algunas veces son contradictorios;
- alcanzar un consenso sobre una decisión cuando diferentes partes interesadas tienen objetivos o valores contradictorios.

B.31.3 Elementos de entrada

Un conjunto de opciones para análisis. Los criterios, basados en objetivos, que se pueden utilizar por igual sobre todas las opciones para establecer las diferencias entre ellas.

B.31.4 Proceso

Por lo general, un grupo de partes interesadas bien informadas que realizan el proceso siguiente:

- a) definen el o los objetivos;
- b) determinan los atributos (criterios o medidas de comportamiento) que se relacionan con cada objetivo;
- c) estructuran los atributos de manera jerárquica;
- d) desarrollan opciones que se evalúan contra los criterios fijados;
- e) determinan la importancia de los criterios y le asignan las categorías correspondientes;
- f) evalúan las alternativas con respecto a los criterios. Esto se puede representar como una matriz de puntuaciones;
- g) combinan las múltiples puntuaciones de un solo atributo en una puntuación única de múltiples atributos;
- h) evalúan los resultados.

Existen diferentes métodos mediante los cuales se puede obtener la ponderación de cada criterio, y diferentes formas de sumar los criterios de puntuación de cada opción en una puntuación única de múltiples atributos. Por ejemplo, las puntuaciones se pueden sumar como una suma ponderada o un producto ponderado o utilizando un proceso jerárquico analítico, una técnica de consecución de las ponderaciones y puntuaciones basadas en comparaciones por parejas. En todos estos métodos se asume que la preferencia por cualquier criterio no depende de los valores de los otros criterios. Cuando esta presunción no es válida, se utilizan modelos diferentes.

Dado que las puntuaciones son subjetivas, el análisis de sensibilidad es útil para examinar el alcance con que las ponderaciones y las puntuaciones influyen en las preferencias generales entre opciones.

B.31.5 Resultados

La presentación del orden jerárquico de las opciones va desde la más a la menos preferida. Si el proceso genera una matriz donde los ejes de la matriz son los criterios ponderados y los criterios de puntuación para cada opción, entonces también se pueden eliminar las opciones que fallen criterios altamente ponderados.

B.31.6 Fortalezas y limitaciones

Fortalezas:

- proporciona una estructura simple para una toma de decisiones eficaz y la presentación de presunciones y de conclusiones;
- puede hacer más manejables problemas de decisión complejos que no son tratables mediante el análisis de costes/beneficios;
- puede ayudar a considerar racionalmente los problemas donde es necesario realizar concesiones mutuas;
- puede ayudar a conseguir el acuerdo entre partes interesadas que tienen objetivos diferentes y por tanto también criterios diferentes.

Limitaciones:

- puede ser afectado por derivaciones y una mala selección de los criterios de decisión;
- la mayoría de los problemas del MCDA no tienen una solución concluyente o única;
- los algoritmos de agregación que calculan los criterios de las ponderaciones a partir de las preferencias establecidas o las opiniones que difieran totalmente, pueden oscurecer la base verdadera de la decisión.

BIBLIOGRAFÍA

- IEC 61511, *Functional safety. Safety instrumented systems for the process industry sector.*
- IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems.*
- IEC 61882, *Hazard and operability studies (HAZOP studies). Application guide.*
- ISO 22000, *Food safety management systems. Requirements for any organization in the food chain.*
- ISO/IEC Guide 51, *Safety aspects. Guidelines for their inclusion in standards.*
- IEC 60300-3-11, *Dependability management. Part 3-11: Application guide. Reliability centred maintenance.*
- IEC 61649, *Weibull analysis.*
- IEC 61078, *Analysis techniques for dependability. Reliability block diagram and boolean methods.*
- IEC 61165, *Application of Markov techniques.*
- ISO/IEC 15909 (all parts), *Software and systems engineering. High-level Petri nets.*
- IEC 62551, *Analysis techniques for dependability. Petri net techniques²⁾*
- IEC 61882, *Hazard and operability studies (HAZOP studies). Application guide.*

2) Pendiente de publicación.

ANEXO ZA (Normativo)**OTRAS NORMAS INTERNACIONALES CITADAS EN ESTA NORMA
CON LAS REFERENCIAS DE LAS NORMAS EUROPEAS CORRESPONDIENTES**

Esta norma europea incorpora disposiciones de otras normas por su referencia, con o sin fecha. Estas referencias normativas se citan en los lugares apropiados del texto de la norma y se relacionan a continuación. Las revisiones o modificaciones posteriores de cualquiera de las normas citadas con fecha, sólo se aplican a esta norma europea cuando se incorporan mediante revisión o modificación. Para las referencias sin fecha se aplica la última edición de esa norma (incluyendo sus modificaciones).

NOTA Cuando una norma internacional haya sido modificada por modificaciones comunes CENELEC, indicado por (mod), se aplica la EN/HD correspondiente.

Norma Internacional	Fecha	Título	EN/HD	Fecha
Guía ISO/IEC 73	—	<i>Gestión del riesgo. Vocabulario. Directrices para la utilización en las normas.</i>	—	—
ISO 31000	—	<i>Gestión del riesgo. Principios y directrices.</i>	—	—

AENOR Asociación Española de
Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032