658.155
I26g
5.1

UNIVERSIDAD MILITAR
NUEVA GRANADA
BIBLIOTECA

NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010

BIBLIOTECA GENERAL
658.155 I26g
45299

2013-04-17

GESTIÓN DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL RIESGO

icontec internacional

E: RISK MANAGEMENT. RISK ASSESSMENT TECHNIQUES

CORRESPONDENCIA:	esta norma es una adopción idéntica (IDT) por traducción de la norma IEC/ISO 31010:2009.
DESCRIPTORES:	gestión; riesgo; incertidumbre; valoración - riesgo.

I.C.S.: 03.100.01

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

Prohibida su reproducción

Editada 2013-04-24

UNIVERSIDAD MILITAR
NUEVA GRANADA
BIBLIOTECA

#97230 Temis OP 610 · 1321300 · Adm. de la seguridad · 14/oct/2015

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La NTC-IEC/ISO 31010 fue ratificada por el Consejo Directivo de 2013-04-17.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 32 Gestión del Riesgo.

ACUEDUCTO DE BOGOTA
AON COLOMBIA S.A. - CORREDORES DE SEGUROS
ASEGURADORA SOLIDARIA DE COLOMBIA
ASEGURADORES TECNICOS LTDA.
ASOCIACION COLOMBIANA DE AUDITORES -ASCOLDA-
BANCO AGRARIO
BANCO DE LA REPUBLICA
CENTRO POLICLINICO DEL OLAYA C.P.O. S.A.
CLUB EL NOGAL
CONCONCRETO S.A.
CONSULTOR INDEPENDIENTE - CARLOS JULIO DÍAZ
CONSULTORES DU & G
CREDIBANCO VISA
DRMS
DU & CO
ECOPETROL S.A.
EMPRESA DE TELEFONOS DE BOGOTA
EMPRESAS PÚBLICAS DE MEDELLIN
EPM
ERNST & YOUNG
GIT LTDA.
GRUPO NACIONAL DE CHOCOLATES
GRUPO SCARE
I TEAM LTDA.
INTEK S.A
OVERSIGHT SAC
POSITIVA COMPAÑÍA DE SEGUROS
PRINTER COLOMBIANA
RELIABILITY MAINTENANCE SERVICES S.A.
RESPONSABILIDAD INTEGRAL
REVAK S.A.
RMS
SALUD TOTAL E.P.S.
TEAM FOODS COLOMBIA
TECNICONTROL
THOMAS MTI
TRL LTDA.

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

ACUEDUCTO METROPOLITANO DE BUCARAMANGA S.A. E.S.P.
AGUAS DE BUGA S.A. E.S.P.
ALFACER DEL CARIBE S.A.

CONTENIDO

Página

INTRODUCCIÓN 1

1. ALCANCE 2

2. REFERENCIAS NORMATIVAS 2

3. TÉRMINOS Y DEFINICIONES 3

4. CONCEPTOS SOBRE LA VALORACIÓN DE RIESGOS 3

4.1 PROPÓSITO Y BENEFICIOS 3

4.2 VALORACIÓN DEL RIESGO Y MARCO DE REFERENCIA PARA LA GESTIÓN DE RIESGOS 3

4.3 VALORACIÓN DEL RIESGO Y EL PROCESO DE GESTIÓN DE RIESGOS 4

5. PROCESO DE VALORACIÓN DEL RIESGO 8

5.1 INFORMACIÓN GENERAL 8

5.2 IDENTIFICACIÓN DEL RIESGO 9

5.3 ANÁLISIS DEL RIESGO 9

5.4 EVALUACIÓN DEL RIESGO 13

5.5 DOCUMENTACIÓN 14

5.6 MONITOREO Y REVISIÓN DE LA VALORACIÓN DEL RIESGO 15

5.7 APLICACIÓN DE LA VALORACIÓN DEL RIESGO DURANTE LAS FASES DEL CICLO DE DURACIÓN 15

6. SELECCIÓN DE LAS TÉCNICAS DE VALORACIÓN DEL RIESGO 16

Página

6.1 GENERALIDADES 16

6.2 SELECCIÓN DE LAS TÉCNICAS 26

6.3 DISPONIBILIDAD DE RECURSOS 17

6.4 LA NATURALEZA Y EL GRADO DE LA INCERTIDUMBRE 17

6.5 COMPLEJIDAD 18

6.6 APLICACIÓN DE LA VALORACIÓN DEL RIESGO DURANTE LAS FASES DEL CICLO DE DURACIÓN 18

6.7 TIPOS DE TÉCNICAS PARA LA VALORACIÓN DEL RIESGO 19

BIBLIOGRAFÍA 103

DOCUMENTO DE REFERENCIA 104

ANEXOS

ANEXO A (Informativo)
COMPARACIÓN DE LAS TÉCNICAS PARA LA VALORACIÓN DEL RIESGO 20

ANEXO B (Informativo)
TÉCNICAS PARA LA VALORACIÓN DEL RIESGO 26

Figura 1. Contribución de la valoración del riesgo al proceso de gestión de riesgos 8

GESTIÓN DE RIESGOS.
TÉCNICAS DE VALORACIÓN DEL RIESGO

INTRODUCCIÓN

Las organizaciones de todos los tipos y tamaños enfrentan un rango de riesgos que pueden afectar el logro de sus objetivos.

Estos objetivos se pueden relacionar con un rango de actividades de la organización, desde iniciativas estratégicas para sus operaciones, procesos y proyectos y verse reflejados en términos de resultados sociales, ambientales, tecnológicos, de inocuidad y seguridad, medidas comerciales, financieras y económicas, así como también impactos sociales, culturales, políticos y en la reputación.

Todas las actividades de una organización involucran riesgos que se deberían gestionar. El proceso de gestión de riesgos ayuda a tomar las decisiones teniendo en cuenta la incertidumbre y la posibilidad de eventos o circunstancias futuras (voluntarias o involuntarias) y sus efectos en los objetivos pactados.

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

- comunicación y consulta a través de todo este proceso;
- establecer el contexto para identificar, analizar, evaluar y tratar el riesgo asociado con cualquier actividad, proceso, función o producto;
- monitoreo y revisión de riesgos;
- reporte registro adecuado de los resultados.

La valoración del riesgo es aquella parte de la gestión de riesgos que suministra un proceso estructurado que identifica cómo pueden verse afectados los objetivos, y analiza el riesgo en términos de las consecuencias y sus probabilidades antes de decidir si se requiere tratamiento posterior.

La valoración del riesgo intenta responder las siguientes preguntas fundamentales:

- ¿qué puede suceder y por qué (mediante la identificación del riesgo)?
- ¿cuáles son las consecuencias?

- ¿cuál es la probabilidad de su ocurrencia en el futuro?

- ¿existen factores que mitigan las consecuencias del riesgo o que reduce la probabilidad del riesgo?

¿Es el nivel de riesgos tolerable o aceptable? y ¿requiere que éste de tratamiento posterior? esta norma pretende reflejar las buenas prácticas actuales en la selección y utilización de las técnicas de valoración del riesgo y no hace referencia conceptos nuevos o evolutivos que no han alcanzado un nivel satisfactorio de consenso profesional.

Esta norma a tiene una naturaleza general de tal modo que puede brindar directrices para muchas industrias y tipos de sistemas. Pueden existir más normas específicas dentro de estas industrias que establecen metodologías de preferencia y niveles de valoración para aplicaciones particulares. Si estas normas están en armonía con esta norma, las normas específicas generalmente serán suficientes.

1. ALCANCE

Esta norma es una norma de soporte para NTC-ISO 31000 y suministra directrices sobre la selección y la aplicación de técnicas sistemáticas para la valoración del riesgo.

La valoración del riesgo que se lleva a cabo de acuerdo con esta norma contribuye a otras actividades de la gestión de riesgos.

Se introduce la aplicación de un rango de técnicas con referencias específicas a otras normas cuando el concepto y la aplicación de las técnicas se describen en mayor detalle.

Esta norma no está destinada para un uso en certificación, reglamentos ni contratos.

Esta norma no suministra criterios específicos para identificar la necesidad de un análisis de riesgos ni especifica el tipo de métodos de análisis de riesgos que se requieren para una aplicación particular.

Esta norma no menciona todas las técnicas y la omisión de una técnica en esta norma no significa que ésta no sea válida. El hecho de que un método sea aplicable a una circunstancia particular no implica que el método se deba aplicar necesariamente.

NOTA Esta norma no trata específicamente de la seguridad. Es una norma genérica para la gestión de riesgos y cualquier referencia a la seguridad tiene una naturaleza puramente informativa. Las directrices sobre la introducción de los aspectos de seguridad en las normas IEC se especifican en la guía ISO/IEC 51.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos de referencia son indispensables para la aplicación de esta norma. Para referencias con fecha, únicamente se aplica la edición citada. Para referencias sin fecha, se aplica la edición más reciente del documento citado (incluyendo todas las enmiendas).

GTC 137, Gestión del riesgo. Vocabulario. ISO/IEC Guide 73.

NTC-ISO 31000, Gestión del Riesgo. Principios y directrices. ISO 31000.

3. TÉRMINOS Y DEFINICIONES

Para el propósito de este documento, se aplican los términos y las definiciones de la GTC 137.

4. CONCEPTOS SOBRE LA VALORACIÓN DE RIESGOS

4.1 PROPÓSITO Y BENEFICIOS

El propósito de la valoración del riesgo es suministrar información y análisis con base en evidencias para tomar decisiones informadas sobre la manera de tratar los riesgos particulares y de seleccionar entre diversas opciones.

Algunos de los beneficios principales de llevar a cabo la valoración del riesgo incluyen:

- entender el riesgo y su impacto potencial en los objetivos;
- brindar información para aquellos que toman las decisiones;
- contribuir a la comprensión de los riesgos con el fin de facilitar la selección de las opciones de tratamiento;
- identificar a los contribuyentes importantes en los riesgos y las conexiones débiles en los sistemas y las organizaciones;
- comparación de los riesgos en sistemas, tecnologías o enfoques alternativos;
- comunicar riesgos e incertidumbres;
- ayudar a establecer las prioridades;
- contribuir a la prevención de incidentes con base en la investigación posterior a ellos;
- seleccionar diferentes formas de tratamiento del riesgo;
- cumplir con los requisitos reglamentarios;
- brindar información que ayudará a evaluar si el riesgo se debería aceptar cuando se compara con criterios predefinidos;
- evaluar los riesgos para la disposición al final de la vida útil.

4.2 VALORACIÓN DEL RIESGO Y MARCO DE REFERENCIA PARA LA GESTIÓN DE RIESGOS

Esta norma asume que la valoración del riesgo se realiza dentro del marco de referencia y el proceso de gestión de riesgos que se describen en NTC-ISO 31000.

Un marco para la gestión de riesgos brinda las políticas, los procedimientos y las disposiciones organizacionales que incluirán la gestión de riesgos en toda la organización y en todos los niveles.

Como parte de este marco, la organización debería tener una política o estrategia para decidir cuándo y cómo se deberían evaluar los riesgos.

UNIVERSIDAD MILITAR
NUEVA GRANADA
BIBLIOTECA

En particular, aquellos que realizan las evaluaciones de riesgos deberían tener claridad sobre:

- el contexto y los objetivos de la organización,
- la extensión y el tipo de riesgos que son tolerables y la manera en que se van a tratar los riesgos no aceptables,
- la forma en que se integra la valoración del riesgo en los procesos de la organización,
- los métodos y las técnicas que se van a utilizar para la valoración del riesgo y su contribución al proceso de gestión de riesgos,
- rendición de cuentas, responsabilidad y autoridad para la realización de la valoración del riesgo,
- los recursos disponibles para llevar a cabo la valoración del riesgo,
- la manera en que se va a reportar y a revisar la valoración del riesgo.

4.3 VALORACIÓN DEL RIESGO Y EL PROCESO DE GESTIÓN DE RIESGOS

4.3.1 Generalidades

La valoración del riesgo incluye los aspectos clave del proceso de gestión de riesgos que se definen en la norma NTC-ISO 31000 y contiene los siguientes elementos:

- comunicación y consulta,
- establecimiento del contexto;
- valoración del riesgo (que incluyen identificación del riesgo, análisis del riesgo y evaluación del riesgo);
- tratamiento del riesgo;
- monitoreo y revisión.

La valoración del riesgo no es una actividad independiente y se debería integrar por completo en otros componentes del proceso de gestión de riesgos.

4.3.2 Comunicación y consulta

El éxito de la valoración del riesgo depende de la comunicación y la consulta eficaces con las partes involucradas.

Hacer partícipes a las partes involucradas en el proceso de gestión de riesgos facilitará:

- el desarrollo de un plan de comunicación,
- la definición correcta del contexto,
- garantizar que se entienden y toman en consideración los intereses de las partes involucradas,

- la unión de diversas áreas de experticia para identificar y analizar el riesgo,
- garantizar que se consideran adecuadamente los diversos puntos de vista en la evaluación de los riesgos,
- garantizar que los riesgos se identifican correctamente,
- asegurar la aprobación y el soporte para el plan de tratamiento.

Las partes involucradas deberían contribuir para establecer la interfaz del proceso de valoración del riesgo con otras disciplinas de la gestión, incluyendo la gestión del cambio, la gestión de proyectos y programas y la gestión financiera.

4.3.3 Establecimiento del contexto

En el establecimiento del contexto se definen los parámetros básicos para la gestión del riesgo y se establecen el alcance y los criterios para el resto del proceso. Para establecer el contexto se toman en consideración los parámetros internos y externos pertinentes para la organización como un todo, así como los antecedentes de los riesgos particulares que se están evaluando.

Cuando se establece el contexto, se determinan y pactan los objetivos de la valoración del riesgo, los criterios de riesgo y el programa de valoración del riesgo.

Para la valoración del riesgo específico, al establecer el contexto se debería incluir la definición del contexto interno, externo y de gestión de riesgos, así como la clasificación de los criterios del riesgo:

a) Establecer el contexto externo implica la familiarización con el entorno en el cual operan la organización y el sistema incluyendo:
   - factores del entorno cultural, político, legal, reglamentario, financiero, económico y competitivo, bien sea internacional, nacional, regional o local;
   - tendencias y motivadores clave que tienen impacto en los objetivos de la organización; y
   - percepciones y valores de las partes involucradas externas.

b) Establecer el contexto interno implica entender:
   - las capacidades de la organización en términos de recursos y conocimiento,
   - los flujos de información y los procesos de toma de decisiones,
   - las partes involucradas internas,
   - los objetivos y las estrategias implementadas para lograrlos,
   - 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 de dirección, las funciones y las responsabilidades).

c) Establecer el contexto del proceso de gestión de riesgos incluye:

- definir la rendición de cuentas y las responsabilidades,
- definir la extensión de las actividades de gestión de riesgos que se van a llevar a cabo, incluyendo las exclusiones e inclusiones específicas,
- definir la extensión del proyecto, el proceso, la función o la actividad en términos de tiempo y localización,
- definir las relaciones entre un proyecto o actividad particular y otros proyectos o actividades de la organización,
- definir las metodologías para la valoración del riesgo,
- definir los criterios del riesgo,
- definir la manera en que se evalúa el desempeño de la gestión de riesgos,
- identificar y especificar las decisiones y las acciones que se deben emprender, e
- identificar los estudios que son necesarios para la elaboración del alcance y el marco de referencia, y la extensión, los objetivos y los recursos necesarios para tales estudios.

d) Definir los criterios del riesgo involucra tomar decisiones sobre:

- la naturaleza y los tipos de consecuencias que se van a incluir y cómo se van a medir,
- la manera en que se van a expresar las probabilidades,
- la manera en que se determinará el nivel de un riesgo,
- los criterios frente a los cuales se decidirá cuándo un riesgo necesita tratamiento,
- los criterios para decidir cuándo un riesgo es aceptable y/o tolerable,
- si se van a tomar en consideración las combinaciones de riesgos y cómo se van a considerar.

Los criterios se pueden basar en fuentes tales como:

- objetivos del proceso pactados,
- los criterios identificados en las especificaciones,
- las fuentes de datos generales,
- los criterios industriales aceptados generalmente, por ejemplo los niveles de integridad de la seguridad,

- la apetencia de la organización con respecto al riesgo,
- los requisitos legales y otros para equipos o aplicaciones específicos.

4.3.4 Valoración del riesgo

La valoración del riesgo es el proceso general de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Los riesgos se pueden evaluar en el ámbito de la organización, de un departamento, para proyectos o actividades individuales o para riesgos específicos. En diferentes contextos, diversas herramientas y técnicas pueden ser adecuadas.

La valoración del riesgo proporciona un entendimiento de los riesgos, sus causas, consecuencias y probabilidades. Esto suministra elementos de entrada para las decisiones sobre:

- si se debería o no emprender una actividad;
- cómo maximizar las oportunidades;
- si es necesario tratar los riesgos;
- la selección entre opciones con riesgos diferentes;
- la prioridad de las opciones para el tratamiento del riesgo;
- la selección más adecuada de las estrategias para el tratamiento del riesgo que ocasionarán riesgos adversos en un grado tolerable.

4.3.5 Tratamiento del riesgo

Habiendo completado la valoración de un riesgo, el tratamiento del riesgo implica la selección y el acuerdo sobre una o más opciones pertinentes para cambiar la probabilidad de ocurrencia del riesgo, su efecto, o ambos, y la implementación de estas opciones.

Esta actividad está seguida por un proceso cíclico de revaloración de los nuevos niveles de riesgo, con el fin de determinar su grado de tolerancia frente a los criterios establecidos previamente y decidir si se requiere tratamiento adicional.

4.3.6 Monitoreo y revisión

Como parte del proceso de gestión de riesgos, los riesgos y los controles se deberían monitorear y revisar regularmente para verificar que:

- las afirmaciones sobre los riesgos siguen siendo válidas;
- las afirmaciones sobre las cuales se basa la valoración del riesgo, incluyendo el contexto interno y externo, siguen siendo válidas;
- los resultados esperados se están alcanzando;
- los resultados de la valoración del riesgo siguen los lineamientos de la experiencia real;

- las técnicas de valoración del riesgo se aplican correctamente;
- los tratamientos del riesgo son eficaces.

Se debería establecer la responsabilidad por la rendición de cuentas con respecto al monitoreo y la realización de las revisiones

5. PROCESO DE VALORACIÓN DEL RIESGO

5.1 INFORMACIÓN GENERAL

La valoración del riesgo brinda a aquellos que toman las decisiones y a las partes responsables una comprensión mejorada de los riesgos que podrían afectar al logro de los objetivos, y a la idoneidad y eficacia de los controles ya implementados. Ésta brinda una base para las decisiones acerca del enfoque más adecuado que se ha de utilizar para tratar los riesgos. El resultado de la valoración del riesgo es un elemento de entrada para el proceso de toma de decisiones de la organización.

La valoración del riesgo es el proceso general de identificación del riesgo, análisis del riesgo y evaluación del riesgo (véase la Figura 1). La manera en la cual se aplica el proceso depende no solamente del contexto del proceso de la gestión de riesgos sino también de los métodos y de las técnicas utilizadas para llevar a cabo la valoración del riesgo.

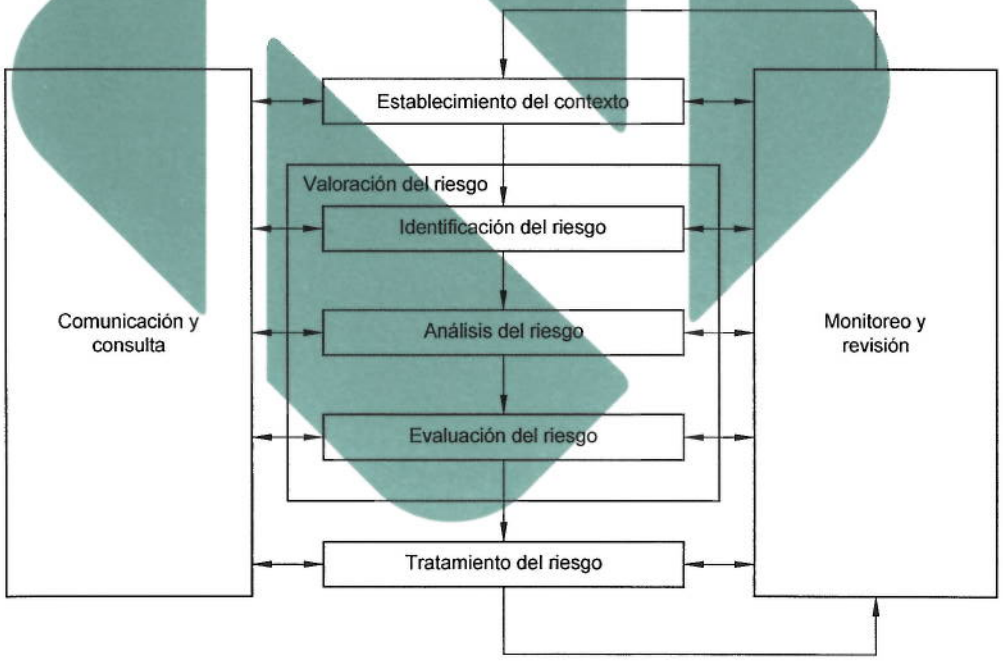


Figura 1. Contribución de la valoración del riesgo al proceso de gestión de riesgos

La valoración del riesgo puede requerir de un enfoque multidisciplinario, dado que los riesgos pueden cubrir un rango amplio de causas y consecuencias.

5.2 IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo es el proceso para hallar, reconocer y registrar los riesgos.

El propósito de la identificación del riesgo es identificar lo que podría suceder o cuáles situaciones podrían existir que afecten el logro de los objetivos del sistema o la organización. Una vez se ha identificado el riesgo, la organización debería identificar todos los controles existentes, tales como las características del diseño, las personas, los procesos y los sistemas.

El proceso de identificación del riesgo incluye identificar las causas y la fuente del riesgo (peligro en el contexto de daño físico), los eventos, las situaciones o las circunstancias que podrían tener un impacto material sobre los objetivos y la naturaleza de dicho impacto.

Los métodos para la identificación del riesgo pueden incluir:

- métodos basados en la evidencia, ejemplos de los cuales son las listas de verificación y las revisiones de los datos históricos;
- enfoques sistemáticos en equipo, en los cuales un equipo de expertos sigue un proceso sistemático para identificar los riesgos por medio de un conjunto estructurado de preguntas o declaraciones;
- técnicas de razonamiento inductivo tales como la de peligro y operatividad (EPO – Estudios de Peligro y Operatividad (HAZOP – *Hazard and Operability*).

Se pueden utilizar varias técnicas de soporte para mejorar la exactitud y la completitud en la identificación del riesgo, incluyendo la lluvia de ideas y la metodología *Delphi*.

Independientemente de las técnicas reales utilizadas, es importante el reconocimiento correcto de los factores humanos y organizacionales cuando se identifica el riesgo. Por lo tanto, las desviaciones de los factores humanos y organizacionales con respecto a lo esperado se deberían incluir en el proceso de identificación del riesgo, así como los eventos de "hardware" o "software".

5.3 ANÁLISIS DEL RIESGO

5.3.1 Generalidades

El análisis del riesgo consiste en el desarrollo de una comprensión del riesgo. Esta actividad suministra un elemento de entrada para la valoración del riesgo y la toma de decisiones acerca de si es necesario tratar el riesgo, y los métodos y estrategias de tratamiento más adecuadas.

El análisis del riesgo consiste en la determinación de las consecuencias y sus probabilidades para los elementos de riesgo identificados, tomando en consideración la presencia (o no) y la eficacia de 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 tales consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y la probabilidad. Un evento puede tener consecuencias múltiples y puede afectar a varios objetivos. Es recomendable tomar en consideración los controles existentes para el riesgo y su eficacia. Varios métodos para estos análisis se describen en el Anexo B. Para aplicaciones complejas puede ser necesaria más de una técnica.

Normalmente, el análisis del riesgo incluye una estimación del rango de las consecuencias que se pueden derivar de un evento, situación o circunstancia, y sus probabilidades asociadas, con el fin de medir el nivel del riesgo. Sin embargo, en algunos casos como por ejemplo cuando es probable que las consecuencias sean insignificantes o cuando se espera que la probabilidad sea extremadamente baja, la estimación de un solo parámetro puede ser suficiente para tomar una decisión.

En algunas circunstancias, una consecuencia puede ocurrir como resultado de un rango de eventos o condiciones diferentes, o cuando el evento específico no está identificado. En este caso, el enfoque de la valoración del riesgo está en el análisis de la importancia y la vulnerabilidad de los componentes del sistema con el fin de definir los tratamientos que se relacionan con los niveles de protección o las estrategias de recuperación.

Los métodos utilizados para el análisis de los riesgos pueden ser cualitativos, semicuantitativos o cuantitativos. El grado de detalle que se requiere dependerá de la aplicación particular, la disponibilidad de datos confiables de las necesidades para la toma de decisión de la organización. Algunos métodos y el grado de detalle del análisis pueden estar prescritos por la legislación.

La valoración cualitativa define la consecuencia, la probabilidad y el nivel del riesgo mediante niveles de importancia tales como "alto", "medio" y "bajo", puede combinar las consecuencias y las probabilidades y evaluar el nivel resultante del riesgo frente a los criterios cualitativos.

Los métodos semicuantitativos utilizan escalas de calificación numérica para la consecuencia y la probabilidad y las combinan para producir un nivel de riesgo utilizando 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 prácticos para las consecuencias y sus probabilidades, y produce valores del nivel de riesgo en unidades específicas definidas en el momento de desarrollar el contexto. El análisis cuantitativo completo no siempre puede ser posible o deseable debido a la información insuficiente acerca del sistema o de la actividad sometida a análisis, la falta de datos, la influencia de factores humanos, etc., o debido a que el esfuerzo en el análisis cuantitativo no está garantizado ni se exige. En tales circunstancias, una calificación comparativa semicuantitativa o cualitativa de los riesgos por parte de especialistas que conozcan muy bien sus campos respectivos, puede ser eficaz.

En los casos en que el análisis es cualitativo, debería haber una explicación clara de todos los términos utilizados y se deberían registrar las bases para todos los criterios.

Incluso cuando se ha llevado a cabo una cuantificación completa, es necesario reconocer que los niveles del riesgo calculado son estimaciones. Se recomienda precaución para garantizar que a ellos no se les atribuye un nivel de exactitud y precisión inconsistentes con la exactitud de los datos y los métodos empleados.

Los niveles del riesgo se deberían expresar en los términos más adecuados para ese tipo de riesgo y de forma tal que se facilite la evaluación del riesgo. En algunos casos, la magnitud de un riesgo se puede expresar como una distribución de probabilidad sobre un rango de consecuencias.

5.3.2 Valoración de los controles

El nivel de riesgo dependerá de la idoneidad y la eficacia de los controles existentes. Los interrogantes que se deben abordar incluyen:

- ¿Cuáles son los controles existentes para un riesgo particular?

- ¿Son tales controles capaces de tratar adecuadamente el riesgo de manera que esté sea controlado a un nivel tolerable?

- En la práctica ¿están los controles funcionando de la manera prevista y se puede demostrar que son eficaces cuando se requieren?

Estos interrogantes sólo se pueden responder con confianza si existen la documentación correcta y los procesos de aseguramiento.

El nivel de eficacia de un control particular o de un conjunto de controles relacionados se puede expresar cualitativamente, semicuantitativamente o cuantitativamente. En la mayoría de los casos, no se garantiza un nivel alto de exactitud. Sin embargo, puede ser útil expresar y registrar una medición de la eficacia del control del riesgo de modo que se puedan hacer juicios sobre si el esfuerzo se amplía mejor mejorando un control o suministrando un tratamiento diferente para el riesgo.

5.3.3 Análisis de las consecuencias

El análisis de las consecuencias determina la naturaleza y el tipo de impacto que se podría presentar, asumiendo que ha ocurrido una situación o circunstancia de un evento particular. Un evento puede tener un rango de impactos de diversas magnitudes y afectar a una gama de objetivos diferentes y a partes involucradas diversas. Los tipos de consecuencias que se han de analizar y las partes involucradas afectadas se habrán decidido en el momento de establecer el contexto.

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

Los impactos pueden tener una consecuencia baja pero una probabilidad alta, o una consecuencia alta con probabilidad baja o algún resultado intermedio. En algunos casos, es adecuado enfocarse en riesgos con resultados potencialmente muy grandes, dado que éstos con frecuencia son de máxima preocupación para los directores. En otros casos, puede ser importante analizar independientemente tanto los riesgos con consecuencia alta como aquellos con consecuencia baja. Por ejemplo, un problema frecuente pero con impacto bajo (o crónico) puede tener efectos acumulativos grandes a largo plazo. Además, las acciones de tratamiento para tratar estos dos tipos diferentes de riesgos con frecuencia son muy diferentes, por lo tanto es útil analizarlos por separado.

El análisis de las consecuencias puede involucrar:

- tomar en consideración los controles existentes para tratar las consecuencias, junto con todos los factores contribuyentes pertinentes que tienen un efecto en las consecuencias;

- relacionar las consecuencias del riesgo con los objetivos originales;

- considerar tanto las consecuencias inmediatas como aquellas que se pueden presentar después de transcurrido un tiempo determinado, si ello es consistente con el alcance de la valoración;

- considerar las consecuencias secundarias, tales como aquellas que tienen impacto en los sistemas, el equipo, las actividades o las organizaciones asociadas.

5.3.4 Análisis de la posibilidad (*Likelihood*) y estimación de la probabilidad

Comúnmente se utilizan tres enfoques generales para estimar la probabilidad; éstos se pueden utilizar individualmente o en conjunto:

a) El uso de los datos históricos pertinentes para identificar el evento o las situaciones que han ocurrido en el pasado y, por lo tanto, poder extrapolar la probabilidad de su ocurrencia en el futuro. Los datos utilizados deberían ser pertinentes para el tipo de sistema, instalación, organización o actividad en consideración y también para las normas operativas de la organización involucrada. Si, históricamente, existe una frecuencia muy baja de la ocurrencia, entonces cualquier estimación de la probabilidad será muy incierta. Esto se aplica especialmente para ocurrencias cero en las que uno no puede asumir que el evento, la situación o las circunstancias no ocurrirán en el futuro.

b) La previsión de la probabilidad utilizando técnicas predictivas tales como el análisis de árbol de fallas y el análisis de árbol de eventos (véase el Anexo B). Cuando los datos históricos no están disponibles o son inadecuados, es necesario derivar la probabilidad mediante el análisis del sistema, la actividad, el equipo o la organización y sus estados asociados de falla o éxito. Los datos numéricos para equipo, personas, organizaciones y sistemas desde el punto de vista de la experiencia operativa o de las fuentes de datos publicados se combinan después para producir una estimación de la probabilidad del evento máximo. Cuando se utilizan técnicas predictivas, es importante garantizar que se ha permitido la tolerancia debida en el análisis para la posibilidad de fallas de modo común que involucran la falla coincidente de diversas partes o componentes dentro del sistema que se originan en la misma causa. Pueden ser necesarias las técnicas de simulación para generar la probabilidad de fallas en el equipo y la estructura debido al envejecimiento y otros procesos de degradación, mediante el cálculo de los efectos de las incertidumbres.

c) La opinión de los expertos se puede utilizar en un proceso sistemático y estructurado para estimar la probabilidad. El juicio de los expertos se debería basar en toda la información pertinente disponible, incluyendo datos históricos, específicos para el sistema, específicos para la organización, experimentales, de diseño, etc. Existe una variedad de métodos formales para lograr el juicio experto, los cuales proporcionan una ayuda para la formulación de los interrogantes correctos. Los métodos disponibles incluyen al enfoque *Delphi*, las comparaciones pareadas, la clasificación en categorías y los juicios absolutos de probabilidad.

5.3.5 Análisis preliminar

Los riesgos se pueden clasificar con el fin de identificar aquellos más significativos o para excluir los riesgos menores o menos significativos en el análisis posterior. El propósito es garantizar que los recursos se dirigirán hacia los riesgos más importantes. Se recomienda precaución para no excluir riesgos bajos que ocurren con frecuencia y tienen un efecto acumulativo significativo.

La clasificación se debería basar en los criterios definidos en el contexto. El análisis preliminar determina uno o más de los siguientes cursos de acción:

- decidir tratar los riesgos sin valoración adicional;
- dejar de lado los riesgos insignificantes que no justificarían el tratamiento, o
- proseguir con una valoración del riesgo más detallada.

Es recomendable documentar las afirmaciones iniciales y los resultados.

5.3.6 Incertidumbres y sensibilidades

Con frecuencia existen incertidumbres considerables asociadas con el análisis del riesgo. Se necesita comprender tales incertidumbres para interpretar y comunicar eficazmente los resultados del análisis del riesgo. El análisis de las incertidumbres asociadas con los datos, los métodos y los modelos utilizados para identificar y analizar el riesgo juega un papel importante en su aplicación. El análisis de la incertidumbre implica la determinación de la variación o la imprecisión en los resultados, derivada de la variación colectiva en los parámetros y las afirmaciones utilizadas para definir los resultados. Un área relacionada estrechamente con el análisis de la incertidumbre es el análisis de sensibilidad.

El análisis de la sensibilidad implica la determinación del tamaño y la importancia de la magnitud del riesgo de cambio en parámetros de entrada individuales. Se utiliza para identificar aquellos datos que necesariamente deben ser exactos y aquellos que son menos sensibles y, por lo tanto, tienen menos efecto en la exactitud total.

La exhaustividad y exactitud del análisis del riesgo se deberían establecer de la manera más completa posible. Es recomendable identificar las fuentes de incertidumbre siempre que sea posible y tratar las incertidumbres tanto de los datos como del modelo/método. Se deberían establecer los parámetros para los cuales el análisis es sensible y el grado de sensibilidad.

5.4 EVALUACIÓN DEL RIESGO

La evaluación del riesgo implica la comparación de los niveles estimados del riesgo con los criterios del riesgo definidos al establecer el contexto, con el fin de determinar la importancia del nivel y el tipo de riesgo.

La evaluación del riesgo utiliza la comprensión del riesgo que se obtuvo durante el análisis para tomar decisiones acerca de las acciones futuras. Las consideraciones éticas, legales, financieras y otras, incluyendo las percepciones del riesgo, también son elementos de entrada para la toma de decisiones.

Las decisiones pueden incluir:

- si el riesgo necesita tratamiento o no;
- las prioridades para el tratamiento;
- si se debería emprender una actividad o no;
- cuál de diversas rutas se debería seguir.

La naturaleza de las decisiones que se deben tomar y los criterios que se van a utilizar para tomar tales decisiones se decidieron al establecer el contexto, pero es necesario considerarlas en más detalle en esta etapa, en la cual se sabe más acerca de los riesgos particulares identificados.

El marco de referencia más sencillo para definir los criterios del riesgo está constituido por un solo nivel que separa los riesgos que necesitan tratamiento de aquellos que no lo necesitan. Esto proporciona resultados atractivamente sencillos pero no refleja las incertidumbres involucradas tanto en la estimación del riesgo como en la definición de los límites entre aquellos que necesitan tratamiento y aquellos que no.

La decisión sobre si tratar un riesgo o no y cómo hacerlo puede depender de los costos y los beneficios de tomar el riesgo y de los costos y beneficios de implementar controles mejorados.

Un enfoque común es dividir los riesgos en tres bandas:

a) una banda superior en donde el nivel del riesgo se considera intolerable cualesquiera sean los beneficios que la actividad pueda suministrar, y el tratamiento del riesgo es esencial sin importar su costo;

b) una banda media (o área "gris") en donde se tienen en cuenta los costos y los beneficios, y las oportunidades se ponderan frente a las consecuencias potenciales;

c) una banda inferior en donde el nivel de riesgo se considera insignificante o tan pequeño que no es necesaria ninguna medida de tratamiento.

El sistema de criterios "tan bajos como sea razonablemente factible" utilizado en las aplicaciones de seguridad siguen este enfoque, en el cual, en la banda media, existe una escala móvil para los riesgos bajos en la cual los costos y los beneficios se pueden comparar directamente, mientras que para los riesgos altos se debe reducir el potencial de daño hasta que el costo de la reducción adicional sea totalmente desproporcionado con respecto al beneficio de seguridad que se obtiene.

5.5 DOCUMENTACIÓN

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

La extensión del informe dependerá de los objetivos y del alcance de la valoración. Excepto para valoraciones muy sencillas, la documentación puede incluir:

- objetivos y alcance;
- descripción de las partes pertinentes del sistema y sus funciones;
- un resumen del contexto externo y del interno de la organización y cómo se relaciona con la situación, el sistema o las circunstancias que se están valorando;
- los criterios de riesgo aplicados y su justificación;
- las limitaciones, afirmaciones y justificaciones de las hipótesis;
- la metodología de la valoración;
- los resultados de la identificación del riesgo;
- los datos, las afirmaciones y sus fuentes y validación;
- los resultados del análisis del riesgo y su evaluación;
- el análisis de sensibilidad e incertidumbre;
- las afirmaciones críticas y otros factores que es necesario controlar;

- la discusión de los resultados;
- las conclusiones y recomendaciones;
- las referencias.

Si la valoración del riesgo da soporte a un proceso de gestión de riesgos continuo, ésta se debería llevar a cabo y documentar de forma tal que se mantenga durante toda la duración del sistema, la organización, el equipo o la actividad. La valoración se debería actualizar a medida que se dispone de información nueva y significativa, en la medida que cambia el contexto, de acuerdo con las necesidades del proceso de gestión.

5.6 MONITOREO Y REVISIÓN DE LA VALORACIÓN DEL RIESGO

El proceso de valoración del riesgo enfatizará el contexto y otros factores que se presume podrían variar con el paso del tiempo y que podrían cambiar la valoración del riesgo o invalidarla. Estos factores se deberían identificar específicamente para su revisión y monitoreo continuos, de forma tal que la valoración del riesgo se pueda actualizar cuando sea necesario.

También se deberían identificar y recolectar los datos que se van a monitorear con el fin de perfeccionar la valoración del riesgo.

La eficacia de los controles también se debería monitorear y documentar con el fin de brindar datos para el uso en el análisis del riesgo. La rendición de cuentas con respecto a la creación y la revisión de la evidencia y la documentación también se debería definir.

5.7 APLICACIÓN DE LA VALORACIÓN DEL RIESGO DURANTE LAS FASES DEL CICLO DE DURACIÓN

Se puede considerar que muchas actividades, proyectos y productos tienen un ciclo de duración que empieza con el concepto inicial y la definición, pasa por la realización y va hasta la terminación final, la cual podría incluir el desmantelamiento y la disposición final del hardware.

La valoración del riesgo se puede aplicar en todas las etapas del ciclo de duración y, usualmente se aplica muchas veces con diversos niveles de detalle para facilitar las decisiones que se deben tomar en cada fase.

Las fases de los ciclos de duración tienen requisitos diferentes que necesitan diferentes técnicas. Por ejemplo, durante la fase de concepto y definición, cuando se identifica una oportunidad, la valoración del riesgo se puede utilizar para decidir si proseguir o no.

Cuando se dispone de varias opciones, la valoración del riesgo se puede usar para evaluar conceptos alternativos con el fin de ayudar a decidir cuál de ellas proporciona el mejor equilibrio de riesgos positivos y negativos.

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

- garantizar que los riesgos para el sistema son tolerables,
- el proceso de perfeccionamiento del diseño,
- los estudios de eficacia en términos de costo,

- identificar los riesgos que tienen impacto en las fases posteriores del ciclo de duración.

A medida que la actividad prosigue, la valoración del riesgo se puede utilizar para obtener información que facilite el desarrollo de procedimientos para condiciones normales y de emergencia.

6. SELECCIÓN DE LAS TÉCNICAS DE VALORACIÓN DEL RIESGO

6.1 GENERALIDADES

Esta sección describe cómo se pueden seleccionar las técnicas para la valoración del riesgo. Los anexos enumeran y explican en más detalle un rango de herramientas y técnicas que se pueden utilizar para llevar a cabo una valoración del riesgo o para facilitar el proceso de valoración del riesgo. Algunas veces puede ser necesario emplear más de un método de valoración.

6.2 SELECCIÓN DE LAS TÉCNICAS

La valoración del riesgo se puede emprender con grados diversos de profundidad y detalle y utilizando uno o muchos métodos que van desde lo sencillo hasta lo complejo. La forma de valoración y sus resultados deberían ser consistentes con los criterios del riesgo desarrollados como parte del establecimiento del contexto. El Anexo A ilustra la relación conceptual entre las muchas categorías de técnicas para la valoración del riesgo y los factores presentes en una situación de riesgo determinada, y proporciona ejemplos ilustrativos de cómo las organizaciones pueden seleccionar las técnicas adecuadas para la valoración del riesgo en una situación particular.

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

- deberían ser justificables y adecuadas para la situación o la organización en cuestión
- deberían suministrar resultados en una forma que mejore la comprensión de la naturaleza del riesgo y de la manera en que se puede tratar;
- deberían poderse utilizar de una manera repetible, verificable y a la que se pueda hacer seguimiento.

Se deberían suministrar las razones para la elección de las técnicas con respecto a la pertinencia y la idoneidad. Cuando se integran los resultados de estudios diferentes, las técnicas utilizadas y los resultados deberían ser comparables.

Una vez que se ha decidido llevar a cabo una valoración del riesgo y se han definido los objetivos y el alcance, las técnicas se deberían seleccionar con base en factores aplicables tales como:

- Los objetivos del estudio. Los objetivos de la valoración del riesgo tendrán un efecto directo en las técnicas utilizadas. Por ejemplo, si se realiza un estudio comparativo entre diferentes opciones, se acepta utilizar modelos de consecuencia menos detallados para las partes del sistema que no están afectadas por la diferencia.

- Las necesidades de quienes toman las decisiones. En algunos casos, se necesita un nivel alto de detalles para tomar una buena decisión, en otros una comprensión más general puede ser suficiente.

- El tipo y el rango de los riesgos que se analizan.

- La magnitud potencial de las consecuencias. La decisión sobre la profundidad hasta la cual se realiza la valoración del riesgo debería reflejar la percepción inicial de las consecuencias (aunque esto se puede modificar una vez se ha completado la evaluación preliminar).

- El grado de experticia, recursos humanos y otros que son necesarios. Un método sencillo, bien realizado, puede suministrar mejores resultados que un procedimiento más sofisticado realizado de forma deficiente, siempre que satisfaga los objetivos y el alcance de la valoración. Comúnmente, el esfuerzo puesto en la valoración debería ser consistente con el nivel potencial del riesgo que se analiza.

- La disponibilidad de información y datos. Algunas técnicas requieren de más información y datos que otras.

- La necesidad de modificación/actualización de la valoración del riesgo. Puede ser necesario modificar/actualizar la valoración en el futuro, y algunas técnicas son más flexibles que otras a este respecto.

- Todos los requisitos reglamentarios y contractuales.

Diversos factores influyen en la selección de un enfoque para la valoración del riesgo, por ejemplo la disponibilidad de recursos, la naturaleza y el grado de la incertidumbre en los datos y la información disponible, así como la complejidad de la aplicación (véase la Tabla A.2).

6.3 DISPONIBILIDAD DE RECURSOS

Los recursos y las capacidades que pueden tener efecto en la escogencia de las técnicas para la valoración del riesgo incluyen:

- la capacidad, experiencia y habilidades del equipo a cargo de la valoración del riesgo;

- las restricciones de tiempo y otros recursos dentro de la organización;

- el presupuesto disponible, si se requieren recursos externos.

6.4 LA NATURALEZA Y EL GRADO DE LA INCERTIDUMBRE

La naturaleza y el grado de incertidumbre requieren de la comprensión de la calidad, cantidad e integridad de la información disponible con respecto al riesgo en cuestión. Ello incluye la disponibilidad de información suficiente acerca del riesgo, sus fuentes y causas, y sus consecuencias para el logro de los objetivos. La incertidumbre se puede derivar de datos con calidad deficiente o de la falta de datos esenciales y confiables. Por ejemplo, los métodos de recolección de datos pueden cambiar, la forma en que las organizaciones utilizan tales métodos puede cambiar o puede que la organización no tenga un método de recolección eficaz para reunir los datos acerca del riesgo identificado.

La incertidumbre también puede ser inherente al contexto externo e interno de la organización. Los datos disponibles no siempre suministran una base confiable para la predicción del futuro.

Para tipos únicos de riesgos, es posible que no se disponga de datos históricos o que existan diversas interpretaciones de los datos disponibles por parte de las diferentes partes involucradas. Aquellos que realizan la valoración del riesgo deben comprender el tipo y la naturaleza de la incertidumbre y considerar las implicaciones para la confiabilidad de los resultados de tal valoración. Éstas se deberían comunicar siempre a quienes toman las decisiones.

6.5 COMPLEJIDAD

Los riesgos pueden ser complejos por sí solos, como por ejemplo en los sistemas complejos en los que es necesario valorar los riesgos a través de todo el sistema en lugar de tratar cada componente por separado e ignorar las interacciones. En otros casos, el tratamiento de un riesgo único puede tener implicaciones en otras partes y puede tener impacto en otras actividades. Es necesario comprender los impactos consecuenciales y las dependencias del riesgo para garantizar que en la gestión del riesgo no se cree una situación intolerable en otra parte del sistema. La comprensión de la complejidad de un solo riesgo o de un portafolio de riesgos en una organización es crucial para la selección del método o las técnicas adecuadas para la valoración del riesgo.

6.6 APLICACIÓN DE LA VALORACIÓN DEL RIESGO DURANTE LAS FASES DEL CICLO DE DURACIÓN

Se puede considerar que muchas actividades, proyectos y productos tienen un ciclo de duración que empieza con el concepto inicial y la definición, pasa por la realización y llega a la terminación final, la cual puede incluir el desmantelamiento y la disposición final del hardware.

La valoración del riesgo se puede aplicar en todas las etapas del ciclo de duración y, usualmente se aplica muchas veces con diversos niveles de detalle para facilitar las decisiones que se deben tomar en cada fase.

Las fases de los ciclos de duración tienen requisitos diferentes que necesitan diferentes técnicas. Por ejemplo, durante la fase de concepto y definición, cuando se identifica una oportunidad, la valoración del riesgo se puede utilizar para decidir si proseguir o no.

Cuando se dispone de varias opciones, la valoración del riesgo se puede usar para evaluar conceptos alternativos para ayudar a decidir cuál de ellas proporciona el mejor equilibrio de riesgos positivos y negativos.

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

- garantizar que los riesgos para el sistema son tolerables,
- el proceso de perfeccionamiento del diseño,
- los estudios de eficacia en términos de costo,
- identificar los riesgos que tienen impacto en las fases posteriores del ciclo de duración.

A medida que la actividad prosigue, la valoración del riesgo se puede utilizar para obtener información que facilite el desarrollo de procedimientos para condiciones normales y de emergencia.

6.7 TIPOS DE TÉCNICAS PARA LA VALORACIÓN DEL RIESGO

Las técnicas para la valoración del riesgo se pueden clasificar de diversas maneras para facilitar la comprensión de sus fortalezas y debilidades relativas. Las tablas del Anexo A correlacionan, con fines informativos, algunas técnicas potenciales con sus categorías.

Cada una de las técnicas se elabora en más detalle en el Anexo B en cuanto a la naturaleza de la valoración que suministran y las directrices para su aplicación en situaciones determinadas.

ANEXO A
(Informativo)

COMPARACIÓN DE LAS TÉCNICAS PARA LA VALORACIÓN DEL RIESGO

A.1 TIPOS DE TÉCNICAS

La primera clasificación muestra cómo se aplican las técnicas a cada paso del proceso de valoración del riesgo, como se indica a continuación:

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

Para cada paso en el proceso de valoración del riesgo, la aplicación del método se describe como rotundamente aplicable, aplicable o no aplicable (véase el Tabla A.1).

A.2 FACTORES QUE INFLUYEN EN LA SELECCIÓN DE LAS TÉCNICAS PARA LA VALORACIÓN DEL RIESGO

A continuación se describen los atributos de los métodos en términos de:

- complejidad del problema y los métodos necesarios para analizarlo,
- la naturaleza y grado de incertidumbre de la valoración del riesgo con base en la cantidad de información disponible y en los requisitos para satisfacer los objetivos,
- la cantidad de recursos necesarios en términos de tiempo y nivel de experticia, necesidades de datos o costos,
- si el método puede suministrar un resultado cuantitativo o no.

Los ejemplos de los tipos de métodos disponibles para la valoración del riesgo se enumeran en la Tabla A.2, en la cual cada método se clasifica como alto, medio o bajo, en términos de estos atributos.

Tabla A.1. Aplicabilidad de las herramientas para la valoración del riesgo

Herramientas y técnicas	Proceso de valoración del riesgo					Véase el Anexo
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Lluvia de ideas	SA[1)]	NA[2)]	NA	NA	NA	B.01
Entrevistas estructuradas o semiestructuradas	SA	NA	NA	NA	NA	B.02
Delphi	SA	NA	NA	NA	NA	B.03
Listas de verificación	SA	NA	NA	NA	NA	B.04
Análisis primario de peligros	SA	NA	NA	NA	NA	B.05
Estudios de peligro y operatividad (EPO)(HAZOP)	SA	SA	A[3)]	A	A	B.06
Análisis de peligros y puntos críticos de control (APPCC [HACCP])	SA	SA	NA	NA	SA	B.07
Valoración del riesgo ambiental	SA	SA	SA	SA	SA	B.08
Estructura "¿qué pasaría si?" (EQPS [SWIFT])	SA	SA	SA	SA	SA	B.09
Análisis de escenario	SA	SA	A	A	A	B.10
Análisis del impacto en el negocio	A	SA	A	A	A	B.11
Análisis de la causa principal (ACP)	NA	SA	SA	SA	SA	B.12
Análisis de modo y efecto de falla (EMEF)	SA	SA	SA	SA	SA	B.13
Análisis de árbol de fallas	A	NA	SA	A	A	B.14
Análisis de árbol de eventos	A	SA	A	A	NA	B.15
Análisis de causa y consecuencia	A	SA	SA	A	A	B.16
Análisis de causa y efecto	SA	SA	NA	NA	NA	B.17
Análisis de capas de protección (ACDP [LOPA])	A	SA	A	A	NA	B.18
Árbol de decisión	NA	SA	SA	A	A	B.19
Análisis de confiabilidad humana	SA	SA	SA	SA	A	B.20
Análisis de esquema en corbatín (bow tie)	NA	A	SA	SA	A	B.21
Mantenimiento enfocado en la confiabilidad	SA	SA	SA	SA	SA	B.22
Análisis de circuito furtivo	A	NA	NA	NA	NA	B.23
Análisis de Markov	A	SA	NA	NA	NA	B.24
Simulación de Monte Carlo	NA	NA	NA	NA	SA	B.25
Estadísticas y redes bayesianas	NA	SA	NA	NA	SA	B.26
Curvas FN	A	SA	SA	A	SA	B.27
Índices de riesgo	A	SA	SA	A	SA	B.28
Matriz de consecuencia y probabilidad	SA	SA	SA	SA	A	B.29
Análisis de costo y beneficio	A	SA	A	A	A	B.30
Análisis de decisión por criterios múltiples (ADCM [MCDA])	A	SA	A	SA	A	B.31

[1)] Rotundamente aplicable RA
[2)] No aplicable NA
[3)] Aplicable A

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

Ejemplo del tipo de técnica y método para la valoración del riesgo	Descripción	Importancia de los factores de influencia			¿Es posible un resultado cuantitativo?
MÉTODOS DE BÚSQUEDA					
Listas de verificación	Una forma sencilla para la identificación del riesgo. Técnica que suministra un listado de incertidumbres típicas que es necesario considerar. Los usuarios consultan listas, códigos o normas desarrollados previamente.	Bajo	Bajo	Bajo	No
Análisis preliminar del peligro	Un método inductivo sencillo para el análisis cuyo objetivo es identificar los peligros y las situaciones y eventos peligrosos que pueden causar daño a una actividad, instalación o un sistema determinados.	Bajo	Alto	Medio	No
MÉTODOS DE SOPORTE					
Entrevista estructurada y lluvia de ideas	Medios para recolectar un conjunto amplio de ideas y evaluación, las cuales son calificadas por un equipo. Las lluvias de ideas puede estar estimulada por mensajes guía o por técnicas de entrevista personalizada o de grupo.	Bajo	Bajo	Bajo	No
Técnica Delphi	Es un medio para combinar opiniones de los expertos que pueden dar soporte a la fuente e influir en la identificación, la probabilidad y la estimación de la consecuencia, y en la evaluación del riesgo. Es una técnica de colaboración para crear consenso entre los expertos. Implica el análisis independiente y la votación de los expertos.	Medio	Medio	Medio	No
Técnica estructurada "¿qué pasaría si?"(EQPS)	Sistema para urgir a un equipo a que identifique los riesgos. Se utiliza normalmente dentro de un taller de facilitación. Está vinculada comúnmente al análisis del riesgo y a la técnica de evaluación.	Medio	Medio	Ninguna	No
Análisis de confiabilidad humana (ACH [HRA])	La valoración de la confiabilidad humana trata del impacto de las personas en el desempeño del sistema y se puede utilizar para evaluar las influencias del error humano en el sistema.	Medio	Medio	Medio	Si
ANÁLISIS DE ESCENARIO					
Análisis de la causa principal (análisis de una sola pérdida)	Se analiza una sola pérdida que ha ocurrido con el fin de entender las causas contribuyentes y la manera en que el sistema o el proceso se pueden mejorar para evitar tales pérdidas en el futuro. El análisis debe considerar los controles implementados en el momento que se presentó la pérdida y cómo se podrían mejorar tales controles.	Medio	Bajo	Medio	No
Análisis de escenario	Se identifican posibles escenarios en el futuro a través de la imaginación o la extrapolación del presente y se toman en consideración diversos riesgos asumiendo que se podría presentar cada uno de estos escenarios. Esto se puede realizar formal o informalmente, cualitativa o cuantitativamente.	Medio	Alto	Medio	No

Continúa...

Tabla A.2. (Continuación)

Ejemplo del tipo de técnica y método para la valoración del riesgo	Descripción	Importancia de los factores de influencia			¿Es posible un resultado cuantitativo?
Valoración del riesgo toxicológico	Se identifican y analizan los peligros y las posibles rutas mediante las cuales un objeto específico podría estar expuesto al peligro. La información sobre el nivel de exposición y la naturaleza del daño causado por un nivel determinado de exposición se combinan para obtener una medida de la probabilidad de que se presente el daño especificado.	Alto	Alto	Medio	Si
Análisis del impacto en el negocio	Brinda un análisis de la manera en que los riesgos de alteración clave podrían afectar a las operaciones de una organización e identifica y cuantifica las capacidades que se necesitarían para su gestión.	Medio	Medio	Medio	No
Análisis de árbol de fallas	Técnica que empieza con un evento no deseado (eventos máximos) y determina todas las maneras en que éste podría ocurrir. Estas maneras se presentan gráficamente en un diagrama de árbol lógico. Una vez que se ha elaborado el árbol de fallas se deberían considerar los modos para reducir o eliminar las causas o fuentes potenciales.	Alto	Alto	Medio	Sí
Análisis de árbol de eventos	Utilización de razonamiento inductivo para transformar las probabilidades de diversos eventos causantes en resultados posibles.	Medio	Medio	Medio	Si
Análisis de causas y consecuencias	Combinación de análisis de árbol de fallas y de árbol de eventos que permite la inclusión de los retrasos. Se toman en consideración tanto las causas como las consecuencias de un evento causal.	Alto	Medio	Alto	Sí
Análisis de causa y efecto	Un efecto puede tener una cantidad de factores contribuyentes que se pueden agrupar en diversas categorías. Con frecuencia los factores contribuyentes se identifican a través de lluvia de ideas y se presentan en una estructura de árbol o de diagrama de Ishikawa (causa y efecto).	Bajo	Bajo	Medio	No
ANÁLISIS DE LA FUNCIÓN					
AMEF y AMEFC	El análisis de modo y efecto de falla es una técnica que identifica los modos y los mecanismos de la falla y sus efectos. Existen varios tipos de AMEF: AMEF del diseño (o producto) que se utiliza para componentes y productos, AMEF del sistema que se utiliza para sistemas, AMEF del proceso que se utiliza para procesos de fabricación y ensamble, AMEF del servicio y AMEF del software. Este análisis puede estar seguido por un análisis de criticidad que define la importancia de cada modo de fallo, cualitativamente, semicualitativamente o cuantitativamente (AMEFC). El análisis de criticidad se puede basar en la probabilidad de que un modo de falla resulte en una falla en el sistema, el nivel del riesgo asociado con el modo de falla o un número para la prioridad del riesgo.	Medio	Medio	Medio	Sí

Tabla A.2. (Continuación)

Ejemplo del tipo de técnica y método para la valoración del riesgo	Descripción	Importancia de los factores de influencia			¿Es posible un resultado cuantitativo?
Mantenimiento enfocado en la confiabilidad	Un método para identificar las políticas que se deberían implementar para la gestión de fallas, en cuanto al logro de manera eficiente y eficaz de la seguridad exigida y la disponibilidad y economía de la operación para todos los tipos de equipo.	Medio	Medio	Medio	Sí
Análisis de circuito fortuito	Una metodología para identificar los errores en el diseño. Una condición fortuita es un hardware o un software latentes, o una condición integrada que puede causar un evento indeseado o inhibir al evento deseado y no es causada por falla en el componente. Estas condiciones se caracterizan por su naturaleza aleatoria y la capacidad para escapar a la detección durante las pruebas más rigurosas de sistemas normalizados. Las condiciones fortuitas pueden causar mal funcionamiento, pérdida de la disponibilidad del sistema, retrasos en el programa o incluso muerte o lesión de las personas.	Medio	Medio	Medio	No
EPO Estudios de peligro y operatividad	Un proceso general de identificación de riesgos para definir las desviaciones posibles con respecto al desempeño previsto o esperado. Utiliza un sistema basado en palabras guía. Se valora la criticidad de las desviaciones.	Medio	Alto	Alto	No
APPCC Análisis de peligros y puntos críticos de control	Un sistema preventivo, proactivo y sistemático para garantizar la calidad del producto, la confiabilidad y seguridad de los procesos mediante la medición y el monitoreo de características específicas que deben estar dentro de límites definidos.	Medio	Medio	Medio	No
VALORACIÓN DE LOS CONTROLES					
ACDP Análisis de capas de protección	(También se puede denominar análisis de barrera). Permite evaluar los controles y su eficacia.	Medio	Medio	Medio	Sí
Análisis en esquema de corbatín	Una forma diagramática sencilla de describir y analizar las rutas de un riesgo desde los peligros hasta los resultados y de revisar los controles. Se puede considerar como la combinación de la lógica de un árbol de fallas que analiza la causa de un evento (representado por el centro de la mariposa) y un árbol de eventos que analiza las consecuencias	Medio	Alto	Medio	Sí
MÉTODOS ESTADÍSTICOS					
Análisis de Markov	Este análisis, en ocasiones denominado análisis de estado-espacio, se utiliza comúnmente en el análisis de sistemas complejos reparables que pueden presentarse en varios estados, incluyendo diversos estados degradados.	Alto	Bajo	Alto	Sí

Tabla A.2. (Final)

Ejemplo del tipo de técnica y método para la valoración del riesgo	Descripción	Importancia de los factores de influencia			¿Es posible un resultado cuantitativo?
Análisis de Monte Carlo	Esta simulación se utiliza para establecer la variación agregada en un sistema, la cual resulta de las variaciones en el sistema, para un número de elementos de entrada, en donde cada elemento de entrada tiene una distribución definida y las entradas se relacionan con la salida a través de relaciones definidas. El análisis se puede utilizar para modelos específicos en los que se pueden definir matemáticamente las interacciones de las diversas entradas. Las entradas se pueden basar en una variedad de tipos de distribución de acuerdo con la naturaleza de la incertidumbre que ellas pretenden representar. Para la valoración del riesgo, se utilizan comúnmente distribuciones triangulares o beta.	Alto	Bajo	Alto	Sí
Análisis bayesiano	Un procedimiento estadístico que utiliza datos de distribución previa para evaluar la probabilidad de un resultado. Este análisis depende de la exactitud de la distribución previa para deducir un resultado exacto. La convicción bayesiana interconecta el modelo de causa y efecto en una variedad de dominios al capturar relaciones probabilísticas de entradas variables para derivar un resultado.	Alto	Bajo	Alto	Sí

ANEXO B
(Informativo)

TÉCNICAS PARA LA VALORACIÓN DEL RIESGO

B.1 LLUVIA DE IDEAS

B.1.1 Información general

La lluvia de ideas implica estimular y fomentar el flujo libre de la conversación entre un grupo de personas con conocimiento para identificar los modos potenciales de falla y los peligros asociados, los riesgos, los criterios para las decisiones y/o las opciones de tratamiento. El término "lluvia de ideas" con frecuencia se utiliza de manera muy laxa para indicar cualquier tipo de discusión de grupo. Sin embargo, la verdadera lluvia de ideas implica técnicas particulares para tratar de garantizar la estimulación de la imaginación de las personas mediante los pensamientos y las declaraciones de los otros del grupo.

La facilitación eficaz es muy importante en esta técnica e incluye la estimulación de la discusión al empezar, la orientación periódica del grupo hacia otras áreas pertinentes y la captura de los aspectos derivados de la discusión (la cual generalmente es muy vívida).

B.1.2 Uso

La lluvia de ideas se puede utilizar junto con otros métodos de valoración del riesgo descritos posteriormente o puede ser independiente como técnica para fomentar el pensamiento imaginativo en cualquier etapa del proceso de gestión de riesgos y en cualquier etapa del ciclo de duración de un sistema. Se puede utilizar para discusiones de alto nivel en las que se identifican los problemas, para la revisión más detallada, o en un nivel detallado para problemas particulares.

La lluvia de ideas enfatiza significativamente la imaginación. Por lo tanto, es particularmente útil para la identificación de los riesgos de las tecnologías nuevas, cuando no existen datos o cuando se necesitan soluciones novedosas para los problemas.

B.1.3 Elementos de entrada

Un grupo de personas con conocimiento sobre la organización, el sistema, el proceso o la aplicación que se está valorando.

B.1.4 Proceso

La lluvia de ideas puede ser formal o informal. La lluvia de ideas formal es más estructurada, con participantes preparados con anticipación y la sesión tiene un propósito y un resultado definidos con medios para evaluar las ideas presentadas. La lluvia de ideas informal es menos estructurada y con frecuencia es más específica para un fin determinado.

En un proceso formal:

- el facilitador prepara antes de la sesión las orientaciones y guías de pensamiento adecuadas para el contexto;
- se definen los objetivos de la sesión y se explican las reglas;

- el facilitador empieza una secuencia de pensamiento y todos exploran las ideas identificando tantos aspectos como sea posible. No hay discusión en este punto acerca de si las cosas deberían o no estar en una lista ni sobre lo que significan las declaraciones particulares, ya que esto tiende a inhibir el flujo libre del pensamiento. Todos los elementos de entrada se aceptan y ninguno se critica, y el grupo se mueve rápidamente para permitir que las ideas promuevan el pensamiento lateral;

- el facilitador puede orientar a las personas en una nueva ruta cuando se ha agotado una dirección de pensamiento o cuando la discusión se desvía demasiado. Sin embargo, el propósito es recolectar tantas ideas diversas como sea posible para el análisis posterior.

B.1.5 Elementos de salida

Los elementos de salida dependen de la etapa del proceso de valoración del riesgo en la cual se apliquen, por ejemplo en la etapa de identificación los elementos de salida podrían ser una lista de riesgos y los controles vigentes.

B.1.6 Fortalezas y limitaciones

Las fortalezas de la lluvia de ideas incluyen:

- fomenta la imaginación, lo cual ayuda a identificar riesgos nuevos y soluciones novedosas;

- hace partícipes a las partes involucradas clave y, por lo tanto, facilitan la comunicación general;

- es relativamente fácil y rápida de establecer.

Las limitaciones incluyen:

- los participantes pueden carecer de la habilidad y el conocimiento, lo cual no les permite ser contribuyentes eficaces;

- dado que relativamente no es estructurada, es difícil demostrar que el proceso ha sido exhaustivo, por ejemplo demostrar que todo los riesgos potenciales se han identificado;

- puede existir una dinámica de grupo particular en la que algunas personas con ideas útiles permanecen en silencio mientras que otras dominan la discusión. Esto se puede solucionar mediante las lluvias de ideas por computador, usando un foro de conversación o una técnica de grupo nominal. La lluvia de ideas por computador se puede establecer para que sea anónima, evitando así los aspectos políticos y personales que pueden impedir el flujo libre de las ideas. En la técnica de grupo nominal, las ideas se presentan de manera anónima a un moderador y luego son discutidas por el grupo.

B.2 ENTREVISTAS EN ESTRUCTURADAS O SEMIESTRUCTURADAS

B.2.1 Información general

En una entrevista estructurada, a los entrevistados individuales se les hace una serie de preguntas preparadas tomadas de una hoja guía que anima al entrevistado a visualizar una

situación desde una perspectiva diferente e identificar así los riesgos a partir de tal perspectiva. La entrevista semiestructurada es similar, pero permite mayor libertad de conversación para explorar los aspectos que se van originando.

B.2.2 Uso

Las entrevistas estructuradas y semiestructuradas son útiles cuando es difícil hacer que las personas se reúnan para una sesión de lluvia de ideas o cuando el flujo libre de una discusión en un grupo no es el adecuado para la situación o las personas implicadas. Estas entrevistas se utilizan con más frecuencia para identificar riesgos o para evaluar la eficacia de los controles existentes como parte del análisis del riesgo. Se pueden aplicar en cualquier etapa de un proyecto o proceso. Constituyen un medio para suministrar a las partes involucradas los elementos de entrada para la valoración del riesgo.

B.2.3 Elementos de entrada

Estos elementos incluyen:

- una definición clara de los objetivos de las entrevistas;
- una lista de los entrevistados seleccionados entre las partes involucradas pertinentes;
- un conjunto elaborado de preguntas.

B.2.4 Proceso

Se crea un conjunto de preguntas pertinentes para guiar al entrevistador. Siempre que sea posible las preguntas deberían ser abiertas, sencillas, tener un lenguaje adecuado para los entrevistados y abarcar solamente un aspecto. También se elaboran posibles preguntas de seguimiento para buscar aclaraciones.

Después las preguntas se le presentan a la persona que está siendo entrevistada. Cuando se busca mayor elaboración, las respuestas deberían ser abiertas. Se recomienda precaución para no "guiar" al entrevistado.

Las respuestas se deberían tomar en consideración con algún grado de flexibilidad con el fin de brindar la oportunidad de explorar las áreas hacia las cuales el entrevistado puede querer dirigirse.

B.2.5 Elementos de salida

Los elementos de salida son los puntos de vista de las partes involucradas sobre los aspectos que se tratan en las entrevistas.

B.2.6 Fortalezas y limitaciones

Las fortalezas de las entrevistas estructuradas son las siguientes:

- las entrevistas estructuradas permiten a las personas tener tiempo para un pensamiento considerado sobre el tema;
- la comunicación personalizada puede permitir mayor profundidad en la consideración de los temas;

- las entrevistas estructuradas permiten la participación de un número mayor de partes involucradas que la lluvia de ideas la cual utiliza un grupo relativamente pequeño.

Las limitaciones son:

- se necesita mucho tiempo para que el facilitador obtenga opiniones variadas de esta manera;
- se tolera el sesgo y no se elimina mediante la discusión del grupo;
- es posible que no se logre la motivación de la imaginación que es una característica de la lluvia de ideas.

B.3 TÉCNICA DELPHI

B.3.1 Información general

Esta técnica es un procedimiento para obtener un consenso confiable de la opinión de un grupo de expertos. Aunque actualmente este término se utiliza con frecuencia de manera amplia para indicar cualquier forma de lluvia de ideas, una característica esencial de la técnica Delphi, tal como se formuló originalmente, es que los expertos expresan sus opiniones individualmente y de manera anónima al tiempo que tienen acceso a los puntos de vista de otros expertos a medida que el proceso avanza.

B.3.2 Uso

Esta técnica se puede aplicar en cualquier etapa del proceso de gestión de riesgos o en cualquier fase de un ciclo de duración de un sistema, siempre que se necesite el consenso de los puntos de vista de los expertos.

B.3.3 Elementos de entrada

Un conjunto de opciones para las cuales se necesita el consenso.

B.3.4 Proceso

Se interroga a un grupo de expertos utilizando un cuestionario semiestructurado. Los expertos no se reúnen de modo que sus opiniones son independientes.

El procedimiento es el siguiente:

- formación de un equipo que asuma y controle el proceso Delphi;
- selección de un grupo de expertos (puede haber uno o más paneles de expertos);
- desarrollo de la primera ronda del cuestionario;
- someter el cuestionario a prueba;
- enviar el cuestionario a los panelistas individualmente;
- se analiza la información proveniente de la primera ronda de respuestas, se combina y se vuelve a distribuir a los panelistas;

- los panelistas responden y el proceso se repite hasta que se logre el consenso.

B.3.5 Elementos de salida

Convergencia hacia el consenso sobre la material en cuestión.

B.3.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- dado que las opiniones son anónimas, aquellas que no son populares se expresan con mayor probabilidad;
- todas las opiniones tienen igual peso, lo cual evita el problema de personalidades dominantes;
- se logra la propiedad de los resultados;
- no es necesario que las personas se reúnan en un lugar y en un momento determinado.

Las limitaciones son:

- es una actividad intensa y que consume mucho tiempo;
- es necesario que los participantes puedan expresarse con claridad por escrito.

B.4 LISTAS DE VERIFICACIÓN

B.4.1 Información general

Las listas de verificación son listados de peligros, riesgos o fallas en el control que se han desarrollado usualmente a partir de la experiencia, bien sea como resultado de una evaluación previa del riesgo o como resultado de fallas en el pasado.

B.4.2 Uso

Una lista de verificación se puede utilizar para identificar los peligros y los riesgos o para valorar la eficacia de los controles. Se pueden utilizar en cualquier etapa del ciclo de duración de un producto, proceso o un sistema. También se pueden utilizar como parte de otras técnicas para la valoración del riesgo, pero son más útiles cuando se aplican para verificar que todo se haya cubierto después de haber aplicado una técnica más imaginativa que identifique los problemas nuevos.

B.4.3 Elementos de entrada

Información y experticia previas con respecto al tema, de manera tal que se puede seleccionar o desarrollar una lista de verificación pertinente y preferiblemente validada.

B.4.4 Proceso

El procedimiento es el siguiente:

- se define en alcance de la actividad;

- se selecciona una lista de verificación que cubra adecuadamente el alcance. Es necesario seleccionar listas de verificación cuidadosamente para el propósito. Por ejemplo, una lista de verificación de controles normales no se puede utilizar para identificar peligros o riesgos nuevos;

- la persona o el grupo que utiliza la lista de verificación recorre cada elemento del proceso o del sistema y revisa si los elementos de la lista de verificación están presentes.

B.4.5 Elementos de salida

Los elementos de salida dependen de la etapa del proceso de gestión de riesgos en la cual se aplican. Por ejemplo, un elemento de salida 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 son las siguientes:

- pueden ser utilizadas por personas no expertas;

- cuando están bien diseñadas, combinan la experticia amplia en un sistema fácil de usar;

- pueden ayudar a garantizar que no se olviden los problemas comunes.

Las limitaciones son:

- tienden a inhibir la imaginación en la identificación de los riesgos;

- ellas abordan "lo que sabemos que sabemos" en lugar de "lo que sabemos que no sabemos" o "lo que no sabemos que no sabemos";

- estas listas fomentan el comportamiento del tipo "marque la casilla";

- tienden a basarse en la observación, de tal manera que omiten problemas que no se observan con facilidad.

B.5 ANÁLISIS PRELIMINAR DEL PELIGRO (APP)

B.5.1 Información general

Este análisis es un método inductivo sencillo cuyo objetivo es identificar los peligros y las situaciones y eventos peligrosos que pueden causar daño a una actividad o instalación determinadas o un sistema específico.

B.5.2 Uso

Este análisis se realiza más comúnmente en las primeras fases del desarrollo de un proyecto cuando existe poca información sobre detalles del diseño o los procedimientos operativos, y con frecuencia puede ser un precursor para estudios adicionales o para brindar información para la especificación del diseño de un sistema. También puede ser útil cuando se analizan sistemas existentes para priorizar los peligros y los riesgos para un análisis posterior o cuando las circunstancias evitan la utilización de una técnica más extensiva.

UNIVERSIDAD MILITA
NUEVA GRANADA
BIBLIOTECA

B.5.3 Elementos de entrada

Los elementos de entrada incluyen:

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

B.5.4 Proceso

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

- materiales utilizados o producidos y su reactividad;
- equipo empleado;
- ambiente operativo;
- distribución;
- interfaces entre los componentes del sistema, etc.

Se puede llevar a cabo un análisis cualitativo de las consecuencias de un evento no deseado y su probabilidad con el fin de identificar los riesgos y realizar una valoración posterior.

Este análisis se debería actualizar durante las fases de diseño, construcción y ensayo con el fin de detectar todos los peligros nuevos y hacer correcciones, si es necesario. Los resultados que se obtienen se pueden presentar de diversas maneras como por ejemplo en tablas o árboles.

B.5.5 Elementos de salida

Los elementos de salida incluyen:

- una lista de peligros y riesgos;
- recomendaciones en forma de aceptación, controles recomendados, especificación de diseño o solicitudes para una valoración más detallada.

B.5.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- se puede utilizar cuando hay información limitada,
- permite considerar los riesgos en etapas muy tempranas del ciclo de duración del sistema.

Las limitaciones son:

- este análisis brinda únicamente una información preliminar; no es exhaustivo ni proporciona información detallada sobre los riesgos y la manera en que se pueden prevenir.

B.6 ESTUDIOS DE PELIGRO Y OPERATIVIDAD (EPO)

B.6.1 Información general

Este estudio estructurado y sistemático de un producto, proceso, procedimiento o sistema planificado o existente. Es una técnica para identificar los riesgos para las personas, el equipo, el ambiente y/o los objetivos de la organización. También se espera que el equipo de estudio, cuando sea posible, suministre una solución para tratar el riesgo.

Este proceso es una técnica cualitativa que se basa en el uso de palabras guía que cuestionan la manera en que la intención del diseño o las condiciones operativas podrían no lograrse en cada paso del diseño, proceso, procedimiento o sistema. Generalmente es realizado por un equipo multidisciplinario durante varias reuniones.

Este análisis es similar al AMEF en que identifica los modos de falla de un proceso, un sistema o un procedimiento, sus causas y consecuencias. Difiere en que el equipo considera los resultados y las desviaciones no deseadas con respecto a las condiciones y los resultados previstos, y se devuelve a las causas posibles y los modos de falla, mientras que el AMEF empieza identificando los modos de falla.

B.6.2 Uso

La técnica EPO se desarrolló inicialmente para analizar sistemas de procesos químicos, pero se ha extendido a otros tipos de sistemas y operaciones complejas. Éstas incluyen sistemas mecánicos y electrónicos, procedimientos y sistemas de software, e incluso cambios organizacionales, y diseño y revisión de contratos legales.

El proceso EPO puede tratar con todas las formas de desviación con respecto a la intensión del diseño debidas a deficiencias en el diseño, los componentes, los procedimientos planificados y las acciones humanas.

Se utiliza ampliamente para la revisión del diseño de software. Cuando se aplica a sistemas de control de instrumentos críticos de seguridad y sistemas de computación puede ser denominado PCAO (peligros de control y análisis de operatividad o peligros de computación y análisis de operatividad).

Un estudio EPO usualmente se inicia en la etapa de diseño de detalles, cuando se dispone de un diagrama completo del proceso previsto, pero cuando los cambios en el diseño todavía son factibles. Sin embargo, también se puede realizar en un enfoque por fases con diferentes palabras guía para cada etapa, a medida que el diseño se desarrolla en detalle. Este estudio también se puede llevar a cabo durante la operación, pero los cambios necesarios pueden ser costosos en esta fase.

B.6.3 Elementos de entrada

Los elementos de entrada esenciales para un estudio EPO incluyen la información actual acerca del sistema, el proceso o el procedimiento que se revisa, y la intensión y el desempeño de las especificaciones del diseño. Los elementos de entrada pueden incluir: planos, hojas de especificación, diagramas de flujo, diagramas lógicos y de control del proceso, planos de distribución, procedimientos operativos y de mantenimiento, y procedimientos de respuesta ante emergencias. Para estudios EPO no relacionados con el hardware, los elementos de entrada pueden ser cualquier documento que describa las soluciones y los elementos del sistema o el procedimiento que se estudia. Por ejemplo, los elementos de entrada pueden ser

diagramas organizacionales y descripciones de funciones, el borrador de un contrato o incluso el borrador de un procedimiento.

B.6.4 Proceso

Este análisis toma el "diseño" y la especificación de proceso, procedimiento o sistema sometido a estudio y revisa cada una de sus partes para descubrir las desviaciones que se pueden presentar con respecto al desempeño previsto, las causas potenciales y las consecuencias probables de una desviación. Esto se logra examinando sistemáticamente la manera en que cada parte del sistema, proceso o procedimiento responderá a los cambios en los parámetros clave, utilizando palabras guía adecuadas. Las palabras guía se pueden adaptar a un sistema, proceso o procedimiento en particular o se pueden utilizar palabras genéricas que incluyan todos los tipos de desviación. La Tabla B.1 brinda ejemplos de palabras guía utilizadas comúnmente para sistemas técnicos. Palabras guía similares tales como "demasiado temprano", "demasiado tarde", "demasiada cantidad", "demasiado poco", "demasiado largo", "demasiado corto", "dirección equivocada", "objeto equivocado", "acción equivocada" se pueden utilizar para identificar los modos de error humano.

Los pasos normales de un estudio EPO incluyen:

- designación de una persona con la responsabilidad y autoridad necesarias para llevar a cabo el estudio y garantizar que todas las acciones que se originen en el estudio están completas;
- definición de los objetivos y el alcance del estudio,
- establecimiento de un conjunto de claves o palabras guía para el estudio;
- definir el equipo a cargo del estudio; este equipo generalmente es multidisciplinario y debería incluir a personal de diseño y operaciones con la experticia técnica adecuada para evaluar los efectos de las desviaciones con respecto al diseño actual o previsto. Es recomendable que el equipo incluya a personas no directamente involucradas en el diseño o el sistema, el proceso o el procedimiento que se está revisando;
- recolección de la documentación exigida.

Dentro de un taller de facilitación con el equipo de estudio:

- dividir el sistema, el proceso o el procedimiento en elementos más pequeños, subsistemas, subprocesos o subelementos para que la revisión sea tangible;
- acordar la intención del diseño para cada subsistema, subproceso o subelemento y después para cada aspecto de dicho subsistema o elemento aplicando las palabras guía una tras otra para postular desviaciones posibles que tendrán resultados no deseados;
- cuando se identifique un resultado no deseado, acordar la causa y las consecuencias en cada caso y sugerir la forma en que se podrían tratar para evitar que ocurran o para mitigar las consecuencias si ocurren;
- documentar la discusión y pactar sobre las acciones específicas para tratar los riesgos identificados.

Tabla B.1. Ejemplo de las posibles palabras guía para el estudio EPO

Términos	Definiciones
Ninguno o no	No se logra ninguna parte del resultado previsto, o la condición prevista está ausente.
Más (mayor)	Incremento cuantitativo en el elemento de salida o en la condición operativa
Menos (menor)	Reducción cuantitativa
Así como	Incremento cuantitativo (por ejemplo el material adicional)
Parte de	Reducción cuantitativa (por ejemplo únicamente uno o dos componentes en una mezcla)
Inverso /opuesto	Opuesto (por ejemplo el retro flujo)
Diferente	No se logra ninguna parte de la intensión, sino que sucede algo completamente diferente (por ejemplo el flujo o el material equivocado)
Compatibilidad	Material, ambiente
Las palabras guía se aplican a parámetros tales como:	
	Propiedades físicas de un material o proceso
	Condiciones físicas tales como temperatura, velocidad
	La intensión especificada de un componente de un sistema o diseño (por ejemplo la transferencia de información)
	Aspectos operacionales

B.6.5 Elementos de salida

Registro de las actas de las reuniones para el análisis EPO con elementos para cada punto de revisión. Se debería incluir: la palabra guía utilizada, la desviación o desviaciones, las causas posibles, las acciones para tratar los problemas identificados y la persona responsable de la acción.

Para toda desviación que no se pueda corregir, se debería evaluar el riesgo de la desviación.

B.6.6 Fortalezas y limitaciones

Un análisis EPO ofrece las siguientes ventajas:

- suministra los medios para examinar sistemática y exhaustivamente un sistema, proceso o procedimiento;
- involucra a un equipo multidisciplinario e incluye a aquellos con la experiencia operacional de la vida real y aquellos que deban realizar acciones para el tratamiento;
- genera soluciones y acciones para el tratamiento del riesgo;
- se aplica a una amplia variedad de sistemas, procesos y procedimientos;
- permite la consideración explícita de las causas y las consecuencias del error humano;
- crea un registro escrito del proceso que se puede utilizar para demostrar la diligencia adecuada.

Las limitaciones incluyen:

- un análisis detallado puede consumir mucho tiempo y por lo tanto puede ser costoso;

- un análisis detallado exige un alto nivel de documentación o de especificación del sistema, el proceso y el procedimiento;

- se pueden focalizar en el hallazgo de soluciones detalladas en lugar de retar las presunciones fundamentales (sin embargo, esto se puede mitigar mediante un enfoque por fases);

- la discusión se puede centrar en aspectos detallados del diseño y no en aspectos más amplios o externos;

- está restringido por el diseño (borrador) y la intención del diseño, así como por el alcance y los objetivos que se dan al equipo;

- el proceso depende significativamente de la experticia de los diseñadores, a quienes se puede dificultar ser suficientemente objetivos para buscar problemas en sus diseños.

B.6.7 Documento de referencia

IEC 61882, *Hazard and Operability Studies (Studies HAZOP). Application Guide.*

B.7 ANÁLISIS DE PELIGROS Y PUNTOS CRÍTICOS DE CONTROL (APPCC)

B.7.1 Información general

Este análisis proporciona una estructura para identificar los peligros e implementar los controles en todas las partes pertinentes de un proceso para protegerlo contra los peligros y mantener la confiabilidad en la calidad y la seguridad de un producto. Este análisis tiene como objeto garantizar que los riesgos son minimizados por los controles en todo el proceso y no solo a través de la inspección del producto final.

B.7.2 Uso

El análisis APPCC fue desarrollado por el programa espacial de la NASA para garantizar la calidad de los alimentos. Este análisis es utilizado actualmente por las organizaciones que operan en cualquier parte de la cadena alimentaria con el fin de controlar los riesgos debido a contaminantes físicos, químicos o biológicos de los alimentos. Su uso también se ha extendido a la elaboración de productos farmacéuticos y a los dispositivos médicos. El principio de identificar las cosas que pueden influir en la calidad del producto y definir los puntos del proceso en donde se pueden monitorear los parámetros críticos y controlar los peligros, se puede generalizar a otros sistemas técnicos.

B.7.3 Elementos de entrada

Este análisis comienza a partir de un diagrama de flujo básico o de un diagrama del proceso, y de la información sobre los peligros que podrían afectar la calidad, la seguridad o la confiabilidad del producto o del resultado del proceso. La información sobre los peligros y sus riesgos, y las formas en que ellos se pueden controlar es un elemento de entrada para este análisis.

B.7.4 Proceso

Este análisis consiste en los siguientes siete principios:

- identificar los peligros y las medidas preventivas relacionadas con tales peligros;
- determinar los puntos en el proceso en donde se pueden controlar o eliminar los peligros (los puntos críticos de control o PCC);
- establecer los límites críticos necesarios para controlar los peligros, es decir, cada PCC debería operar dentro de parámetros específicos para garantizar el control del peligro;
- monitorear los límites críticos para cada PCC a intervalos definidos;
- establecer las acciones correctivas, si el proceso se encuentra por fuera de los límites establecidos;
- establecer los procedimientos de verificación;
- implementar los procedimientos de conservación de registros y de documentación para cada etapa.

B.7.5 Elementos de salida

Registros documentados que incluyen la hoja de trabajo sobre el análisis del peligro y un **plan** APPCC.

La hoja de trabajo para el análisis del peligro indica para cada etapa del proceso:

- los peligros que se podrían introducir, controlar o exacerbar en esta etapa,
- si los peligros presentan un riesgo significativo (con base en la consideración de la consecuencia y la probabilidad a partir de una combinación de experiencia, datos y literatura técnica);
- una justificación para la importancia;
- las posibles medidas preventivas para cada peligro;
- si las medidas de control y monitoreo se pueden aplicar en esta etapa (es decir, ¿es éste un PCC?).

El plan APPCC delinea los procedimientos que se han de seguir para garantizar el control de un diseño, producto, proceso o procedimiento específico. El plan incluye una lista de todos los PCC, y para cada uno de ellos incluye:

- los límites críticos para las medidas preventivas;
- las actividades de monitoreo y control continuo (incluyendo qué, cómo y cuándo se realizará el monitoreo y quien lo hará);
- las acciones correctivas que se requieren si se detectan desviaciones con respecto a los límites críticos;
- actividades de verificación y conservación de registros.

B.7.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- un proceso estructurado que brinda evidencia documentada para el control de calidad, así como la identificación y reducción de los riesgos;
- un enfoque en la practicidad de cómo y cuándo se pueden prevenir los peligros y controlar los riesgos en un proceso;
- mejor control del riesgo a través de todo el proceso en lugar de depender de la inspección del producto final;
- capacidad para identificar los peligros introducidos por las acciones humanas y la manera en que éstos se pueden controlar en el punto de introducción o posteriormente.

Las limitaciones incluyen:

El análisis APPCC exige, como elementos de entrada para el proceso, que los peligros estén identificados, que los riesgos que ellos representan estén definidos y que su importancia sea entendida. También es necesario definir los controles adecuados. Éstos se exigen con el fin de especificar los puntos críticos de control y los parámetros de control durante el análisis y puede ser necesario combinarlos con otras herramientas para lograrlo;

Cuando se toma acción cuando los parámetros de control exceden los límites definidos se pueden omitir los cambios graduales en los parámetros de control que son estadísticamente significativos y por lo tanto se deberían activar.

B.7.7 Documento de referencia

ISO 22000, *Food Safety Management Systems. Requirements for Any Organization in the Food Chain.*

B.8 VALORACIÓN DE LA TOXICIDAD

B.8.1 Información general

La valoración del riesgo ambiental se usa aquí para cubrir el proceso seguido en la valoración de los riesgos para las plantas, los animales y los humanos como resultado de la exposición a una variedad de peligros ambientales. La gestión del riesgo se refiere a los pasos para la toma de decisiones que incluyen la evaluación del riesgo y el tratamiento del riesgo.

El método implica el análisis del peligro o de la fuente de daño y de la manera en que la población objeto se ve afectada, así como de las vías por la cuales un peligro puede alcanzar a la población objeto susceptible. Esta información se combina posteriormente para obtener la extensión probable y la naturaleza del daño.

B.8.2 Uso

El proceso se utiliza para valorar los riesgos para las plantas, los animales y los humanos como resultado de la exposición a peligros tales como sustancias químicas, microorganismos u otras especies.

Aspectos de la metodología, como el análisis de la trayectoria, de exploran diversas vías por las cuales el objeto puede verse expuesto a una fuente de riesgo, se pueden adaptar y utilizar en un rango muy amplio de diversas áreas de riesgo, aparte de la sanidad y el ambiente humano, y es útil para identificar tratamientos para reducir el riesgo.

B.8.3 Elementos de entrada

El método exige la disponibilidad de datos adecuados sobre la naturaleza y las propiedades de los peligros, la susceptibilidad de la población o las poblaciones objeto y la forma en que estos dos factores interactúan. Normalmente, estos datos se basan en investigación, la cual se puede basar en datos de laboratorio o epidemiológicos.

B.8.4 Proceso

El procedimiento es el siguiente:

a) Formulación del problema: incluye el establecimiento del alcance de la valoración

mediante la definición del rango de las poblaciones objeto y los tipos de peligro de interés.

b) Identificación del peligro: implica la identificación de todos los orígenes posibles de daño para la población objeto que provienen de los peligrosos cubiertos por el alcance del estudio. Normalmente, la identificación del peligro depende del conocimiento experto y de una revisión de la literatura.

c) Análisis del peligro: incluye la comprensión de la naturaleza del peligro y la manera en que éste interactúa con el objeto. Por ejemplo, al considerar la exposición humana a los efectos químicos, el peligro podría incluir la toxicidad aguda y crónica, el potencial de daño para el ADN, el potencial para causar cáncer o defectos de nacimiento. Para cada efecto peligroso, se compara la magnitud del efecto (la respuesta) con la cantidad de peligro al cual se ha visto expuesto el objeto (la dosis) y, siempre que sea posible, se determina el mecanismo mediante el cual se produce el efecto. Se toma nota de los niveles en los cuales no haya ningún efecto observable (NEO) ni efecto adverso observable (NEAO). Estos aspectos algunas veces se utilizan como criterio para la aceptabilidad del riesgo.

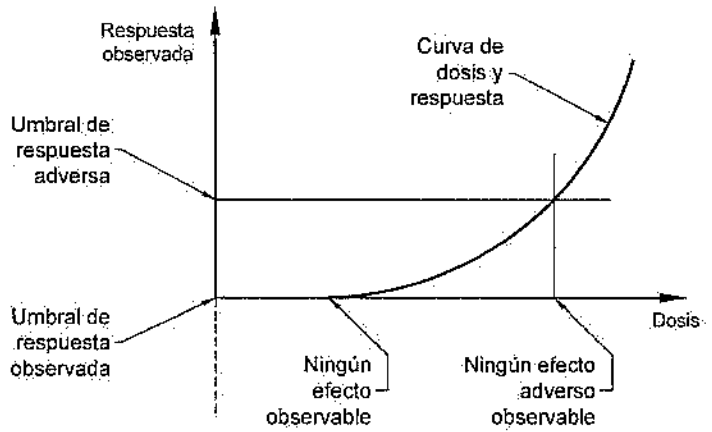


Figura B.1. Curva de dosis-respuesta

Para la exposición química, los resultados de la prueba se utilizan para derivar curvas de dosis y respuesta como aquella que se ilustra de forma esquemática en la Figura B.1. Estas curvas usualmente se derivan de pruebas en animales o de sistemas experimentales tales como las células o los tejidos de cultivo.

Los efectos de otros peligros tales como los microorganismos o las especies introducidas se pueden determinar a partir de datos de campo y de estudios epidemiológicos. Se determina la naturaleza de la interacción de las enfermedades o las plagas con el objeto y se estima la probabilidad de un nivel particular de daño debido a la exposición particular al peligro.

d) Análisis de la exposición: en este paso se examina la manera en la cual una sustancia peligrosa o sus residuos podrían llegar hasta la población objeto susceptible y en qué cantidad. Con frecuencia, esto implica un análisis de trayectoria que considere las diferentes vías que podría tomar el peligro, las barreras que podrían prevenir que éste llegue hasta el objeto, y los factores que podrían influir en el nivel de exposición. Por ejemplo, al considerar el riesgo derivado de una aspersión química el análisis de la exposición consideraría la cantidad de sustancia química que se dispersó, en qué forma y en qué condiciones lo hizo, si existió alguna exposición directa de los humanos o los animales, qué cantidad podría quedar como residuo en las plantas, el destino ambiental de los plaguicidas que llegan al suelo, si se pueden acumular en los animales o si llegan al agua subterránea. En bioseguridad, el análisis de trayectoria podría considerar la manera en que las plagas llegan al país, se integran en el ambiente, se establece y se dispersan.

e) Caracterización del riesgo: en este paso, se reúne la información proveniente del análisis del peligro y del análisis de la exposición para estimar las probabilidades de las consecuencias particulares, cuando se combinan los efectos de todas las trayectorias. Cuando hay una gran cantidad de peligros o de trayectorias, se puede llevar a cabo una clasificación inicial y realizar un análisis detallado del peligro y la exposición, así como la caracterización del riesgo en los escenarios de riesgo más alto.

B.8.5 Elementos de salida

El elemento de salida normalmente es una indicación del nivel del riesgo debido a la exposición de un objeto particular a un peligro particular en el contexto en cuestión. El riesgo se puede expresar cuantitativamente, semicuantitativamente o cualitativamente. Por ejemplo, el riesgo de cáncer a menudo se expresa cuantitativamente como la probabilidad de que una persona desarrolle cáncer en un periodo específico dada una exposición específica a un contaminante. El análisis semicuantitativo se puede utilizar para derivar un índice de riesgo para un contaminante o una plaga particular y el resultado cualitativo puede ser un nivel de riesgo (por ejemplo alto, medio, bajo) o una descripción con datos prácticos de los efectos probables.

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 incrementan el riesgo.

El análisis de trayectoria generalmente 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 unos nuevos.

Sin embargo, necesita tener datos adecuados que con frecuencia no están disponibles o tienen un nivel alto de incertidumbre asociada. Por ejemplo, las curvas de dosis y respuesta derivadas

de animales expuestos a niveles altos de un peligro se deberían extrapolar para estimar los efectos de niveles muy bajos del contaminante para los humanos y existen muchos modelos mediante los cuales se puede lograrlo. Cuando el objeto es el ambiente y no los humanos, y el peligro no es químico, los datos que son directamente pertinentes para las condiciones particulares del estudio pueden ser limitados.

B.9 TÉCNICA ESTRUCTURADA "¿QUÉ PASARÍA SI?" (EQPS)

B.9.1 Información general

Esta técnica se desarrolló originalmente como una alternativa más sencilla para el análisis EPO. La técnica es un estudio sistemático, basado en el trabajo de equipo, que utiliza un conjunto de palabras o frases de "indicación" que el facilitador utiliza durante un taller para estimular a los participantes a que identifiquen los riesgos. El facilitador y el equipo utilizan frases normales del tipo "qué pasaría si" en combinación con las indicaciones para investigar cómo un sistema, un elemento de la planta, la organización o el procedimiento se verán afectados por las desviaciones con respecto al comportamiento de las operaciones normales. Esta técnica normalmente se aplica más a nivel del sistema con un nivel más bajo de detalle que el EPO.

B.9.2 Uso

Aunque esta técnica se diseñó originalmente para el estudio de peligros en plantas químicas y petroquímicas, en la actualidad se aplica ampliamente a sistemas, elementos de la planta, procedimientos y organizaciones en general. En particular, se utiliza para examinar las consecuencias de los cambios y los riesgos así alterados o creados.

B.9.3 Elementos de entrada

El sistema, el procedimiento, el elemento de la planta y/o el cambio se deben definir cuidadosamente antes de que el estudio pueda empezar. Tanto el contexto externo como el interno se establecen a través de entrevistas y mediante el estudio de documentos, planes y planos por parte del facilitador. Normalmente, el elemento, la situación o el sistema para el estudio se dividen en nodos o elementos clave para facilitar el proceso de análisis, pero esto generalmente no ocurre con el nivel de definición que se exige para el análisis EPO.

Otro elemento de entrada importante es la experticia y la experiencia presentes en el equipo de estudio, el cual se debe seleccionar cuidadosamente. Todas las partes involucradas deberían estar representadas, si es posible, junto con aquellos con la experiencia en elementos, sistemas, cambios o situaciones similares.

B.9.4 Proceso

El proceso general es el siguiente:

a) Antes de empezar el estudio, el facilitador elabora un listado de indicaciones convenientes con palabras o frases que se pueden basar en un conjunto normal o se pueden crear para permitir una revisión exhaustiva de los peligros o los riesgos.

b) En el taller se discuten y se alcanzan acuerdos sobre el contexto interno y externo del elemento, el sistema, el cambio o la situación, y también el alcance del estudio.

c) El facilitador pide a los participantes que planteen y discutan:

- los riesgos y peligros conocidos;
- la experiencia y los incidentes previos;
- los controles y las salvaguardas conocidas y existentes;
- los requisitos reglamentarios y las restricciones.

d) La discusión se ve facilitada por la creación de una pregunta utilizando una frase "qué pasaría si" y una palabra o un tema de indicación. Las frases "qué pasaría si" que se pueden usar son "¿que si...?", "¿qué sucedería si...?" "¿podría alguien o algo...?", "¿alguna vez algo o alguien...?". La intención es estimular al equipo de estudio para que explore escenarios potenciales, sus causas, consecuencias e impactos.

e) Los riesgos se resumen y el equipo toma en consideración los controles existentes.

f) La descripción del riesgo, sus causas, consecuencias y los controles esperados se confirman con el equipo y se registran.

g) El equipo considera si los controles son adecuados y eficaces y llega a un acuerdo sobre una declaración de la eficacia del control del riesgo. Si ésta es menos que satisfactoria, el equipo considera adicionalmente las tareas para el tratamiento del riesgo y define los controles potenciales.

h) Durante la discusión, se plantean preguntas "¿qué pasaría si...?" adicionales para identificar los riesgos adicionales.

i) El facilitador utiliza la lista de indicaciones para monitorear la discusión y sugerir aspectos y escenarios adicionales para que el equipo los discuta.

j) Es normal utilizar un método de valoración del riesgo cualitativo o semicuantitativo para calificar las acciones creadas en términos de prioridad. Normalmente, esta valoración del riesgo se realiza tomando en consideración los controles existentes y su eficacia.

B.9.5 Elementos de salida

Los elementos de salida incluyen un registro del riesgo con las acciones o las tareas calificadas según el riesgo. Estas tareas posteriormente se pueden convertir en la base para un plan de tratamiento.

B.9.6 Fortalezas y limitaciones

Las fortalezas de esta técnica son:

- tiene aplicación amplia para todas las formas de plantas o sistemas físicos, situaciones o circunstancias, organizaciones o actividades;
- necesita mínima preparación del equipo;
- es relativamente rápida y los peligros y riesgos mayores se hacen aparentes rápidamente en la sesión del taller;

- el estudio está "orientado a los sistemas" y permite a los participantes revisar la respuesta del sistema a las desviaciones en lugar de sólo examinar las consecuencias de la falla del componente;

- se puede utilizar para identificar las oportunidades de mejora de los procesos y los sistemas y, generalmente, se puede usar para identificar las acciones que originan o mejoran las probabilidades de éxito;

- la participación en el taller de aquellos responsables de rendir cuentas acerca de los controles existentes y de las acciones posteriores para el tratamiento del riesgo refuerza su responsabilidad;

- crear un registro del riesgo y un plan de tratamiento del riesgo con poco esfuerzo de más;

- aunque con frecuencia se utiliza una forma de clasificación del riesgo cualitativa o semicuantitativa para la valoración del riesgo y para priorizar la atención en las secciones resultantes, la técnica EQPS se puede utilizar para identificar riesgos y peligros que se pueden considerar en un estudio cuantitativo más adelante.

Las limitaciones son:

- para ser eficiente, se necesita un facilitador experimentado y capaz;

- se necesita de preparación cuidadosa de tal manera que no se desperdicie el tiempo del equipo durante el taller;

- si el equipo del taller no tiene una base amplia y suficiente de experiencia o si el sistema de indicaciones no es exhaustivo, es posible que no se identifiquen algunos riesgos o peligros;

- la aplicación de alto nivel de la técnica puede no revelar causas complejas, detalladas o correlacionadas.

B.10 ANÁLISIS DE ESCENARIO

B.10.1 Información general

Análisis de escenario es un nombre que se da al desarrollo de modelos descriptivos de la forma en que el futuro se podría presentar. Se puede utilizar para identificar riesgos considerando los avances futuros posibles y explorando sus implicaciones. Se pueden utilizar conjuntos de escenarios que reflejen (por ejemplo) "el mejor caso", "el peor caso" y "el caso esperado" para analizar las consecuencias potenciales y su probabilidad para cada escenario, como una forma de análisis de sensibilidad cuando se analiza el riesgo.

El poder del análisis del escenario se ilustra al considerar los cambios mayores que han sucedido en los últimos 50 años en la tecnología, las preferencias del consumidor, las actitudes sociales, etc. El análisis del escenario no puede predecir las probabilidades de tales cambios pero si puede considerar las consecuencias y ayudar a las organizaciones a desarrollar las fortalezas y la flexibilidad necesarias para adaptarse a los cambios previsibles.

B.10.2 Uso

Este análisis se puede utilizar para facilitar la toma de decisiones sobre las políticas y planificar estrategias futuras, así como para considerar las actividades existentes. Puede tener un rol en los tres componentes de la valoración del riesgo. Para la identificación y el análisis, se pueden utilizar grupos de escenarios que reflejen (por ejemplo) "el mejor caso", "el peor caso" y "el caso esperado" para identificar lo que podría suceder en circunstancias particulares y analizar las consecuencias potenciales y las probabilidades para cada escenario.

El análisis del escenario se puede utilizar para anticipar el modo en que tanto las amenazas como las oportunidades se podrían desarrollar y también se puede usar para todo tipo de riesgo con marcos temporales a corto y largo plazo. Con marcos temporales a corto plazo y datos adecuados, los escenarios probables se pueden extrapolar desde el presente. Para marcos temporales a largo plazo o con datos inadecuados, el análisis del escenario se hace más imaginativo y se podría decir que se trata de análisis de futuros.

El análisis del escenario puede ser útil cuando existen diferencias de distribución significativas entre los resultados positivos y los resultados negativos en el espacio, el tiempo y los grupos en la comunidad o la organización.

B.10.3 Elementos de entrada

El prerrequisito para un análisis del escenario es un equipo de personas que entre ellos tengan una comprensión de la naturaleza de los cambios pertinentes (por ejemplo los posibles avances en la tecnología) e imaginación para pensar el futuro sin extrapolar necesariamente desde el pasado. También es útil el acceso a la literatura y a los datos acerca de los cambios que ya han ocurrido.

B.10.4 Proceso

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

Habiendo establecido un equipo y los canales de comunicación pertinentes, y después de definir el contexto del problema y los aspectos que se van a considerar, el siguiente paso es identificar la naturaleza de los cambios que podrían ocurrir. Paras ello será necesario investigar las tendencias principales y la sincronización probable de los cambios en las tendencias, así como un pensamiento imaginativo acerca del futuro.

Los cambios que se van a considerar pueden incluir:

- cambios externos (por ejemplo los cambios tecnológicos);
- decisiones que es necesario tomar en el futuro cercano pero que pueden tener una variedad de resultados;
- las necesidades de las partes involucradas y la manera en que ellas podrían cambiar;
- cambios en el ambiente macro (reglamentos, demografía, etc.). Algunos serán inevitables y algunos serán inciertos.

En ocasiones, un cambio se puede deber a las consecuencias de otro riesgo. Por ejemplo, el riesgo del cambio climático es el resultado de los cambios en las demandas del consumidor con respecto a las grandes cantidades de alimentos. Esto tendrá influencia en los alimentos que se podrán exportar con beneficios, así como aquellos que se pueden cultivar localmente.

Los factores locales y macro o las tendencias se pueden enumerar y calificar ahora según (1) importancia e (2) incertidumbre. Se presta atención especial a los factores que son más importantes y más inciertos. Los factores o las tendencias clave se correlacionan entre sí para mostrar las áreas en donde se pueden desarrollar los escenarios.

Se propone una serie de escenarios enfocados cada uno en un cambio plausible en los parámetros.

Después, se escriben una "historia" para cada escenario que cuenta cómo podría usted pasar desde aquí hacia aquel escenario sujeto al análisis. Las historias pueden incluir detalles plausibles que añaden valor a los escenarios.

Los escenarios se pueden usar entonces para probar y evaluar el interrogante original. En la prueba se toman en consideración todos los factores significativos pero predecibles (por ejemplo los patrones de uso), y luego explora qué tan "exitosa" sería la política (actividad) en este nuevo escenario, y los resultados "previos a las pruebas" utilizando preguntas "¿qué pasaría si...?" basadas en presunciones modelo.

Cuando se ha evaluado una pregunta o una propuesta con respecto a cada escenario, puede ser obvio que se necesita modificación para hacer la más robusta o menos riesgosa. También debería ser posible identificar algunos indicadores guía que muestren el momento en que ocurre el cambio. El monitoreo y la respuesta ante los indicadores guía puede brindar la oportunidad para el cambio en las estrategias planificadas.

Dado que los escenarios son únicamente "tajadas" definidas de futuros posibles, es importante asegurarse de tener en cuenta la probabilidad de que ocurra un resultado (escenario) particular, es decir, adoptar un marco de referencia del riesgo. Por ejemplo, cuando se utilizan escenarios para el mejor caso, el peor caso y el caso esperado se debería intentar cualificar o expresar la probabilidad de que ocurra cada escenario.

B.10.5 Elementos de salida

Es posible que no exista un escenario que se adapte mejor, pero uno de ellos debería dar como resultado una percepción más clara del rango de opciones y del modo de modificar el curso seleccionado de las acciones a medida que se mueven los indicadores.

B.10.6 Fortalezas y limitaciones

El análisis del escenario toma en consideración un rango de futuros posibles, lo cual puede ser preferible al enfoque tradicional de confiar en previsiones altas, medias, bajas que asumen, a través del uso de datos históricos, que los eventos futuros probablemente seguirán las tendencias del pasado. Esto es importante para situaciones en las que existe poco conocimiento vigente sobre el cual basar las predicciones o cuando se consideran riesgos en el futuro a largo plazo.

Sin embargo, esta fortaleza tiene una debilidad asociada, y es que cuando existe incertidumbre alta algunos de los escenarios pueden no ser realistas.

Las principales dificultades al utilizar el análisis del escenario están asociadas con la disponibilidad de datos y la capacidad de los analistas y de quienes toman las decisiones para desarrollar escenarios realistas susceptibles a la prueba de los resultados posibles.

Los peligros de utilizar el análisis del escenario como herramienta para la toma de decisiones son que los escenarios utilizados pueden no tener una fundamentación adecuada; que los datos sean especulativos y que los resultados no realistas no se puedan reconocer como tales.

B.11 ANÁLISIS DEL IMPACTO EN EL NEGOCIO

B.11.1 Información general

El análisis del impacto en el negocio, también conocido como valoración del impacto en el negocio, analiza la manera en que los riesgos clave de alteración podrían afectar las operaciones de una organización e identifica y cuantifica las capacidades que serían necesarias para su gestión. Específicamente, este análisis brinda una comprensión pactada sobre:

- la identificación y criticidad de los procesos clave del negocio, las funciones y los recursos asociados, y las interdependencias importantes que existen para la organización;
- la manera en que los eventos perturbadores afectarán la capacidad y la habilidad para lograr los objetivos críticos para el negocio;
- la capacidad y habilidad necesarias para la gestión del impacto de una alteración y la recuperación de la organización hasta niveles de operación pactados.

B.11.2 Uso

Este análisis se utiliza para determinar la criticidad y los marcos temporales de recuperación de los procesos y los recursos asociados (personas, equipo, tecnología de la información) para garantizar el logro continuo de los objetivos. Además, el análisis facilita la determinación de las interdependencias y las interrelaciones entre procesos, partes internas y externas, y los enlaces de la cadena de suministro.

B.11.3 Elementos de entrada

Los elementos de entrada incluyen:

- un equipo que emprenda el análisis y desarrolle un plan;
- información relacionada con los objetivos, el ambiente, las operaciones y las interdependencias de la organización;
- detalles sobre las actividades y las operaciones de la organización, incluyendo procesos, recursos de soporte, relaciones con otras organizaciones, disposiciones subcontratadas, partes involucradas;
- consecuencias financieras y operacionales de la pérdida de los procesos críticos;
- cuestionario preparado;
- lista de los entrevistados de las áreas pertinentes de la organización y/o de las partes involucradas que serán contactadas.

B.11.4 Proceso

Este análisis se puede emprender utilizando cuestionarios, entrevistas, talleres estructurad combinaciones de estos tres, con el fin de comprender los procesos críticos, los efectos c pérdida de tales procesos y los marcos temporales de recuperación que se requieren así c los recursos de soporte.

Los pasos clave incluyen:

- con base en la valoración del riesgo y la vulnerabilidad, confirmación de los proc clave y los elementos de salida de la organización para determinar la criticidad de procesos;
- determinación de las consecuencias de una alteración en los procesos crí identificados en términos financieros y/u operacionales durante períodos definidos;
- identificación de las interdependencias con las partes involucradas clave tanto inte como externas. Esto podría incluir la asociación de la naturaleza de interdependencias en toda la cadena de suministro;
- determinación de los recursos vigentes disponibles y el nivel esencial de los recu necesarios para continuar operando en un nivel mínimo aceptable después d alteración;
- identificación de procesos y soluciones alternas actualmente en uso o cuyo desar ha sido planificado. Puede ser necesario desarrollar procesos y soluciones alte cuando los recursos o las habilidades son inaccesibles o insuficientes durant alteración;
- determinación del tiempo máximo aceptable fuera de servicio para cada proceso base en las consecuencias identificadas y los factores críticos de éxito para tal func Este tiempo máximo representa el periodo máximo de tiempo durante el cua organización puede tolerar la pérdida de capacidad;
- determinación del objetivo o los objetivos del tiempo de recuperación para cualc equipo especializado o para la tecnología de la información. Este dato represent tiempo durante el cual la organización se propone recuperar el equipo especializado capacidad de la tecnología de la información;
- confirmación del nivel actual de preparación de los procesos críticos para gestionar alteración. Se puede incluir la evaluación del nivel de redundancia dentro del proc (por ejemplo el equipo de repuesto) o la existencia de otros proveedores.

B.11.5 Elementos de salida

Los elementos de salida son los siguientes:

- una lista de prioridades de los procesos críticos y las interdependencias asociadas;
- impactos financieros y operacionales documentados debido a la pérdida de procesos críticos;
- recursos de soporte necesarios para los procesos críticos identificados;

- marcos temporales fuera de servicio para el proceso crítico y los marcos temporales asociados de recuperación de la tecnología de la información.

B.11.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- la comprensión de los procesos críticos, la cual brinda a la organización la habilidad para continuar logrando sus objetivos establecidos;
- la comprensión de los recursos que se requieren;
- la oportunidad de redefinir los procesos operacionales de una organización para facilitar la versatilidad de la organización.

Las limitaciones incluyen:

- la falta de conocimiento por parte de los participantes involucrados en diligenciar los cuestionarios, realizar las entrevistas o los talleres;
- la dinámica de grupo puede afectar al análisis completo de un proceso crítico;
- las expectativas simples o demasiado optimistas de los requisitos de recuperación;
- dificultad para lograr un nivel adecuado de comprensión de las operaciones y las actividades de la organización.

B.12 ANÁLISIS DE CAUSA PRINCIPAL (ACP)

B.12.1 Información general

El análisis de una pérdida mayor para evitar que se vuelva a presentar comúnmente se denomina análisis de causa principal, análisis de falla de causa principal o análisis de pérdida. El análisis ACP se enfoca en valorar las pérdidas debidas a diversos tipos de fallas mientras que el análisis de las pérdidas se relaciona principalmente con las pérdidas financieras o económicas debidas a factores externos o a catástrofes. En este análisis de intenta identificar las causas originales o principales en lugar de tratar únicamente con los síntomas inmediatos obvios. Se reconoce que la acción correctiva no siempre puede ser totalmente eficaz y que puede ser necesaria la mejora continua. Este análisis se aplica con más frecuencia a la evaluación de la pérdida mayor, pero también se puede utilizar para analizar pérdidas en una base más global para determinar en donde realizar mejoras.

B.12.2 Uso

Este análisis se aplica a diversos contextos con las siguientes áreas amplias de utilización:

- el ACP con base en la seguridad se utiliza para investigaciones de accidentes y en salud y seguridad ocupacional;
- el análisis de falla se utiliza en sistemas tecnológicos relacionados con la confiabilidad y el mantenimiento;

- el ACP con base en la producción se aplica en el campo del control de calidad para la fabricación industrial;
- el ACP con base en el proceso se focaliza en los procesos del negocio;
- el análisis ACP con base en el sistema se ha desarrollado como una combinación de las áreas anteriores para tratar los sistemas complejos con aplicación en la gestión de cambio, la gestión de riesgos y el análisis de los sistemas.

B.12.3 Elementos de entrada

El elemento de entrada básico para este tipo de análisis es toda la evidencia reunida a partir d una falla o una pérdida. Los datos de otras fallas similares también se pueden considerar en e análisis. Otros elementos de entrada pueden ser los resultados de la prueba de hipótesi específicas.

B.12.4 Proceso

Cuando se identifica la necesidad de un ACP, se asigna un grupo de expertos para que lleve a cabo el análisis y formulen recomendaciones. El tipo de experto dependerá principalmente d la experticia específica necesaria para analizar la falla.

Aunque se pueden utilizar métodos diferentes para realizar el análisis, los pasos básicos pa ejecutarlo son similares e incluyen:

- formación del equipo;
- establecer el alcance y los objetivos del ACP;
- recolección de los datos y la evidencia provenientes de la falla o la pérdida;
- realizar un análisis estructurado para determinar la causa principal;
- desarrollar soluciones y plantear recomendaciones;
- implementar las recomendaciones;
- verificar el éxito de las recomendaciones implementadas.

Las técnicas de análisis estructurado pueden ser las siguientes:

- técnica de los "cinco porqués", es decir, preguntar repetidamente "¿por qué?" pa descartar capas de causas y subcausas;
- análisis de modo y efecto de falla;
- análisis de árbol de fallas;
- diagramas de Ishikawa o en espina de pescado;
- análisis de Pareto;
- mapeo de la causa principal.

La evaluación de las causas a menudo avanza desde las causas físicas evidentes inicialmente hasta las causas relacionadas con el humano y finalmente las causas fundamentales subyacentes o de gestión. Los factores causales deben poder ser controlados o eliminados por las partes involucradas para que la acción correctiva sea eficaz y tenga mérito.

B.12.5 Elementos de salida

Los elementos de salida del ACP incluyen:

- documentación de los datos y la evidencia recolectados;
- hipótesis consideradas;
- conclusión sobre la causa principal más probable de la falla o la pérdida;
- recomendaciones para la acción correctiva.

B.12.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- participación de los expertos correspondientes que trabajan en un ambiente de equipo;
- análisis estructurado;
- consideración de todas las hipótesis probables;
- documentación de los resultados;
- necesidad de producir recomendaciones finales.

Las limitaciones son:

- los expertos que se requieren pueden no estar disponibles;
- la evidencia crítica puede ser destruida en la falla o eliminada durante la limpieza;
- puede que al el equipo no se le permita el tiempo ni los recursos suficientes para evaluar completamente la situación;
- puede que no sea posible implementar adecuadamente las recomendaciones.

B.13 ANÁLISIS DE MODOS Y EFECTOS DE FALLAS (AMEF) Y ANÁLISIS DE MODOS Y EFECTOS DE FALLA Y CRITICIDAD (AMEFC)

B.13.1 Información general

El análisis AMEF es una técnica utilizada para identificar los modos en los cuales los componentes, los sistemas o los procesos pueden fallar en cumplir la intención de su diseño.

Este análisis identifica:

- todos los modos de falla potenciales de las diversas partes de un sistema (un modo de falla es aquello que se observa fallando o que se ejecuta incorrectamente);
- los efectos que estas fallas pueden tener en el sistema;
- el mecanismo de la falla;
- cómo evitar las fallas y/o mitigar los efectos de las fallas en el sistema.

El análisis AMEFC es una extensión del análisis AMEF de modo tal que el modo de falla identificado se califica de acuerdo con su importancia o criticidad.

Este análisis de criticidad usualmente es cualitativo o semicuantitativo pero se puede cuantificar utilizando índices reales de falla.

B.13.2 Uso

Existen varias aplicaciones para el análisis AMEF: AMEF del diseño (o producto) que se utiliza para los componentes y los productos, AMEF del sistema que se utiliza para sistemas, AMEF del proceso que se utiliza para procesos de fabricación y ensamble, AMEF del servicio y AMEF del software.

Estos análisis AMEF - AMEFC se pueden aplicar durante el diseño, la fabricación o el funcionamiento de un sistema físico.

Para mejorar la fiabilidad, sin embargo, los cambios generalmente se implementan con mayor facilidad en la etapa de diseño. Estos dos análisis también se pueden aplicar a procesos y procedimientos. Por ejemplo, se utilizan para identificar el potencial de errores médicos en los sistemas del cuidado de la salud y las fallas en los procedimientos de mantenimiento.

Estos análisis se pueden utilizar para:

- facilitar la selección de alternativas de diseño con alta fiabilidad,
- garantizar que se han tenido en cuenta todos los modos de falla de los sistemas y los procesos así como sus efectos en el éxito operacional,
- identificar los modos y los efectos del error humano,
- proporcionar una base para planificar los ensayos y el mantenimiento de los sistemas físicos,
- mejorar el diseño de procedimientos y procesos,
- brindar información cualitativa o cuantitativa para técnicas de análisis tales como análisis de árbol de fallas.

Estos análisis pueden brindar elementos de entrada para otras técnicas de análisis como ejemplo el análisis de árbol de fallas, bien sea a nivel cualitativo o cuantitativo.

B.13.3 Elementos de entrada

Los análisis AMEF y AMEFC necesitan información acerca de los elementos del sistema co detalles suficientes para realizar un análisis indicativo de los modos en los cuales puede falla

cada elemento. Para un AMEF detallado del diseño, el elemento puede estar en el nivel detallado de componente individual, mientras que para el AMEF de sistemas de nivel más alto, los elementos pueden definirse en nivel superior.

La información puede incluir:

- planos o un diagrama de flujo del sistema que se está analizando y sus componentes, o los pasos de un proceso;
- comprensión de la función de cada paso de un proceso o componente de un sistema;
- detalles de los parámetros ambientales y de otros que pueden tener efecto en la operación;
- comprensión de los resultados de las fallas particulares;
- información histórica sobre las fallas que incluya datos sobre el índice de falla, siempre que sea posible.

B.13.4 Proceso

El proceso AMEF es el siguiente:

a) definir el alcance y los objetivos del estudio;

b) reunir al equipo;

c) entender el sistema/proceso que se va a someter al análisis AMEFC;

d) dividir el sistema en sus componentes o en sus pasos;

e) definir la función de cada paso o cada componente;

f) para cada componente o paso indicado identificar:

- ¿de qué manera posible puede fallar cada parte?
- ¿qué mecanismos podrían producir estos modos de falla?
- ¿cuáles podrían ser los efectos si se produjeran las fallas?
- ¿es la falla inofensiva o dañina?
- ¿cómo se detecta la falla?

g) identificar las disposiciones inherentes en el diseño para compensar la falla.

Para el análisis AMEFC, el equipo de estudio clasifica cada uno de los modos de falla identificados de acuerdos con su criticidad.

Hay varias formas de lograrlo. Los métodos comunes incluyen:

- el índice de criticidad del modo,

- el nivel de riesgo,
- el número de la prioridad del riesgo.

La criticidad del modelo es una medición de la probabilidad de que el modo que se está estudiando produzca una falla del sistema en su totalidad; se define como:

Probabilidad del efecto de falla * índice del modo de falla * tiempo de operación del sistema

Este análisis se aplica con más frecuencia a las fallas del equipo en las cuales cada uno de estos términos se puede definir cuantitativamente y todos los modos de falla tienen la misma consecuencia.

El nivel de riesgo se obtiene al combinar las consecuencias del modo de falla que ocurre con la probabilidad de falla. Se utiliza cuando las consecuencias de diversos modos de falla son diferentes y se puede aplicar a sistemas de equipos o procesos. El nivel de riesgo se puede expresar cualitativamente, semicuantitativamente o cuantitativamente.

El número de la prioridad del riesgo es una medición semicuantitativa de la criticidad que se obtiene multiplicando los números de las escalas de calificación (usualmente entre 1 y 10) para la consecuencia de la falla, la posibilidad de la falla y la habilidad para detectar el problema. (A una falla se le asigna una prioridad mayor si ésta es difícil de detectar). Este método se utiliza con más frecuencia en las aplicaciones de aseguramiento de la calidad.

Una vez que se han identificado los mecanismos y los modos de falla, se pueden definir e implementar las acciones correctivas para los modos de falla más significativos.

El AMEF se documenta en un informe que contenga:

- los detalles del sistema que se sometió al análisis;
- la forma en que se realizó el ejercicio;
- las presunciones hechas en el análisis;
- las fuentes de datos;
- los resultados que incluyan las hojas de trabajo diligenciadas,
- la criticidad (si se realizó en su totalidad) y la metodología utilizada para definirla;
- todas las recomendaciones de análisis adicional, cambios en el diseño o características que se deben incorporar en los planes de ensayo, etc.

El sistema se puede volver a valorar mediante otro ciclo de AMEF después de que se completen las acciones.

B.13.5 Elementos de salida

El elemento de salida principal del AMEF es una lista de los modos de falla, los mecanismos de falla y los efectos en cada componente de un sistema o cada paso de un proceso (que puede incluir información sobre la posibilidad de que se presente la falla). También se suministra información sobre las causas de la falla y las consecuencias para el sistema en su totalidad. El elemento de salida del AMEFC incluye una calificación de la importancia con base en la

posibilidad de que el sistema presente fallas, el nivel de riesgo resultante del modo de falla o una combinación del nivel de riesgo y la "capacidad de detectar" el modo de falla.

El análisis AMEFC puede suministrar un elemento de salida cuantitativo si se utilizan datos adecuados del índice de falla y consecuencias cuantitativas.

B.13.6 Fortalezas y limitaciones

Las fortalezas de estos análisis son:

- se aplican ampliamente a modos de falla humana, del equipo y del sistema y al hardware, el software y los procedimientos;
- identifican los modos de falla del componente, sus causas y sus efectos en el sistema, y los presentan en un formato de lectura fácil;
- evitan la necesidad de modificaciones costosas al equipo en servicio al identificar los problemas tempranamente en el proceso de diseño;
- identifican modos de falla de punto único y los requisitos para los sistemas de redundancia o seguridad;
- brindan elementos de entrada para los programas de monitoreo del desarrollo al enfatizar los aspectos clave que se deben monitorear.

Las limitaciones incluyen:

- se pueden utilizar únicamente para identificar modos únicos de falla, no para combinaciones de modos de falla;
- a menos que se controlen y se enfoquen adecuadamente, los estudios pueden consumir mucho tiempo y ser costosos;
- estos análisis pueden ser difíciles y tediosos para sistemas complejos de capas múltiples.

B.13.7 Documento de referencia

IEC 60812, *Analysis Techniques for System Reliability. Procedures for Failure Mode and Effect Analysis (FMEA).*

B.14 Análisis de árbol de fallas (AAF)

B.14.1 Información general

Este análisis es una técnica para identificar y analizar los factores que contribuyen a un evento no deseado específico (denominado el "evento máximo"). Los factores causales se identifican de manera deductiva, se organizan de modo lógico y se representan pictóricamente en un diagrama de árbol que ilustra los factores causales y su relación lógica con el evento máximo.

Los factores identificados en el árbol pueden ser eventos que están asociados a fallas de los componentes del hardware, errores humanos u otros eventos pertinentes que ocasionan el evento no deseado.

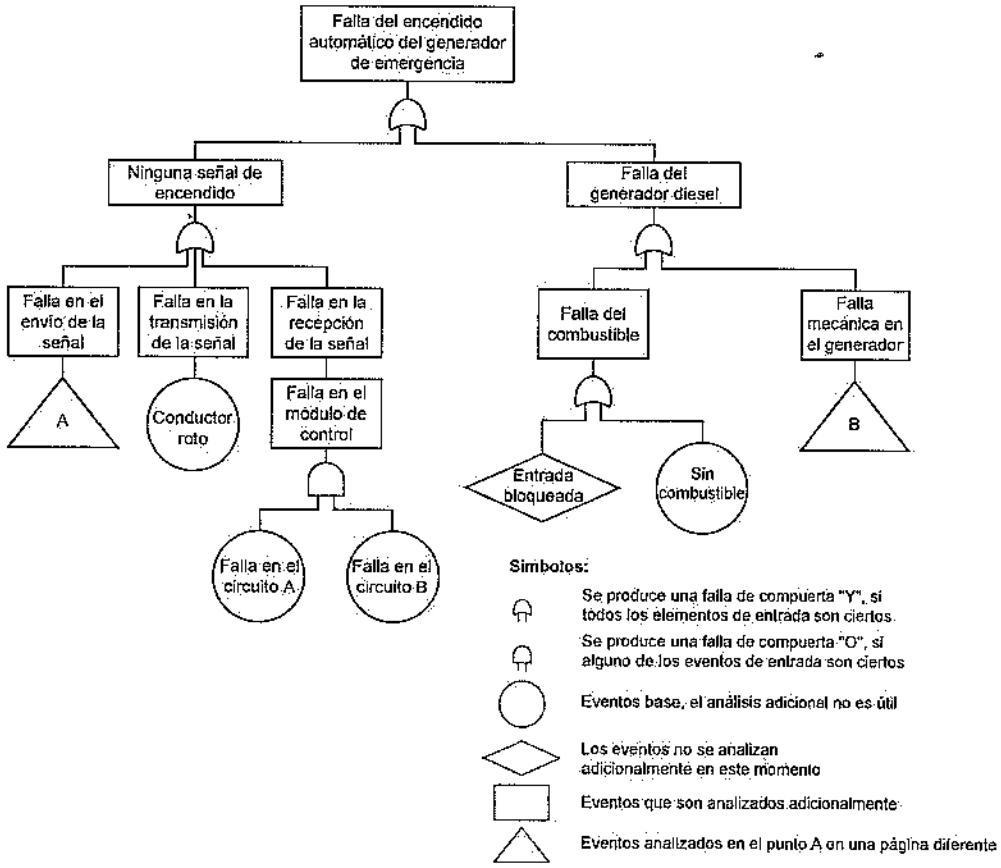


Figura B.2. Ejemplos de un análisis de árbol de fallas tomado de IEC 60300-3-9

B.14.2 Uso

El árbol de fallas se puede utilizar cualitativamente para verificar las causas potenciales y las trayectorias para una falla (el evento máximo) o cuantitativamente para calcular la probabilidad del evento máximo, dado el conocimiento de las probabilidades de los eventos causales.

Se puede utilizar en la etapa de diseño de un sistema para identificar las causas potenciales de falla y por tanto seleccionar entre diversas opciones de diseño. Se puede utilizar en la fase de operativa para identificar la manera en que las fallas mayores se pueden presentar y la importancia relativa de diferentes trayectorias para el evento principal. Un árbol de fallas también se puede utilizar para analizar una falla que ha ocurrido con el fin de presentar en un diagrama la manera en que los diversos eventos se unen para causar la falla.

B.14.3 Elementos de entrada

Para el análisis cualitativo, se requiere de la comprensión del sistema y de las causas de las fallas, así como del entendimiento técnico de la manera en que puede fallar el sistema. Los diagramas detallados son útiles para facilitar el análisis.

Para el análisis cuantitativo, se requieren los datos de los índices de falla o la probabilidad de encontrarse en estado de falla para todos los eventos básicos en el árbol de fallas.

B.14.4 Proceso

Los pasos para desarrollar un árbol de fallas son los siguientes:

- Se define el elemento máximo que se va a analizar. Éste puede ser una falla o un resultado más amplio de la falla. Cuando se analiza el resultado, el árbol puede contener una sección relacionada con la mitigación de la falla real.

- Al empezar con el evento máximo se identifican las posibles causas inmediatas o los modos de falla que ocasionan el evento máximo.

- Se analiza cada uno de estos modos de falla/causa para identificar cómo se podría producir su falla.

- Se continúa con la identificación paso a paso de la operación no deseable del sistema hasta niveles sucesivamente inferiores del sistema hasta que el análisis adicional no sea productivo. En un sistema de hardware éste podría ser el nivel de falla del componente. Los eventos y los factores causales en el nivel más bajo del sistema que han sido analizados se conocen como eventos base.

- Cuando se pueden asignar probabilidades a los eventos base, se puede calcular la probabilidad del evento máximo. Para que la cuantificación sea válida debe tener la capacidad de demostrar que, para cada compuerta, todos los elementos de entrada son tanto necesarios como suficientes para producir el evento de salida. Si éste no es el caso, el árbol de fallas no es válido para el análisis de la probabilidad pero puede ser una herramienta útil para presentar las relaciones causales.

Como parte de la cuantificación puede ser necesario simplificar el árbol de fallas utilizando álgebra booleana para explicar los modos de falla duplicados.

Al igual que suministrar una estimación de la probabilidad del evento principal, se pueden identificar juegos mínimos de fallas, que forman trayectorias separadas individuales hacia el evento principal y se puede calcular su influencia en el evento máximo.

Excepto para árboles de falla sencillos, se necesita un paquete de software para manejar correctamente los cálculos cuando se presentan eventos repetidos en varios lugares en el árbol de fallas, y para calcular los juegos mínimos de fallas. Las herramientas de software ayuden a garantizar la consistencia, la corrección y la verificación.

B.14.5 Elementos de salida

Los elementos de salida del análisis de árbol de fallas son los siguientes:

- una representación gráfica de la forma en que se puede presentar el evento máximo, la cual ilustra la interacción de las trayectorias cuando dos o más eventos simultáneos deben ocurrir;

- una lista de los juegos mínimos de fallas (trayectorias individuales para la ~~falla~~) con la probabilidad de que cada uno de ellos se presente (cuando se dispone de los datos);

- la probabilidad del evento máximo.

B.14.6 Fortalezas y limitaciones

Las fortalezas de este análisis son:

- Permite un enfoque disciplinado que es altamente sistemático, pero al mismo tier suficientemente flexible para permitir el análisis de una variedad de factores incluyen las interacciones humanas y los fenómenos físicos.

- La aplicación del enfoque "máximo-mínimo", implícito en esta técnica, enfoca la aten en aquellos efectos de la falla que se relacionan directamente con el evento máximo.

- El análisis AAF es útil especialmente para analizar sistemas con muchas interface interacciones.

- La representación gráfica acarrea la comprensión fácil del comportamiento del siste los factores incluidos, pero dado que los árboles con frecuencia son grandes procesamiento de los árboles de fallas puede requerir de sistemas de computado Este rasgo permite incluir relaciones lógicas más complejas (por ejemplo compue No Y y No O) pero también dificulta la verificación del árbol de fallas.

- El análisis lógico de los árboles de fallas y la identificación de los juegos mínimos fallas es útil para identificar las trayectorias de fallas sencillas en sistemas complejos en donde se podrían omitir las combinaciones particulares de los ever que ocasionan el evento máximo.

Las limitaciones incluyen:

- Se incluyen las incertidumbres en las probabilidades de los eventos base en cálculos de la probabilidad del evento máximo. Esto puede ocasionar niveles altos incertidumbre cuando no se conocen con exactitud las probabilidades de la falla elemento base; sin embargo es posible un grado alto de confianza en un sistema que comprende bien.

- En algunas situaciones, los eventos causales no se reúnen y puede ser d determinar si se han incluido todas las trayectorias importantes para el evento máxi En esta situación no es posible el análisis de la probabilidad.

- El árbol de fallas es un modelo estático, no se abordan las interdependencias tiempo.

- Los árboles de fallas sólo pueden tratar con los estados binarios (fallido/no fallido).

- Aunque los modos de error humano se pueden incluir en un árbol de fallas cualital en general, las fallas de grado o calidad que a menudo caracterizan al error humano se pueden incluir fácilmente.

- Un árbol de fallas no permiten incluir con facilidad los efectos dominó o las fa condicionales.

B.14.7 Documento de Referencia

IEC 61025, *Fault Tree Analysis (FTA)*

IEC 60300-3-9, *Dependability Management. Part 3: Application Guide. Section 9: Risk Analysis of Technological Systems.*

B.15 ANÁLISIS DE ÁRBOL DE EVENTOS (AAE)

B.15.1 Información general

Este análisis es una técnica gráfica para representar las secuencias mutuamente excluyentes de los eventos que siguen a un evento detonante de acuerdo con el funcionamiento o la falta de funcionamiento de los diversos sistemas diseñados para mitigar sus consecuencias (véase Figura B.3). Se puede aplicar tanto cualitativa como cuantitativamente.

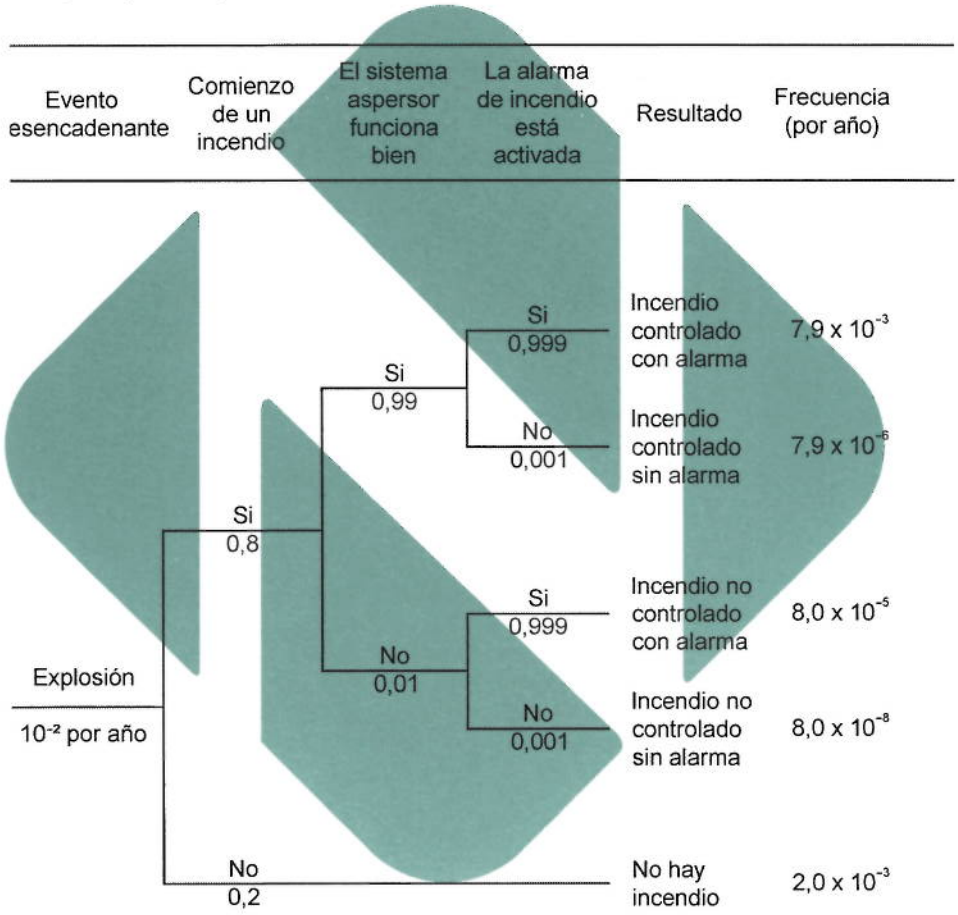


Figura B.3. Ejemplo de un árbol de eventos

La Figura B.3 ilustra los cálculos sencillos para un ejemplo de árbol de eventos, cuando las ramas son totalmente independientes.

Al dispersarse en abanico como un árbol, el análisis AAE puede representar los eventos agravantes o mitigantes en respuesta al evento desencadenante, tomando en consideración sistemas, funciones o barreras adicionales.

B.15.2 Uso

El análisis AAE se puede utilizar para modelar, calcular y clasificar (desde el punto de vista del riesgo) diversos escenarios de accidente posteriores al evento desencadenante.

Este análisis se puede utilizar en cualquier etapa del ciclo de duración de un producto o proceso. Se puede utilizar cualitativamente para ayudar a idear escenarios potenciales y secuencias de eventos después de un evento desencadenante y la manera en que los resultados se ven afectados por diversos tratamientos, barreras o controles destinados a mitigar resultados no deseados.

El análisis cuantitativo lleva por sí solo a considerar la aceptabilidad de los controles. Se utiliza con más frecuencia para modelar fallas cuando existen salvaguardas múltiples.

Este análisis se puede utilizar para modelar eventos desencadenantes que podrían ocasionar pérdida o ganancia. Sin embargo, en las circunstancias en que se buscan trayectorias para optimizar la ganancia, el modelado se realiza con más frecuencia utilizando un árbol de decisiones.

B.15.3 Elementos de entrada

Los elementos de entrada incluyen:

- la lista adecuada de los eventos desencadenantes;
- información sobre tratamientos, barreras y controles, y sus probabilidades de falla (para el análisis cuantitativo);
- comprensión de los procesos en los cuales escala la falla inicial.

B.15.4 Proceso

Un árbol de eventos empieza con la selección del evento desencadenante. Éste puede ser un incidente como por ejemplo una explosión de polvo o un evento causal como una falla de la energía eléctrica. Posteriormente se hace un listado en secuencia de las funciones o de los sistemas implementados para mitigar los resultados. Para cada función o sistema, se traza una línea que representa su éxito o su fracaso. Se puede asignar una probabilidad de la falla particular a cada línea, con la estimación de su probabilidad condicional, por ejemplo mediante un juicio experto o un análisis de árbol de fallas. De este modo se modelan las diversas trayectorias desde el evento desencadenante.

Observe que las probabilidades en el árbol de eventos son probabilidades condicionales, por ejemplo la probabilidad de que un aspersor funcione no es la probabilidad que se obtiene a partir de ensayos en condiciones normales sino la probabilidad de que funcione en condiciones de incendio causado por una explosión.

Cada trayecto a través del árbol representa la probabilidad de que ocurran todos los eventos en dicho trayecto. Por lo tanto, la frecuencia del resultado se representa mediante el producto de las probabilidades condicionales individuales y la frecuencia del evento desencadenante, dado que los diversos eventos son independientes.

B.15.5 Elementos de salida

Los elementos de salida de un análisis de árbol de eventos incluyen los siguientes:

- descripciones cualitativas de los problemas potenciales como combinaciones de eventos que producen diversos tipos de problemas (rango de resultados) a partir de los eventos desencadenantes;

- estimaciones cuantitativas de las frecuencias o probabilidades de los eventos y la importancia relativa de diversas secuencias de falla y eventos contribuyentes;

- listado de recomendaciones para reducir los riesgos;

- evaluaciones cuantitativas de la eficacia de las recomendaciones.

B.15.6 Fortalezas y limitaciones

Las fortalezas de este análisis incluyen las siguientes:

- el análisis representa de un modo diagramático claro los escenarios potenciales posteriores a un evento desencadenante, su análisis y la influencia del éxito o la falla de los sistemas o las funciones de mitigación;

- explica los efectos de tiempo, dependencia y dominó que son difíciles de modelar en los árboles de fallas;

- representa gráficamente las secuencias de eventos que no son posibles de representar cuando se usan árboles de falla.

Las limitaciones incluyen:

- Con el fin de utilizar este análisis como parte de una valoración exhaustiva, es necesario identificar todos los eventos desencadenantes potenciales. Esto se puede realizar utilizando otro método de análisis (por ejemplo el EPO y APP), sin embargo, siempre existe el potencial de omitir algunos eventos desencadenantes importantes.

- Con los árboles de eventos únicamente se tratan los estados de éxito o falla de un sistema y es difícil incorporar eventos retrasados de éxito o recuperación;

- Cualquier trayecto es condicional en los eventos que ocurrieron en puntos previos de las ramas a lo largo del trayecto. Por lo tanto se abordan muchas dependencias a lo largo de los trayectos posibles. No obstante, algunas de las dependencias, por ejemplo los componentes comunes, los sistemas de utilidad y los operadores, pueden ser omitidos si no se manejan cuidadosamente, y pueden llevar a estimaciones optimistas del riesgo.

B.16 ANÁLISIS DE CAUSA Y CONSECUENCIA

B.16.1 Generalidades

El análisis de causa y consecuencia es una combinación de los análisis de árbol de fallas y árbol de eventos. Comienza a partir de un evento crítico y analiza las consecuencias por medio de una combinación de salidas lógicas SI/NO que representan condiciones que pueden ocurrir o fallas de los sistemas diseñados para mitigar las consecuencias del evento desencadenante. Las causas de las condiciones o las fallas se analizan por medio de árboles de fallas (véase sección B.15).

B.16.2 Uso

Este análisis se desarrolló originalmente como una herramienta de confiabilidad para l sistemas críticos de seguridad con el fin de obtener una comprensión más completa de l fallas del sistema. Así como análisis de árbol de fallas, este análisis se utiliza para represent la lógica de la falla que ocasiona un evento crítico, pero añade la funcionalidad de un árbol fallas permitiendo el análisis de las fallas secuenciales en el tiempo. Este método tambi permite incorporar demoras de tiempo en el análisis de las consecuencias, lo cual no es posit con los árboles de eventos.

El método se utiliza para analizar los diversos trayectos o caminos que un sistema podría tom después de un evento crítico, dependiendo del comportamiento de los subsistemas particular (por ejemplo los sistemas de respuesta ante emergencias). Si se cuantifica, proporciona u estimación de la probabilidad de diversas consecuencias posibles después de un ever crítico.

Dado que cada secuencia en un diagrama de causa y consecuencia es una combinación subdivisiones de árboles de fallas, el análisis de causa y consecuencia se puede usar co una herramienta para elaborar árboles de fallas más grandes.

Elaborar y usar los diagramas es complejo y éstos se utilizan o tienden a ser utilizados cuan la magnitud de la consecuencia potencial de la falla justifica un esfuerzo intenso.

B.16.3 Elementos de entrada

Se requiere del entendimiento del sistema, así como sus modos y escenarios de falla.

B.16.4 Proceso

La Figura B.4 ilustra un diagrama conceptual de un análisis típico de causa y consecuencia.

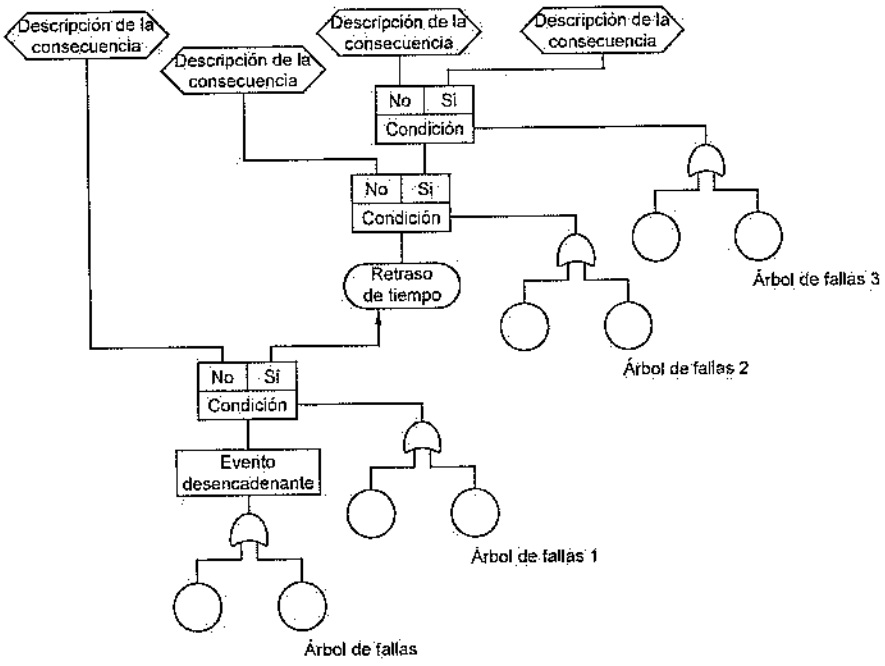


Figura B.4. Ejemplo de un análisis de causa y consecuencias

El procedimiento es el siguiente:

a) Identificar el evento crítico (o desencadenante), equivalente al evento principal de un árbol de fallas y al evento desencadenante en un árbol de eventos.

b) Desarrollar y validar el árbol de fallas para las causas del evento desencadenante tal como se describe en la sección B.14. Se utilizan los mismos símbolos de un análisis de árbol de fallas convencional.

c) Decidir el orden en el cual se van a considerar las condiciones. Este orden podría ser una secuencia lógica como por ejemplo la secuencia de tiempo en el cual ocurren.

d) Construir las trayectorias para las consecuencias dependiendo de las diversas condiciones. Esto es similar a un árbol de eventos pero bifurcaciones en las trayectorias del árbol de eventos se ilustra con un cuadro etiquetado con la condición particular a la cual se aplica.

e) Siempre que las fallas para cada cuadro de condición sean independientes, se puede calcular la probabilidad de cada consecuencia. esto se logra asignando primero probabilidades a cada elemento de salida del cuadro de condición (utilizando los árboles de falla correspondientes, según convenga). La probabilidad de que una secuencia cualquiera conduzca a una consecuencia particular se obtiene al multiplicar las probabilidades de cada secuencia de las condiciones que terminan en esa consecuencia particular. Si más de una secuencia finaliza en la misma consecuencia, se suman las probabilidades de cada secuencia. Si existen dependencias entre las fallas de las condiciones en una secuencia (por ejemplo una falla en la energía eléctrica puede causar la falla de varias condiciones) entonces se deberían tratar las dependencias antes del cálculo.

B.16.5 Elementos de salidas

Los elementos de salida de un análisis de causa y consecuencia es una representación de como un sistema puede fallar, que ilustra tanto las causas como las consecuencias. También una estimación de la probabilidad de ocurrencia de cada consecuencia potencial basada en el análisis de las probabilidades de ocurrencia de las condiciones particulares después del evento crítico.

B.16.6 Fortalezas y limitaciones

Las ventajas del análisis de causa y consecuencia son las mismas para los árboles de eventos y los árboles de falla combinados. Además, este análisis supera algunas de las limitaciones de dichas técnicas ya que puede analizar eventos que se desarrollan en el paso del tiempo. El análisis de causa y consecuencia brinda una visión global del sistema.

Las limitaciones consisten en que este análisis es más complejo que los análisis de árbol de fallas y árbol de eventos, tanto en su construcción como en la manera en que se tratan las dependencias durante la cuantificación.

B.17 ANÁLISIS DE CAUSA Y EFECTO

B.17.1 Información general

El análisis de causa y efecto es un método estructurado para identificar las posibles causas de un evento no deseado o de un problema. Este análisis organiza los factores contribuyentes

potenciales en categorías amplias, de tal manera que todas las hipótesis posibles se pueden considerar. Sin embargo, por sí solo no indica las causas reales dado que éstas sólo se pueden determinar mediante evidencia real y prueba empírica de las hipótesis. La información se organiza bien sea en un diagrama en espina de pescado (también denominado Ishikawa) o en un diagrama de árbol (véase el literal B.17.4).

B.17.2 Uso

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

Se utiliza para permitir la consideración de todos los escenarios y las causas posibles generadas por un equipo de expertos y permite establecer el consenso sobre las causas más probables que después se pueden someter a prueba empírica o a evaluación de los datos disponibles. Tiene mayor utilidad al comienzo de un análisis para ampliar el pensamiento acerca de las posibles causas y luego establecer hipótesis potenciales que se pueden considerar más formalmente.

La elaboración de un diagrama de causa y efecto se puede realizar cuando existe la necesidad de:

- identificar las posibles causas raíz, las razones básicas, de un efecto, problema o una condición específicos;
- clasificar y relacionar algunas de las interacciones entre los factores que afectan a un proceso particular;
- analiza los problemas existentes de tal modo que se puedan tomar acciones correctivas

Los beneficios de elaborar un diagrama de causa y efecto incluyen:

- concentra la atención de los miembros a cargo de la revisión en un problema específico
- ayuda a determinar las causas principales de un problema utilizando un enfoque estructurado;
- fomenta la participación del grupo y utiliza el conocimiento del grupo para el producto o el proceso;
- utiliza un formato ordenado, fácil de leer para diagramar las relaciones de causa efecto;
- indica las posibles causas de la variación en un proceso;
- identifica las áreas en las que se deberían recolectar datos para el estudio adicional.

El análisis de causa y efecto se puede utilizar como un método para llevar a cabo el análisis de causa principal (véase sección B.12).

B.17.3 Elementos de entrada

Los elementos de entrada para un análisis de causa y efecto pueden provenir de la experticia y la experiencia de los participantes o de un modelo desarrollado previamente que se haya utilizado en el pasado.

B.17.4 Proceso

Este análisis debería ser realizado por un equipo de expertos con conocimiento del problema que requiere solución.

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

- establecer el efecto que se va a analizar y ubicarlo en un cuadro. El efecto puede ser positivo (un objetivo) o negativo (un problema) dependiendo de las circunstancias;
- determinar las principales categorías de las causas representadas en los cuadros del diagrama de Ishikawa. Típicamente, para un problema en el sistema, las categorías podrían ser personas, equipo, ambiente, procesos, etc. sin embargo, éstas se seleccionan para que se adapten al contexto particular;
- completar las causas posibles para cada categoría mayor con ramas y sub ramas para describir la relación entre ellas;
- continuar preguntándose "¿por qué?" o "¿qué causó qué?" para conectar las causas;
- revisar todas las ramas para verificar la consistencia y completitud, y asegurarse de que las causas se aplican al efecto principal;
- identificar las causas más probables con base en la opinión del equipo de expertos y la evidencia disponible.

Normalmente, los resultados se representan en un diagrama de espina de pescado o Ishikawa o un diagrama en árbol. El diagrama Ishikawa está estructurado separando las causas en categorías principales (representadas por las líneas que se alejan del eje central) con ramas y sub ramas que describen las causas más específicas en tales categorías.

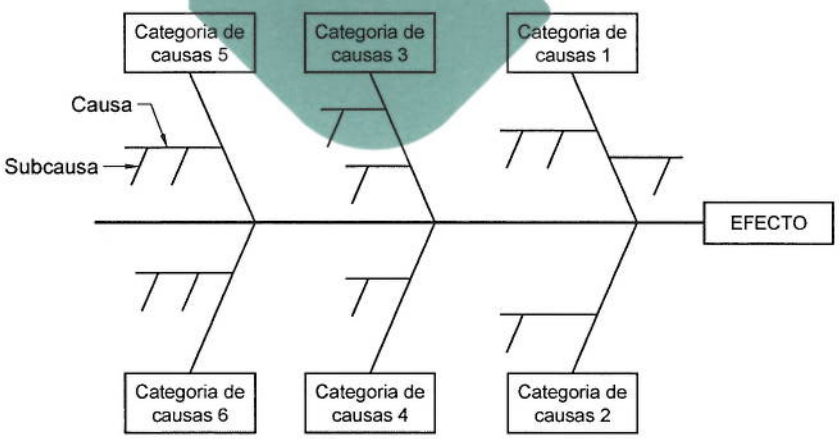


Figura B.5. Ejemplo de un diagrama de Ishikawa o en espina de pescado

La representación en árbol es similar en apariencia al árbol de fallas, aunque éste con frecuencia se representa con el árbol desarrollándose de izquierda a derecha en lugar de hacerlo hacia abajo en la página. Sin embargo, éste no se puede cuantificar para producir una probabilidad del evento principal dado que las causas son posibles factores que contribuyen más que las fallas con una probabilidad de ocurrencia conocida.

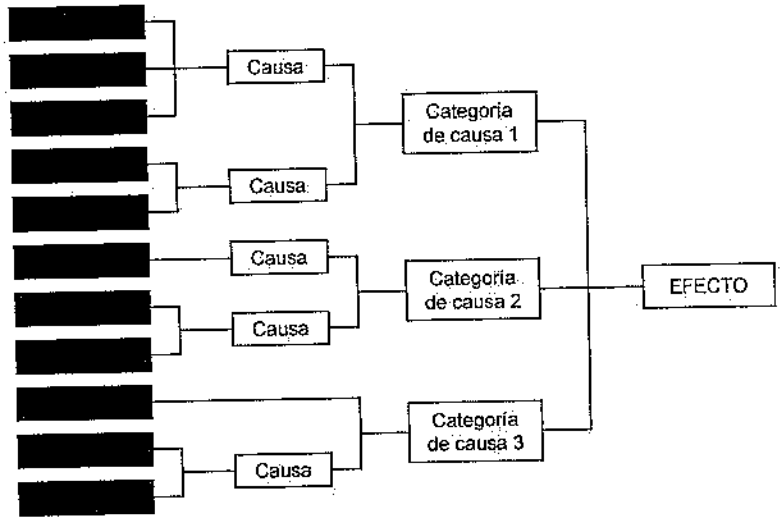


Figura B.6. Ejemplo de una formulación en árbol del análisis de causa y efecto

Los diagramas de causa y efecto generalmente se utilizan cualitativamente. Es posible asumir que la probabilidad del problema es 1 y asignar probabilidades a las causas genéricas, y posteriormente a las subcausas con base en el grado de convicción acerca de su importancia. Sin embargo, los factores contribuyentes con frecuencia interactúan y contribuyen al efecto de maneras complejas que pueden hacer que la cuantificación no sea válida.

B.17.5 Elementos de salida

El elemento de salida de un análisis de causa y efecto es un diagrama que ilustra las causas posibles y probables. Este diagrama se debe verificar y probar empíricamente antes de que se puedan hacer recomendaciones.

B.17.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- participación de los expertos en el tema trabajando en un ambiente de equipo;
- análisis estructurado;
- consideración de todas las hipótesis probables;
- ilustración de los resultados de manera gráfica fácil de leer;
- identificación de las áreas en donde se necesitan datos adicionales;

UNIVERSIDAD MILITAR
NUEVA GRANADA
BIBLIOTECA

- se puede utilizar para identificar los factores que contribuyen tanto a los efectos deseados como a los no deseados. Tomar un enfoque positivo sobre un aspecto puede fomentar mayor pertenencia y participación.

Las limitaciones incluyen:

- es posible que el equipo no tenga la experticia necesaria;
- este no es un proceso completo en sí mismo y es necesario que forme parte de un análisis de causa principal para producir recomendaciones;
- es una técnica de representación de ideas más que una técnica de análisis independiente;
- la separación de los factores causales en categorías principales al comienzo del análisis implica que las interacciones entre las categorías pueden no ser consideradas adecuadamente, por ejemplo cuando la falla en el equipo es causada por un error humano, o los problemas humanos son causados por un diseño deficiente.

B.18 ANÁLISIS DE CAPAS DE PROTECCIÓN (ACDP)

B.18.1 Información general

Este análisis es un método semicuantitativo para estimar los riesgos asociados con un evento o un escenario no deseado. Analiza si existen suficientes medidas para controlar o mitigar el riesgo.

Se selecciona un par de causa y consecuencia y se identifican las capas de protección que evitan que la causa origine la consecuencia no deseada. Se realiza un cálculo de orden de magnitud para determinar si la protección es adecuada para reducir el riesgo hasta un nivel tolerable.

B.18.2 Uso

El análisis ACDP se puede utilizar de modo cualitativo sencillamente para revisar las capas de protección entre un peligro o un evento causal y un resultado. Normalmente, se aplicaría un enfoque semicuantitativo para añadir rigor a los procesos de clasificación, por ejemplo después de un EPO o un APP.

El análisis proporciona una base para la especificación de capas de protección independientes (CPI) y niveles de integridad de la seguridad (NIS) para sistemas instrumentados, tal como se describe en la serie de normas IEC 61508 e IEC 61511, en la determinación de los requisitos del nivel de integridad de la seguridad para sistemas de seguridad instrumentados. El análisis ACDP se puede utilizar para ayudar a distribuir eficazmente los recursos para la reducción del riesgo mediante el análisis de la reducción del riesgo producida por cada capa de protección.

B.18.3 Elementos de entrada

Los elementos de entrada incluyen:

- información básica sobre los riesgos, incluyendo peligros, causas y consecuencias tales como las que proporciona el análisis AAP;

- información sobre los controles implementados o propuestos;
- frecuencias de los eventos causales y probabilidades de falla de las capas d protección, mediciones de consecuencias y una definición de riesgo tolerable;
- frecuencia de las causas desencadenantes, probabilidades de falla de las capas d protección, mediciones de las consecuencias y una definición de riesgo tolerable.

B.18.4 Proceso

El análisis ACDP se realiza utilizando un equipo de expertos que aplican el siguient procedimiento:

- identificar las causas desencadenantes de un resultado no deseado y buscar dato sobre sus frecuencias y consecuencias;
- seleccionar un único par de causa y consecuencia;
- se identifican las capas de protección que evitan que la causa prosiga hasta l consecuencia indeseada y se analizan para determinar su eficacia;
- identificar las capas de protección independientes (CPI) (no todas las capas d protección son CPI);
- estimar la probabilidad de falla de cada capa de protección independiente;
- la frecuencia de la causa desencadenante se combina con las probabilidades de falla d cada CPI y las probabilidades de cualquier modificador condicional (un modificadc condicional es por ejemplo si estará presente una persona que sufra el impacto) par determinar la frecuencia de ocurrencia de la consecuencia no deseada. Se utiliza órdenes de magnitud para las frecuencias y las probabilidades;
- el nivel de riesgo calculado se compara con los niveles de tolerancia del riesgo par determinar si se requiere protección adicional.

Una CPI es un sistema o una acción de recursos que puede evitar que un escenario prosig hasta su consecuencia no deseada, independiente del evento causal o de cualquier otra cap de protección asociada a dicho escenario.

Una CPI incluye:

- rasgos del diseño;
- mecanismos de protección física;
- sistemas de apagado e interbloqueo
- alarmas críticas e intervención manual;
- protección física posterior al evento;
- sistemas de respuesta ante emergencias (los procedimientos y las inspecciones no so CPI).

B.18.5 Elementos de salida

Se deben suministrar recomendaciones con respecto a los controles adicionales y la eficacia de tales controles para reducir el riesgo.

El análisis es una de las técnicas utilizadas para la valoración de los NIS cuando se tratan sistemas de seguridad relacionados/instrumentados.

B.18.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- requiere menos tiempo y recursos que el análisis de árbol de fallas o de la valoración totalmente cuantitativa del riesgo, pero es más riguroso que los juicios cualitativos subjetivos;
- ayuda a identificar y enfocarse en los recursos en las capas de protección más críticas;
- identifica operaciones, sistemas y procesos para los que hay salvaguardas insuficientes;
- enfatiza las consecuencias más graves.

Las limitaciones incluyen:

- el análisis ACDP enfatiza un par de causa y consecuencia y un escenario a la vez. Las interacciones complejas entre los riesgos o entre los controles no están cubiertas;
- los riesgos cuantificados pueden no explicar las fallas de modo común;
- este análisis no se aplica a escenarios muy complejos en los que existen muchos pares de causa y efecto o una amplia variedad de consecuencias que a afectan partes involucradas diferentes.

B.18.7 Documentos de referencia

IEC 61508 (todas las partes), *Functional safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.*

IEC 61511, *Functional Safety. Safety Instrumented Systems for the Process Industry Sector.*

B.19 ANÁLISIS DE ÁRBOL DE DECISIONES

B.19.1 Información general

Un árbol de decisiones representa alternativas de decisión y resultados de modo secuencial que toman en consideración los resultados inciertos. Es similar a un árbol de eventos en que empieza desde un evento desencadenante o una decisión inicial y modela diferentes trayectorias y resultados derivados de los eventos que se pueden presentar, así como diversas decisiones que se pueden tomar.

B.19.2 Uso

El árbol de decisiones se utiliza en la gestión de riesgos del proyecto y en otras circunstancias para facilitar la selección del mejor curso de acción cuando existe incertidumbre. La representación gráfica también puede ayudar a comunicar los motivos de las decisiones.

B.19.3 Elementos de entrada

Un plan del proyecto con los puntos de decisiones. Información sobre los posibles resultados de las decisiones y sobre la oportunidad de los eventos que podrían afectar a las decisiones.

B.19.4 Proceso

Un árbol de decisiones empieza con una decisión inicial, por ejemplo proseguir con el proyecto A en lugar del proyecto B. A medida que los dos proyectos hipotéticos prosiguen, ocurrirán eventos diferentes y será necesario tomar diferentes decisiones predecibles. Estas decisiones están representadas en formato de árbol, similar a un árbol de eventos. La probabilidad de los eventos se puede estimar junto con el costo o la utilidad del resultado final de esa trayectoria.

La información con respecto a la mejor trayectoria de decisión lógicamente es aquella que produce el valor calculado máximo esperado como producto para todas las probabilidades condicionales a lo largo de la trayectoria y el valor del resultado.

B.19.5 Elementos de salida

Los elementos de salida incluyen:

- un análisis lógico del riesgo que presentan diversas opciones que se pueden tomar;
- un cálculo del valor esperado para cada trayecto posible.

B.19.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- suministra una representación gráfica clara de los detalles de un problema de decisión;
- permite un cálculo de la mejor trayectoria a través de toda una situación.

Las limitaciones incluyen:

- los árboles de decisiones grandes pueden ser demasiado complejos para facilitar la comunicación con otros;
- puede existir una tendencia a exceder la simplificación de la situación para poder representarla en un diagrama de árbol.

B.20 VALORACIÓN DE LA CONFIABILIDAD HUMANA (VCH)

B.20.1 Información general

La valoración de la confiabilidad humana trata del impacto de los humanos en el desempeño del sistema y se puede utilizar para evaluar las influencias del error humano en el sistema.

Muchos procesos tienen potencial para el error humano, especialmente cuando el tiempo disponible para que el operario tome decisiones es corto. La probabilidad de que se desarrollen problemas lo suficiente para ser graves puede ser pequeña. Sin embargo, en ocasiones la acción humana será la única defensa para evitar que una falla inicial progrese hacia un accidente.

La importancia de este análisis ha sido ilustrada por varios accidentes en los cuales los errores humanos críticos contribuyeron a una secuencia catastrófica de eventos. Tales accidentes son advertencias contra las valoraciones de riesgo que únicamente enfatizan el hardware y el software en un sistema. También ilustran los peligros por ignorar la posibilidad de la contribución del error humano. Además, este análisis es útil para subrayar errores que pueden impedir la productividad y para revelar los modos en que estos errores y otras fallas (hardware y software) se pueden "recuperar" por acción de los operarios humanos y el personal de mantenimiento.

B.20.2 Uso

La VCH se puede utilizar cualitativa o cuantitativamente. Cualitativamente se utiliza para identificar el potencial de error humano y sus causas, de manera que se pueda reducir la probabilidad de error. La VHC cuantitativa se utiliza para proporcionar datos sobre las fallas humanas para el análisis de árbol de fallas u otras técnicas.

B.20.3 Elementos de entrada

Los elementos de entrada para la VCH incluyen:

- información para definir las labores que las personas deberían ejecutar;
- experiencia sobre los tipos de error que se presentan en la práctica y sobre el potencial para el error;
- experticia sobre el error humano y su cuantificación.

B.20.4 Proceso

El proceso de la VCH es el siguiente:

- **Definición del problema**. ¿Qué tipos de participación humana se van a investigar/evaluar?
- **Análisis de las labores**. ¿Cómo se van a llevar a cabo las labores y qué tipo de ayudas serán necesarias para dar soporte al desempeño?
- **Análisis del error humano**. ¿Cómo puede fallar el desempeño de la labor? ¿Cuáles errores podrían presentarse y cómo se podrían recuperar?
- **Representación**. ¿Cómo pueden estos errores o fallas en el desempeño de la labor integrarse con otros eventos de hardware, software y ambientales para permitir el cálculo de las probabilidades de falla del sistema total?
- **Clasificación**. ¿Existen errores o labores que no requieran de cuantificación detallada?
- **Cuantificación**. ¿Cuál es la probabilidad de los errores individuales y las fallas en las labores?

- **Valoración del impacto.** ¿Cuáles errores o labores son más importantes, es deci cuales tienen la máxima contribución a la confiabilidad o al riesgo?

- **Reducción del error.** ¿Cómo se puede lograr una confiabilidad humana superior?

- **Documentación.** ¿Cuáles detalles de la VCH es necesario documentar?

En la práctica, el proceso de la VCH prosigue paso a paso aunque en algunas ocasiones cor partes (por ejemplo el análisis de las labores y la identificación del error) que prosiguer paralelas entre sí.

B.20.5 Elementos de salida

Los elementos de salida incluyen:

- una lista de errores que se pueden presentar y los métodos mediante los cuales se pueden reducir – preferiblemente a través del rediseño del sistema;

- modos de error, causas y consecuencias de los tipos de error;

- una valoración cualitativa o cuantitativa del riesgo impuesto por los errores.

B.20.6 Fortalezas y limitaciones

Las fortalezas de la VCH incluyen:

- este análisis proporciona un mecanismo formal para incluir al error humano en la consideración de los riesgos asociados con los sistemas en donde los humanos a menudo tienen una función importante;

- la consideración formal de los modos y los mecanismos del error humano puede ayuda a reducir la probabilidad de falla debida al error.

Las limitaciones incluyen:

- la complejidad y variabilidad de los humanos, lo cual dificulta la definición de modos de fallas sencillos y de las probabilidades;

- muchas actividades de los humanos no tienen un modo sencillo del éxito/falla. la VCH tiene dificultades al tratar con fallas parciales o fallas en la calidad o la toma deficiente de las decisiones.

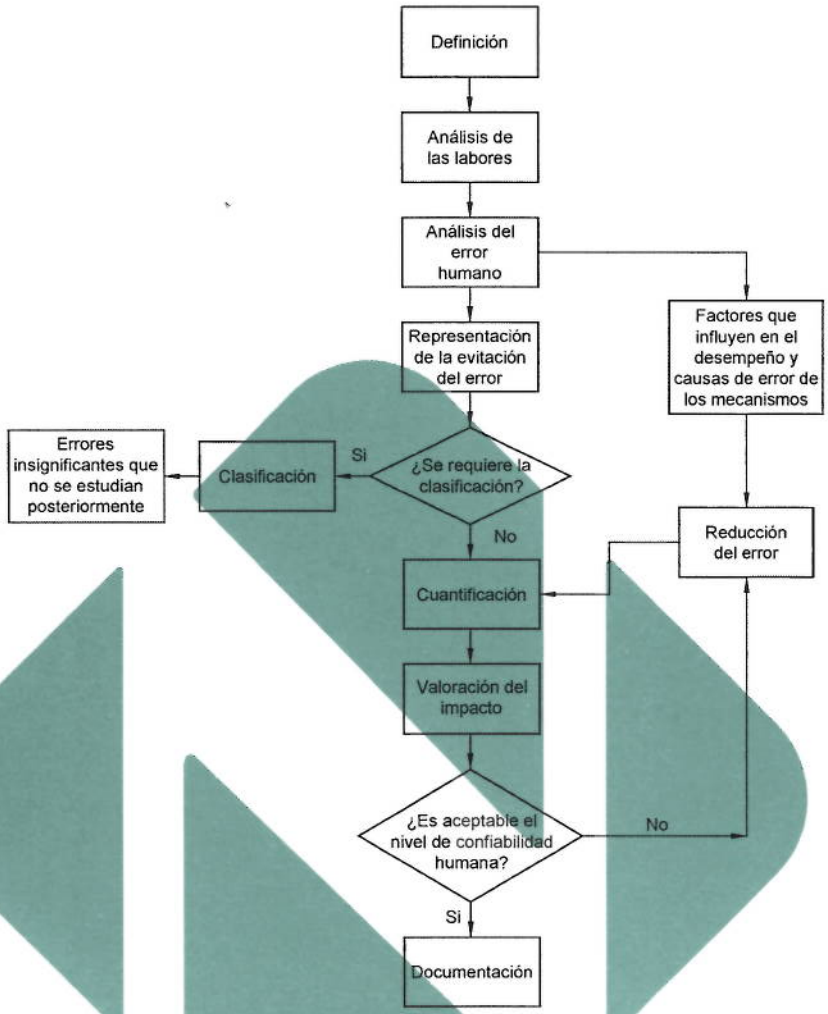


Figura B.7. Ejemplo de valoración de la confiabilidad humana

B.21 ANÁLISIS EN ESQUEMA DE CORBATÍN

B.21.1 Información general

Este análisis es un modo diagramático sencillo de describir y analizar las trayectorias de un riesgo desde las causas hasta las consecuencias. Se puede considerar una combinación del pensamiento de un árbol de fallas que analiza la causa de un evento (representado por el centro del moño) y un árbol de eventos que analiza las consecuencias. Sin embargo, el énfasis del análisis en corbatín está en las barreras entre las causas y el riesgo, y el riesgo y las consecuencias. Los diagramas en corbatín se pueden construir comenzando con árboles de eventos y de fallas, pero con más frecuencia se elaboran directamente a partir de una sesión de lluvia de ideas.

B.21.2 Uso

Este análisis se utiliza para representar un riesgo, mostrando un rango de causas y consecuencias posibles. Se utiliza cuando la situación no amerita la complejidad de un análisis total de árbol de fallas o cuando hay mayor énfasis en garantizar que existe una barrera o control para cada trayectoria de falla Es útil cuando hay trayectorias claramente independientes hacia la falla.

El análisis con frecuencia es más fácil de entender que los árboles de fallas y eventos, y por ello puede ser una herramienta útil de comunicación cuando el análisis se logra utilizando técnicas más complejas.

B.21.3 Elementos de entrada

Se requiere de la comprensión de la información sobre las causas y las consecuencias de un riesgo y de las barreras y controles que pueden prevenirlo, mitigarlo o estimularlo.

B.21.4 Proceso

Este análisis se realiza de la siguiente manera:

a) Se identifica un riesgo particular para su análisis y se representa como el nudo central del corbatín.

b) Se hace un listado de las causas del evento teniendo en cuenta las fuentes de riesgo (o de peligros en un contexto de seguridad).

c) Se identifica el mecanismo mediante el cual la fuente de riesgo origina el evento crítico.

d) Se trazan líneas entre cada causa y el evento formando la parte izquierda del corbatín. Se pueden identificar los factores que podrían ocasionar el escalamiento y se incluyen en el diagrama.

e) Las barreras que deberían evitar que cada causa produzca las consecuencias no deseadas se pueden representar como barras verticales a través de la línea. Cuando hay factores que podrían causar el escalamiento, las barreras para el escalamiento también se pueden representar. El enfoque se puede utilizar para consecuencias positivas en donde las barras reflejan los "controles" que estimulan la generación del evento.

f) En la parte derecha del corbatín, se identifican las diversas consecuencias potenciales del riesgo y se trazan líneas que se irradian desde el evento del riesgo hasta a consecuencia potencial.

g) Las barreras para las consecuencias se representan como barras a través de las líneas radiales. El enfoque se puede utilizar para consecuencias positivas en donde las barras reflejan los "controles" que sustentan la generación de las consecuencias.

h) Las funciones de la gestión que soportan a los controles (tales como entrenamiento e inspección) se pueden ilustrar bajo el corbatín y vincular con el control respectivo.

Puede ser posible algún grado de cuantificación en un diagrama de corbatín, en donde las trayectorias son independientes, se conoce la probabilidad de una consecuencia o resultado en particular y se puede estimar una cifra para la eficacia de un control. Sin embargo, en muchas

situaciones, las trayectorias y las barreras no son independientes y los controles pueden ser procedimentales y, de este modo, la eficacia no es clara. La cuantificación a menudo se lleva a cabo de manera más adecuada utilizando AAF y AAE.

B.21.5 Elementos de salida

El elemento de salida es un diagrama sencillo que muestra las principales trayectorias de riesgo y las barreras implementadas para evitar o mitigar las consecuencias indeseables o para simular y promover las consecuencias deseadas.

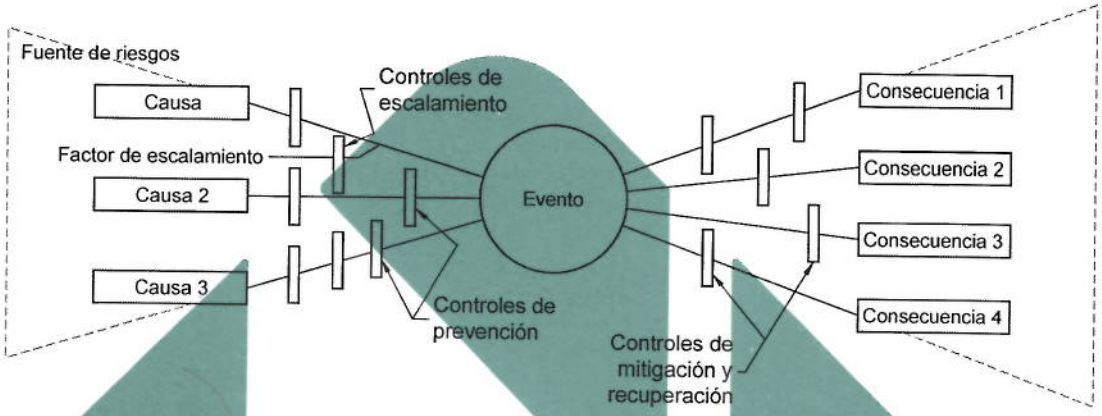


Figura B.8. Ejemplo de un diagrama de corbatín para consecuencias no deseadas

B.21.6 Fortalezas y limitaciones

Las fortalezas de este análisis son:

- es sencillo de entender y suministra una representación pictórica clara del problema;
- enfatiza la atención en los controles que supuestamente están implementados tanto para prevenir como para mitigar y su eficacia;
- se puede utilizar para consecuencias deseables;
- no necesita de un nivel alto de experticia para su utilización.

Las limitaciones incluyen:

- no se puede representar cuando se producen simultáneamente causas múltiples para originar las consecuencias (es decir, cuando existen compuertas y en un árbol de fallas que representa el lado izquierdo del corbatín);
- es posible que simplifique demasiado las situaciones complejas, particularmente cuando se intenta hacer la cuantificación.

B.22 MANTENIMIENTO CENTRADO EN LA CONFIABILIDAD

B.22.1 Información general

El mantenimiento centrado en la confiabilidad (MCC) es un método para identificar las políticas que se deberían implementar para gestionar las fallas con el fin de lograr de manera eficiente y eficaz la seguridad, la disponibilidad y la economía que se requieren para la operación de todos los tipos de equipo.

El MCC es actualmente una metodología aprobada y aceptada para utilizar en un amplio rango de industrias.

Este método suministra un proceso de decisión para identificar requisitos de mantenimiento preventivo eficaz y aplicable para el equipo, de acuerdo con las consecuencias de seguridad, operacionales y económicas de las fallas identificables, y el mecanismo de degradación responsable de tales fallas. El resultado final del trabajo a través de todo el proceso es un juicio sobre la necesidad de llevar a cabo una labor de mantenimiento u otra acción como por ejemplo cambios operacionales. Los detalles con respecto al uso y la aplicación del MCC se suministran en la norma IEC 60300-3-11.

B.22.2 Uso

Todas las labores se basan en la seguridad con respecto al personal y al ambiente y en preocupaciones operacionales o económicas. Sin embargo, conviene observar que los criterios considerados dependerán de la naturaleza del producto y su aplicación. Por ejemplo, será necesario que un proceso de producción sea viable económicamente y puede ser sensible a consideraciones ambientales estrictas, mientras que un elemento del equipo de defensa debería ser exitoso en términos operacionales pero puede ser menos estricto en cuanto a criterios de seguridad, economía y ambiente. Los máximos beneficios se pueden lograr a través de tener como objetivo el análisis donde las fallas tendrían efectos graves para la seguridad, el ambiente, la economía o las operaciones.

El método se utiliza para garantizar que se ejecuta el mantenimiento eficaz y aplicable, y en general se aplica durante la fase de diseño y desarrollo y después se implementa durante la operación y el mantenimiento.

B.22.3 Elementos de entrada

La aplicación exitosa de este método requiere de una buena comprensión del equipo y la estructura, el ambiente operacional y los sistemas asociados, los subsistemas y los elementos del equipo junto con las posibles fallas y las consecuencias de tales fallas.

B.22.4 Proceso

Los pasos básicos del programa MCC son los siguientes:

- iniciación y planificación;
- análisis de las fallas funcionales;
- selección de las labores;
- implementación;
- mejora continua.

El MCC se basa en los riesgos dado que sigue los pasos básicos de la valoración del riesgo. El tipo de valoración del riesgo es un análisis de modo y efecto de falla y su criticidad (AMEFC), pero requiere de un enfoque específico para el análisis cuando se utiliza en este contexto

La identificación del riesgo se enfoca en las situaciones en donde se pueden eliminar o reducir las fallas potenciales en cuanto a la frecuencia y/o las consecuencias realizando labores de mantenimiento. Esto se realiza identificando las normas de funciones y de desempeño que se requieren y las fallas del equipo y los componentes que pueden interrumpir tales funciones.

El análisis del riesgo consiste en la estimación de la frecuencia de cada falla sin que se realice mantenimiento. Las consecuencias se establecen definiendo los efectos de la falla. Una matriz de riesgos que combine la frecuencia de la falla y las consecuencias permite establecer categorías para los niveles del riesgo.

La evaluación del riesgo se realiza entonces seleccionando la política adecuada para la gestión de la falla para cada modo de falla.

La totalidad del proceso MCC se documenta extensamente para referencia y revisión futuras. La recolección de datos sobre la falla y datos relacionados con el mantenimiento permite el monitoreo de los resultados y la implementación de las mejoras.

B.22.5 Elementos de salida

El MCC proporciona una definición de labores de mantenimiento tales como monitoreo de la condición, restauración programada, reemplazo programado, hallazgo de fallas o mantenimiento no preventivo. Otras acciones posibles que pueden resultar del análisis pueden incluir el rediseño, los cambios en procedimientos de operación o mantenimiento o entrenamiento adicional. Luego se identifican los intervalos para estas labores y los recursos que se necesitan.

B.22.6 Documentos de referencia

IEC 60300-3-11, *Dependability Management. Part 3-11: Application Guide. Reliability Centred Maintenance*.

B.23 ANÁLISIS FORTUITO (AF) Y ANÁLISIS DE CIRCUITO FORTUITO (ACF)

B.23.1 Información general

El análisis fortuito es una metodología para identificar errores de diseño. Una condición fortuita es un hardware, un software o una condición integrada latente que puede causar un evento no deseado o inhibir que se produzca el elemento deseado, y que no es causado por una falla del componente. Estas condiciones se caracterizan por su naturaleza aleatoria y la capacidad de escapar a la detección de los ensayos de sistemas normalizados más rigurosos. Las condiciones fortuitas pueden causar la operación inadecuada, la pérdida de disponibilidad del sistema, retrasos del programa o incluso la muerte o la lesión del personal.

B.23.2 Uso

El análisis de circuito fortuito fue desarrollado a finales de la década de 1960 por la NASA con el fin de verificar la integridad y la funcionalidad de sus diseños. Este análisis sirvió como una herramienta útil para descubrir rutas de circuitos eléctricos no intencionales, y facilitó la creación de soluciones para aislar cada función. Sin embargo, a medida que la tecnología

avanzó, las herramientas para el análisis del circuito fortuito también tuvieron que progresar. El análisis fortuito incluye y excede significativamente la cobertura del análisis de circuito fortuito. Este análisis puede localizar problemas tanto en el hardware como en el software utilizando cualquier tecnología. Las herramientas del análisis fortuito pueden integrar en un solo análisis varios análisis como el de árbol de fallas, el modo y efecto de falla, estimados de confiabilidad, etc. lo cual ahorra tiempo y costos en del proyecto.

B.23.3 Elementos de entrada

El análisis fortuito es único con respecto al proceso de diseño en cuanto utiliza diferentes herramientas (árboles de red, grupos de árboles y pistas o preguntas que ayudan al analista a identificar las condiciones fortuitas) con el fin de hallar un tipo específico de problema. Los árboles de red y los grupos de árboles son agrupaciones topológicas del sistema real. Cada árbol de red representa una subfunción e ilustra todos los elementos de entrada que pueden afectar al resultado de la subfunción. Los grupos de árboles se elaboran combinando árboles de red que contribuyen al elemento de salida de un sistema particular. Un grupo de árboles adecuado presenta la salida del sistema en términos de todas sus entradas relacionadas. Éstas, junto con otras, se convierten en los elementos de entrada para el análisis.

B.23.4 Proceso

Los pasos básicos para realizar un análisis fortuito consisten en:

- preparación de los datos;
- construcción del árbol de red;
- evaluación de las trayectorias de la red;
- recomendaciones finales e informe.

B.23.5 Elementos de salida

Un circuito fortuito es un trayecto inesperado o un flujo lógico dentro de un sistema que, ba determinadas condiciones, puede desencadenar una función no deseada o inhibir a ur función deseada. El trayecto puede incluir hardware, software, condiciones del operador combinaciones de estos elementos. Los circuitos fortuitos no son el resultado de la falla d hardware sino condiciones latentes, inadvertidamente diseñadas en el sistema, codificadas e el programa de software o disparadas por el error humano. Existen cuatro categorías c circuitos fortuitos:

a) trayectos fortuitos: trayectos inesperados a lo largo de los cuales fluye corrient energía, o secuencias lógicas en una dirección no intencionada;

b) sincronización fortuita: eventos que ocurren en una secuencia inesperada o conflictiva;

c) indicaciones fortuitas: presentación ambigua o falsa de las condiciones operativas c sistema que pueden hacer que éste o un operador emprenda una acción no deseada;

d) etiquetas fortuitas: etiquetado incorrecto o impreciso de las funciones del sistema, p ejemplo las entradas para el sistema, los controles, los buses de representación q pueden hacer que un operador aplica un estímulo incorrecto al sistema.

B.23.6 Fortalezas y limitaciones

Las fortalezas incluyen:

- el análisis fortuito es bueno para identificar los errores en el diseño;
- funciona mejor cuando se aplica junto con el análisis EPO;
- es muy bueno para tratar con sistemas que tienen estados múltiples, tales como las plantas de lote y semilote.

Las limitaciones incluyen:

- el proceso es un poco diferente dependiendo de si se aplica a circuitos eléctricos, plantas de procesos, equipos mecánicos o software;
- el método depende de establecer árboles de red correctos.

B.24 ANÁLISIS DE MARKOV

B.24.1 Información general

Este análisis se utiliza cuando el estado futuro de un sistema depende únicamente de su estado presente. Comúnmente se usa para el análisis de sistemas reparables que pueden existir en múltiples estados y el uso de un análisis de confiabilidad de bloque sería inadecuado para analizar correctamente el sistema. El método se puede ampliar a sistemas más complejos utilizando procesos de Markov con orden superior y únicamente está restringido por el modelo, los cálculos matemáticos y las afirmaciones.

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

Aunque este análisis se puede realizar manualmente, la naturaleza de las técnicas permite el uso de programas de computación, muchos de los cuales existen en el mercado.

B.24.2 Uso

Esta técnica de análisis se puede usar en varias estructuras de sistemas, con o sin reparación, incluyendo:

- componentes independientes en paralelo;
- componentes independientes en serie;
- sistemas de carga compartida;
- sistema de espera, incluyendo el caso en donde puede ocurrir la falla de conmutación;
- sistemas degradados.

La técnica del análisis de *Markov* también se puede usar para calcular la disponibilidad, que incluye tomar en consideración los componentes de repuesto para las reparaciones.

B.24.3 Elementos de entrada

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

- lista de los diversos estados en los que se puede encontrar el sistema, subsistema o componente (por ejemplo totalmente operativo, operación parcial (es decir, un estado degradado), estado de falla, etc.);
- una comprensión clara de las transiciones posibles que es necesario modelar. por ejemplo, en la falla de la llanta de un carro es necesario considerar el estado de la rueda de repuesto y por lo tanto la frecuencia de inspección;
- la tasa de cambio de un estado a otro, representada comúnmente por una probabilidad de cambio entre los estados para eventos independientes, o la tasa de falla (λ) y/o la tasa de reparación (μ) para los eventos continuos.

B.24.4 Proceso

Esta técnica de análisis se centra alrededor del concepto de "estados", por ejemplo "disponible" y "en falla", y en la transición entre estos dos estados con el paso del tiempo que se basa en una probabilidad constante de cambio. Se utiliza una matriz de probabilidad transicional estocástica para describir la transición entre cada uno de los estados con el fin de permitir el cálculo de los diversos elementos de entrada.

Para ilustrar la técnica del análisis de *Markov*, consideremos un sistema complejo que solamente puede estar en tres estados: funcionamiento, degradado y en falla, definidos como S1, S2, S3 respectivamente. Cada día, el sistema existe en uno de estos tres estados. La Tabla B.2 ilustra la probabilidad de que mañana el sistema se encuentre en el estado Si, donde i puede ser 1, 2 o 3.

Tabla B.2. Matriz de *Markov*

		Estado hoy		
		S1	S2	S3
Estado 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 las probabilidades se denomina matriz de *Markov* o matriz de transición. Observe que la suma de cada columna es 1 dado que es la suma de todos los posibles resultados en cada caso. El sistema también se puede representar mediante un diagrama de Markov en donde los círculos representan los estados y las flechas representan la transición, junto con la probabilidad acompañante.

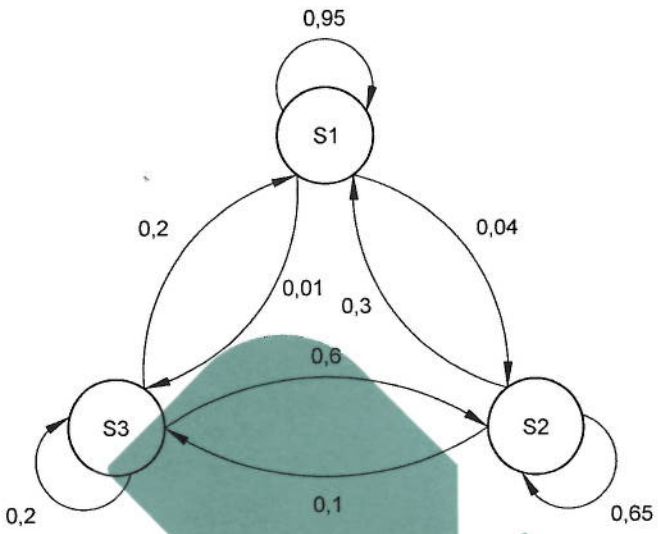


Figura B.9. Ejemplo del diagrama de *Markov* para el sistema

Las flechas que provienen de un estado y regresan a éste usualmente no se representan, pero se ilustran en estos ejemplos para qué estén completos.

Si Pi representa la probabilidad de encontrar el sistema en el estado i para i=1, 2, 3, entonces las ecuaciones simultáneas que se deben resolver son:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \qquad \text{(B.1)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \qquad \text{(B.2)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \qquad \text{(B.3)}$$

Estas tres ecuaciones no son independientes y no resolverán los tres valores desconocidos. La siguiente ecuación se debería utilizar y una de las anteriores se debería descartar.

$$1 = P1 + P2 + P3 \qquad \text{(B.4)}$$

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

Considere dos elementos que operan en paralelo con cualquiera de ellos que se requiere en operación para que el sistema funcione. Los elementos pueden estar en operación o en falla y la disponibilidad del sistema depende del estado de los elementos.

Los estados se pueden considerar como:

Estado 1 ambos elementos funcionan correctamente;

Estado 2 un elemento ha fallado y está en reparación, el otro está funcionando;

Estado 3 ambos elementos han fallado y uno está en reparación.

Si se asume que la tasa de falla continua para cada elemento es λ y la tasa de reparación es μ entonces el diagrama de la transición del estado es:

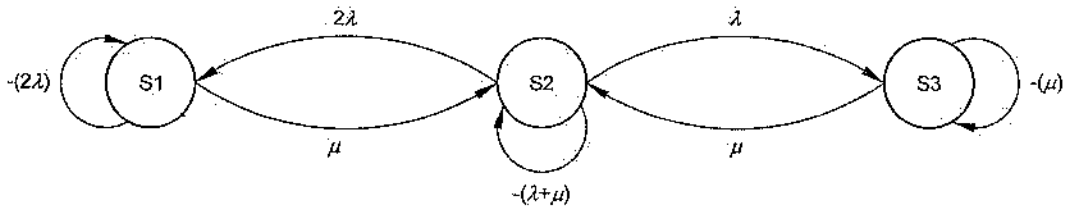


Figura B.10. Ejemplo de diagrama de transición del estado

Observe que la transición del estado 1 hasta el estado 2 es 2λ ya que la falla de cualquiera de los dos elementos llevará al sistema hasta el estado 2.

Si Pi (t) es la probabilidad de estar en un estado inicial i en el momento t, y

Si Pi (t + δt) es la probabilidad de estar en un estado final en el momento t + δt,

La matriz de probabilidad de transición es:

Tabla B.3. Matriz de *Markov* final

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

Es inútil que se presenten valores cero dado que no es posible pasar del estado 1 al estado 3 ni desde el estado 3 al estado 1. De igual modo, las columnas suman cero cuando se especifican las tasas.

Las ecuaciones simultáneas se convierten en:

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

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

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

En aras de la sencillez, se asumirá que la disponibilidad que se requiere es la disponibilidad de estado estable.

Cuando δt tiende al infinito, dPi/dt tendrá tendencia a ser cero y las ecuaciones se hacen más fáciles de resolver. También se debería utilizar la ecuación adicional que se ilustra en la ecuación (B.4):

Observe que la ecuación A(t) = P1(t) + P2(t) se puede expresar como:

$$A = P1 + P2$$

En consecuencia, $A = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 Elementos de salida

Los elementos de salida del análisis de *Markov* lo constituyen las diversas probabilidades de estar en diversos estados y, por lo tanto, una estimación de las probabilidades de falla y/o de disponibilidad, uno de los componentes esenciales de un sistema.

B.24.6 Fortalezas y limitaciones

Las fortalezas de un análisis de *Markov* incluyen:

- capacidad para calcular las probabilidades para sistemas con capacidad de reparación y múltiples estados degradados.

Las limitaciones de este análisis incluyen:

- asumir las probabilidades constantes de cambio del estado; sea falla o reparación;
- todos los eventos son estadísticamente independientes dado que los estados futuros son independientes de todos los estados pasados, excepto para el estado inmediatamente anterior;
- necesita del conocimiento de todas las probabilidades del cambio de estado;
- conocimiento de las operaciones de la matriz;
- los resultados son difíciles de comunicar al personal no técnico.

B.24.7 Comparaciones

El análisis de *Markov* es similar al análisis de redes de Petri por la capacidad de monitorear y observar los estados del sistema, aunque es diferente dado que las redes de Petri pueden existir en múltiples estados al mismo tiempo.

B.24.8 Documentos de referencia

IEC 61078, *Analysis Techniques for Dependability. Reliability Block Diagram and Boolean Methods.*

IEC 61165, *Application of Markov Techniques.*

ISO/IEC 15909 (todas las partes), *Software and Systems Engineering. High-Level Petri Nets.*

B.25 SIMULACIÓN DE MONTE CARLO

B.25.1 Información general

Muchos sistemas son demasiado complejos para modelar los efectos de la incertidumbre en ellos utilizando técnicas analíticas, pero se pueden evaluar considerando los elementos de entrada como variables aleatorias y realizando una cantidad N de cálculos (denominados simulaciones) mediante el muestreo del elemento de entrada con el fin de obtener N productos posibles del resultado deseado.

Este método puede abordar situaciones complejas que serían muy difíciles de comprender y solucionar mediante métodos analíticos. Se pueden desarrollar sistemas utilizando hojas de cálculo y otras herramientas convencionales, pero están a disposición herramientas más sofisticadas para ayudar con los requisitos complejos, muchas de las cuales actualmente no son costosas. Cuanto la técnicas se desarrolló, primero la cantidad de repeticiones necesarias para las simulaciones de Monte Carlo hacían que el proceso fuera lento y demorado, pero los progresos en los computadores y los desarrollos teóricos, por ejemplo el muestreo por hipercubo latino, han hecho que el tiempo de procesamiento sea casi insignificante para muchas aplicaciones.

B.25.2 Uso

Esta simulación suministra medios para evaluar el efecto de la incertidumbre en los sistemas para un rango amplio de situaciones. Típicamente se utiliza para evaluar el rango de resultados posibles y la frecuencia relativa de los valores en ese rango para mediciones cuantitativas de un sistema tales como costo, duración, rendimiento, demanda y mediciones similares. Esta simulación se puede utilizar con dos propósitos diferentes:

- propagación de la incertidumbre en modelos analíticos convencionales;
- cálculos probabilísticos cuando las técnicas analíticas no funcionan.

B.25.3 Elementos de entrada

El elemento de entrada para una simulación de Monte Carlo es un buen modelo del sistema e información sobre los tipos de elementos de entrada, las fuentes de incertidumbre que se van a representar y el elemento de salida que se requiere. Los datos de entrada con incertidumbre se representan como variables aleatorias con distribuciones que están más o menos dispersas de acuerdo con el nivel de incertidumbre. Distribuciones uniformes, triangulares, normales y normales logarítmicas se utilizan con frecuencia para este fin.

B.25.4 Proceso

El proceso es el siguiente:

a) Se define un modelo o un algoritmo que representa lo más estrechamente posible al comportamiento del sistema que se está estudiando.

b) El modelo se ejecuta varias veces utilizando números aleatorios para producir elementos de salida del modelo (simulaciones del sistema); cuando la aplicación es para modelar los efectos de la incertidumbre, el modelo está en forma de ecuación que suministra las relaciones entre los parámetros de entrada y un elemento de salida. Los valores seleccionados para los elementos de entrada se toman de las distribuciones adecuadas de la probabilidad que representan la naturaleza de la incertidumbre en estos parámetros.

c) En cualquier caso un computador ejecuta el modelo varias veces (con frecuencia hasta 10 000 veces) con diferentes elementos de entrada y produce elementos de salida múltiples. Éstos se pueden procesar utilizando estadísticas convencionales para obtener información sobre, por ejemplo, valores promedio, desviación estándar, intervalos de confianza.

A continuación se presenta un ejemplo de simulación.

Consideremos el caso de dos elementos que funcionan en paralelo y únicamente se requiere de uno de ellos para que el sistema funcione. El primer elemento tiene una confiabilidad de 0,9 y el otro de 0,8.

Es posible elaborar una hoja de cálculo con las siguientes columnas.

Tabla B.4. Ejemplo de una simulación de Monte Carlo

	Elemento 1		Elemento 2		
Número de simulación	Número aleatorio	¿Funciona?	Número aleatorio	¿Funciona?	Sistema
1	0,577 243	SI	0,059 355	SI	1
2	0,746 909	SI	0,311 324	SI	1
3	0,541 728	SI	0,919 765	NO	1
4	0,423 274	SI	0,643 514	SI	1
5	0,917 776	NO	0,539 349	SI	1
6	0,994 043	NO	0,972 506	NO	0
7	0,082 574	SI	0,950 241	NO	1
8	0,661 418	SI	0,919 868	NO	1
9	0,213 376	SI	0,367 555	SI	1
10	0,565 657	SI	0,119 215	SI	1

El generador aleatorio crea un número entre 0 y 1 que se utiliza para comparar con la probabilidad de cada elemento para determinar si el sistema es operativo. Con sólo 10 ejecuciones, no se debería esperar que el resultado de 0,9 fuera exacto. El enfoque usual es incluir una calculadora para comparar el resultado total a medida que la simulación progresa para alcanzar el nivel de exactitud que se requiere. En este ejemplo, el resultado de 0,9799 se logró después de 20 000 repeticiones.

El modelo anterior se puede ampliar de varios modos. Por ejemplo:

- ampliando el modelo mismo (por ejemplo considerar que el segundo elemento se convierte inmediatamente en operativo sólo cuando falla el primer elemento);
- cambiando la probabilidad fija para una variable (un buen ejemplo es la distribución triangular) cuando la probabilidad no se puede definir con exactitud;
- utilizando tasas de falla combinadas con los aleatorios para derivar un tiempo de falla (exponencial, *Weibull*, otra distribución adecuada) e integrando tiempos de reparación.

Las aplicaciones incluyen, entre otras cosas, la valoración de la incertidumbre en previsiones financieras, desempeño de inversión, costo de proyectos y previsiones de programación, interrupciones del proceso de la empresa y requisitos de dotación del personal.

Las técnicas analíticas no pueden brindar resultados pertinentes o cuando existe incertidumbre en los datos de los elementos de entrada y por lo tanto en los elementos de salida.

B.25.5 Elementos de salida

El elemento de salida podría ser un solo valor, determinado tal como se indicó en el ejemplo anterior, podría ser un resultado expresado como la distribución de la probabilidad o la frecuencia, o podría ser la identificación de las funciones principales dentro del modelo que tienen el impacto máximo en el elemento de salida.

En general, una simulación de Monte Carlo se utilizará para evaluar la distribución total de los resultados que se podrían originar o las medidas clave provenientes de la distribución como por ejemplo:

- la probabilidad de que se produzca un resultado definido;
- el valor de un resultado en el cual los propietarios del problema tienen un nivel determinado de confianza de que éste no se excederá ni superará, un costo que tiene menos del 10 % de probabilidad de excederse o una duración con el 80 % de certeza de ser excedida.

Un análisis de las relaciones entre los elementos de entrada y los de salida puede aclarar la importancia relativa de los factores en funcionamiento e identificar los objetos de esfuerzo útiles para influir la incertidumbre en el resultado.

B.25.6 Fortalezas y limitaciones

Las fortalezas de este análisis incluyen las siguientes:

- el método puede, en principio acomodarse a cualquier distribución en una variable de entrada, incluyendo las distribuciones empíricas derivadas de observaciones de sistemas relacionados;
- los modelos son relativamente sencillos de desarrollar y se pueden ampliar a medida que se originan las necesidades;
- se pueden representar todas las influencias o las relaciones que se originan en la realidad, incluyendo los efectos sutiles tales como las dependencias condicionales;
- se puede aplicar el análisis de sensibilidad para identificar influencias fuertes y débiles;
- los modelos se pueden entender con facilidad ya que la relación entre las entradas y las salidas es transparente;
- se dispone de modelos de comportamiento eficientes como las redes de Petri (norma IEC 62551 futura) que han probado ser eficientes para los propósitos de la simulación de Monte Carlo;
- proporciona una medición de la exactitud de un resultado;
- el software es de fácil adquisición y relativamente barato.

Las limitaciones son las siguientes:

- la exactitud de las soluciones depende de la cantidad de simulaciones que se pueda realizar (esta limitación se hace menos importante con el incremento en las velocidades de los computadores);
- depende de su capacidad de representar las incertidumbres en parámetros mediante una distribución válida;
- los modelos grandes y complejos pueden ser un reto para quienes elaboran el modelo dificultar la participación de las partes involucradas en el proceso;

- la técnica puede no ponderar adecuadamente eventos de consecuencia alta/probabilidad baja y, por lo tanto no permite que el análisis refleje la apetencia de la organización por el riesgo.

B.25.7 Documentos de referencia

IEC 61649, *Weibull Analysis.*

IEC 61551, *Analysis Techniques for Dependability. Petri Net Techniques*[1]

ISO/IEC *Guide 98-3:208, Uncertainty Measurement. Part 3: Guide to the of Uncertainty Measurement (GUM1995).*

B.26 ESTADÍSTICA BAYESIANA Y REDES DE BAYES

B.26.1 Información general

Este tipo de estadísticas se atribuye al reverendo Thomas Bayes. Su premisa es que toda información ya conocida (la previa) se puede combinar con la medición posterior (la posterior) para establecer una probabilidad global. La expresión general del teorema de Bayes puede ser:

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

en donde

La probabilidad de X se denomina P (X);

La probabilidad de X con la condición de que Y haya ocurrido se denomina P (X | Y); y E_i es el iésimo evento.

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

La estadística bayesiana difiere de la estadística clásica en que no asume que todos los parámetros de distribución son fijos, sino que los parámetros son variables aleatorias. Se puede comprender más fácil una probabilidad bayesiana si se considera como el grado de convicción de una persona en un evento determinado en oposición a lo clásico que se basa en evidencia física. Dado que el enfoque bayesiano se basa en la interpretación subjetiva de la probabilidad, suministra una base fácil para el pensamiento decisivo y el desarrollo de redes bayesianas (o redes de convicción, redes de trabajo de convicción o redes bayesianas).

Las redes de Bayes utilizan un modelo clásico para representar un conjunto de variables y sus relaciones probabilísticas. La red está compuesta de nodos que representan una variable aleatoria y flechas que unen un nodo primario con un nodo secundario (en donde un nodo primario es una variable que influye directamente en otra variable (secundaria).

B.26.2 Uso

En años recientes, la utilización de la teoría y las redes de Bayes se ha dispersado en parte debido a su atractivo intuitivo y también por la disponibilidad de herramientas de cómputo de software. Las redes de Bayes se han utilizado en una amplia variedad de temas: diagnóstico médico, modelado de imágenes, genética, reconocimiento del habla, economía, exploración espacial y en los potentes motores de búsqueda de la red que se utilizan hoy en día. Éstas pueden ser útiles en un área en la que existe el requisito de determinar variables a través de la

[1] Actualmente en estudio.

utilización de relaciones y datos estructurales. Las redes de Bayes se pueden utilizar p aprender las relaciones causales con el fin de obtener la comprensión acerca del dominio problema y predecir las consecuencias de la intervención.

B.26.3 Elementos de entrada

Las entradas son similares a las del modelo de Monte Carlo. Para una red de Bayes, ejemplos de los pasos a seguir incluyen los siguientes:

- definir las variables del sistema;
- definir los vínculos causales entre las variables;
- especificar las probabilidades condicionales y previas;
- añadir la evidencia a la red;
- realizar la actualización de las convicciones;
- extraer las convicciones posteriores.

B.26.4 Proceso

La teoría de Bayes se puede aplicar en una amplia variedad de modos. Este ejen considerará la creación de una Tabla de Bayes en la que se utiliza un ensayo médico p determinar si el paciente tiene una enfermedad. La convicción antes de realizar el ensayo que el 99 % de la población no tiene esta enfermedad y el 1 % si la tiene, es deci información previa. La exactitud del ensayo ha mostrado que si la persona tiene la enferme el resultado del ensayo es positivo el 98 % de las veces. También existe una probabilidad que si usted no tiene la enfermedad, el resultado del ensayo es positivo el 10 % de las ve La Tabla de Bayes suministra la siguiente información:

Tabla B.5. Datos de la tabla de Bayes

	Previa	Probabilidad	Producto	Posterior
Tiene la enfermedad	0,01	0,98	0,009 8	0,090 1
Sin enfermedad	0,99	0,10	0,099 0	0,909 9
Sumas	1		0,108 8	1

Utilizando la regla de Bayes, el producto se determina combinando la información previa probabilidad. La información posterior se determina dividiendo el valor del producto por el del producto. El elemento de salida muestra que un resultado de ensayo positivo indica qu información previa se ha incrementado de 1 % a 9 %. Más significativamente, existe oportunidad fuerte de que incluso con un ensayo positivo, tener la enfermedad sea improba Al examinar la ecuación (0,01 x 0,98)/((0,01 x 0,98)+(0,99 x 0,1)) muestra que el valor "resultado positivo-sin enfermedad" tiene un papel importante en los valores posteriores.

Consideremos la siguiente red de Bayes:

UNIVERSIDAD MILITAR
NUEVA GRANADA
BIBLIOTECA

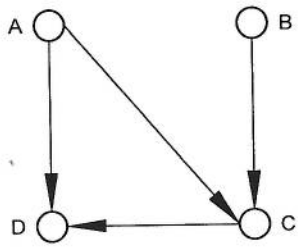


Figura B.11. Muestra de una red de Bayes

Con las probabilidades condicionales previas definidas en las siguientes tablas y utilizando la anotación de que Y indica positivo y N implica negativo, lo positivo podría ser "tener la enfermedad" como se indicó anteriormente, o podría ser alta y N podría ser baja.

Tabla B.6. Probabilidades previas para los nodos 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 nodo C con los nodos A y 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 nodo D con los nodos A y 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 $P(A \mid D=N, C=Y)$, es necesario calcular primero $P(A,B \mid D=N, C=Y)$.

Utilizando la regla de Bayes, se determina el valor $P(D \mid A,C)P(C \mid A,B)P(A)P(B)$ como se indica a continuación y la última columna muestra las probabilidades normalizadas que suman 1 derivadas del ejemplo anterior (resultados redondeados)

Tabla B.9. Probabilidad posterior para los nodos A y B con los nodos D y 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 x 0,5 x 0,9 x 0,6 = 0,110	0,4
Y	N	0,4 x 0,9 x 0,9 x 0,4 = 0,130	0,48
N	Y	0,8 x 0,2 x 0,1 x 0,6 = 0,010	0,04
N	N	0,8 x 0,7 x 0,1 x 0,4 = 0,022	0,08

Para derivar P (A| D=N, C=Y), es necesario sumar todos los valores de B.

Tabla B.10. Probabilidad posterior para el nodo A con los nodos D y C definidos

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

Esto demuestra que el valor previo para P (A=N) se ha incrementado de 0,1 hasta un valo posterior de 0,12 que constituye sólo un cambio pequeño. Por otra parte P(B=N| D=N, C=Y) h cambiado desde 0,4 hasta 0,56, el cual es un cambio más significativo.

B.26.5 Elementos de salida

El enfoque bayesiano se puede aplicar en la misma extensión que la estadística clásica con u amplio rango de elementos de salida, por ejemplo al análisis de datos para derivar estimadore puntuales e intervalos de confianza. Su popularidad reciente se da en relación con las redes d Bayes para derivar distribuciones posteriores. La salida gráfica proporciona un modelo de fá comprensión y los datos se pueden modificar fácilmente para considerar las correlaciones y sensibilidad de los parámetros.

B.26.6 Fortalezas y limitaciones

Fortalezas:

- todo lo que se necesita es el conocimiento de los valores previos;
- las declaraciones de inferencia se entienden fácilmente;
- la regla de Bayes es todo lo que se requiere;
- proporciona un mecanismo para utilizar convicciones subjetivas en un problema.

Limitaciones:

- definir todas las interacciones en las redes de Bayes para sistemas complejos problemático;
- el enfoque bayesiano necesita del conocimiento de una multitud de probabilidad condicionales que generalmente son proporcionadas por el juicio de expertos. L herramientas de software únicamente pueden suministrar respuestas con base en est presunciones.

B.27 CURVAS FN

B.27.1 Información general

Las curvas FN son representaciones gráficas de la probabilidad de los eventos que causan nivel específico de daño a una población específica. Más a menudo se refieren a la frecuen de ocurrencia de una cantidad determinada de casualidades.

Las curvas FN muestra la frecuencia acumulativa (F) con la cual N o más miembros de población se verán afectados. Valores altos de N que se podrían presentar con frecuencia alta son de interés significativo porque suelen ser social y políticamente inaceptables.

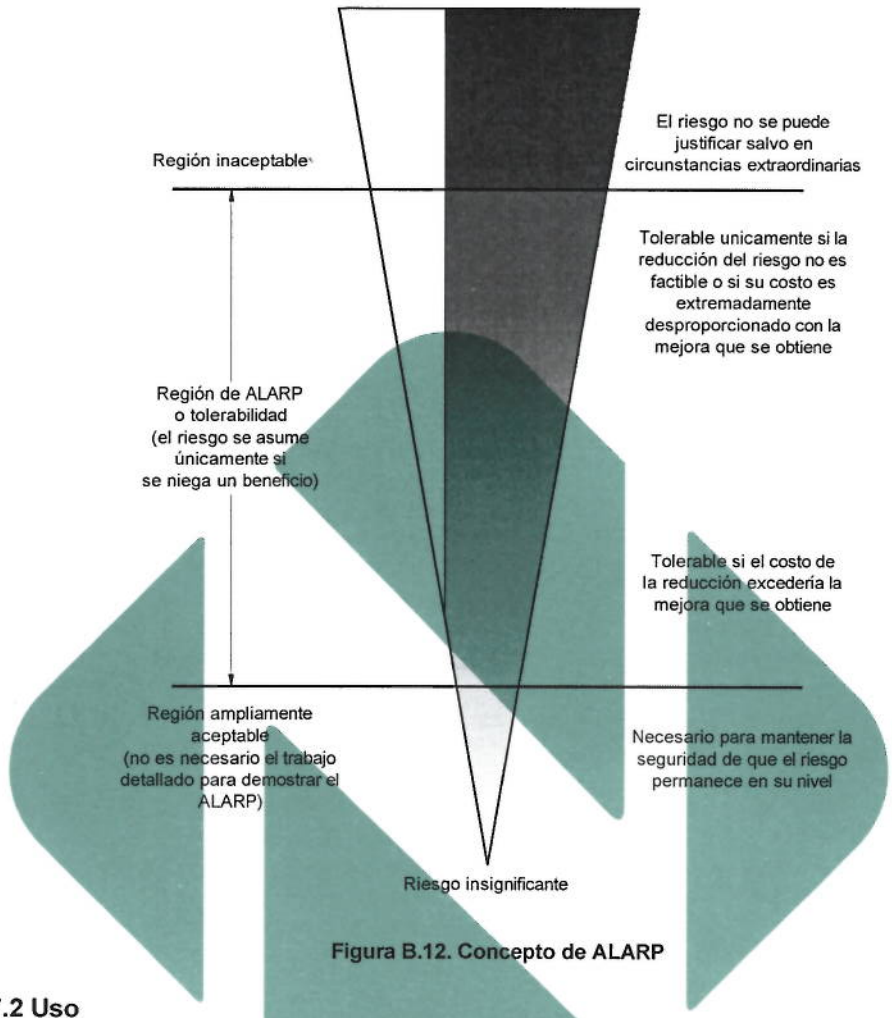


Figura B.12. Concepto de ALARP

B.27.2 Uso

Estas curvas son un modo de representar los elementos de salida del análisis del riesgo. Muchos eventos tienen una probabilidad alta de un resultado con consecuencia baja y una probabilidad baja de un resultado con una consecuencia alta. Las curvas brindan una representación del nivel del riesgo que es una línea que describe este rango más que un solo punto que representa un par de probabilidad y consecuencia.

Estas curvas se pueden utilizar para comparar riesgos, por ejemplo para comparar los riesgos predichos frente a los criterios definidos como una curva FN, o para comparar los riesgos predichos con los datos de incidentes históricos, o con criterios de decisión (también se expresa como curva F/N).

Estas curvas se pueden utilizar para diseño de sistemas o procesos o para la gestión de los sistemas existentes.

B.27.3 Elementos de entrada

Las entradas son:

- conjuntos de pares de consecuencia y probabilidad en un periodo de tiemp determinado;

- la salida de datos de un análisis de riesgo cuantitativo que suministra probabilidade estimadas para las cantidades específicas de casualidades;

- datos provenientes tanto de los registros como del análisis de riesgo cuantitativo.

B.27.4 Proceso

Los datos disponibles se registran en una gráfica con la cantidad de casualidades (para u nivel específico de daño, es decir la muerte) formando la abscisa con la probabilidad de N más casualidades conformando la ordenada. Debido al gran rango de valores, ambos ejes s encuentran normalmente en escala logarítmica.

Las curvas FN se pueden elaborar estadísticamente utilizando números "reales" proveniente de pérdidas pasadas o se pueden calcular a partir de estimaciones de modelos de simulació Los datos utilizados y las presunciones hechas pueden implicar que estos dos tipos de curv FN suministran información diferente y se deberían utilizar independientemente y para fine diferentes. En general, las curvas FN teóricas son más útiles para la gestión de un sistem existente en particular.

Ambos enfoques de derivación pueden consumir mucho tiempo de modo que es común utiliz una mezcla de ambos. Los datos empíricos formarán puntos fijos con casualidades conocida con precisión que ocurren en accidentes/incidentes conocidos en un periodo específico d tiempo, y el análisis de riesgo cuantitativo que suministra otros puntos por extrapolación interpolación.

La necesidad de considerar accidentes de frecuencia baja y consecuencia alta puede requer de la consideración de periodos largos de tiempo para reunir datos suficientes para un anális correcto. Esto a su vez puede hacer que los datos disponibles sean sospechosos, si lo eventos desencadenantes cambian con el paso del tiempo.

B.27.5 Elementos de salida

Una línea que representa el riesgo a través de un rango de valores de consecuencias que s pueden comparar con los criterios que son adecuados para la población que se est estudiando y el nivel específico de daño.

B.27.6 Fortalezas y limitaciones

Las curvas FN son una manera útil de representar la información del riesgo que pueden utiliz los gerentes y los diseñadores del sistema para ayudar a tomar decisiones acerca del riesgo los niveles de seguridad. Son útiles para presentar información tanto sobre la frecuencia com la consecuencia en un formato accesible.

Estas curvas son adecuadas para la comparación de riesgos provenientes de situacione similares cuando se dispone de datos suficientes. No se deberían utilizar para compara riesgos de tipo diferente con características variables en circunstancias en que la cantidad y l calidad de datos varían.

Una limitación de estas curvas es que no dicen nada acerca del rango de efectos o de los resultados de los incidentes sino el número de personas impactadas, y no hay forma de identificar las diferentes maneras en que puede ocurrir el nivel de daño. Estas curvas

representan un tipo de consecuencia particular, usualmente el daño para las personas. Las curvas FN no constituyen un método para la valoración del riesgo sino una manera de representar los resultados de dicha valoración.

Estas curvas constituyen un método bien establecido para presentar los resultados de la valoración del riesgo pero exigen preparación de analistas con habilidades, y a menudo su interpretación y la valoración por parte de no especialistas es difícil.

B.28 ÍNDICES DE RIESGO

B.28.1 Información general

Un índice de riesgo es una medición semicuantitativa del riesgo, la cual es una estimación derivada utilizando un enfoque de puntaje usando escalas ordinarias. Los índices de riesgo se pueden utilizar para calificar una serie de riesgos utilizando criterios similares de manera que se puedan comparar. Los puntajes se aplican a cada componente del riesgo, por ejemplo las características contaminantes (fuentes), el rango de las posibles trayectorias de exposición y el impacto en los receptores.

Los índices de riesgo esencialmente son un enfoque cualitativo para calificar y comparar los riesgos. Aunque se utilizan números, esto es simplemente para permitir la manipulación. En muchos casos, cuando el sistema o el modelo subyacente no se conocen bien o no se puede representar, es mejor utilizar un enfoque cualitativo más abiertamente.

B.28.2 Uso

Los índices se pueden utilizar para clasificar diversos riesgos asociados con una actividad si el sistema se comprende bien. Permiten la integración de un rango de factores que tienen impacto en el nivel de riesgo en un puntaje numérico sencillo para el nivel de riesgo.

Los índices se usan para muchos tipos de riesgo, usualmente como un dispositivo para delimitar el alcance con el fin de clasificar el riesgo de acuerdo con el nivel de riesgo. Esto se puede utilizar para determinar cuáles riesgos necesitan valoración profunda y posiblemente cuantitativa.

B.28.3 Elementos de entrada

Los elementos de entrada se derivan del análisis del sistema, o de una descripción amplia del contexto. Esto exige una buena comprensión de todas las fuentes de riesgo, las trayectorias posibles y de aquello que se podría ver afectado. Se pueden utilizar herramientas como el análisis de árbol de fallas, el análisis de árbol de eventos y el análisis de decisión general para dar soporte al desarrollo de los índices de riesgo.

Dado que la elección de escalas ordinales es, en algún grado, arbitraria, se necesitan datos suficientes para validar el índice.

B.28.4 Proceso

El primer paso es comprender y describir el sistema. Una vez que el sistema ha sido definido, se desarrollan puntajes para cada componente de modo que se puedan combinar para obtener un índice compuesto. Por ejemplo, en un contexto ambiental, las fuentes, la trayectoria y los receptores tendrán un puntaje, observando que en algunos casos puede haber trayectorias y receptores múltiples para cada fuente. Los puntajes individuales se combinan de acuerdo con

un esquema que toma en consideración las realidades físicas del sistema. Es importante los puntajes para cada parte del sistema (fuentes, trayectorias y receptores) sean consiste internamente y mantengan sus relaciones correctas. Los puntajes se pueden suministrar componentes del riesgo (por ejemplo probabilidad, exposición, consecuencia) o para fact que incrementan el riesgo.

Los puntajes se pueden sumar, restar, multiplicar y/o dividir de acuerdo con este model alto nivel. Los efectos acumulativos se pueden tener en cuenta mediante la suma de puntajes (por ejemplo sumando los puntajes de diferentes trayectorias). Es estrictament válido aplicar fórmulas matemáticas a las escalas ordinales. Por lo tanto, una vez se desarrollado el sistema de puntaje, el modelo se debería validar aplicándolo a un sist conocido. El desarrollo de un índice es un enfoque reiterativo y se puede probar va sistemas diferentes para combinar los puntajes antes de que el analista este cómodo co validación.

La incertidumbre se puede abordar mediante el análisis de sensibilidad y variando los punt para determinar cuáles parámetros son los más sensibles.

B.28.5 Elementos de salida

El elemento de salida es una serie de números (índices combinados) que se relacionan una fuente particular y que se pueden comparar con índices desarrollados para otras fue dentro del mismo sistema o que se pueden modelar de la misma manera.

B.28.6 Fortalezas y limitaciones

Fortalezas:

- los índices puede suministrar una buena herramienta para calificar riesgos diferentes
- permiten la incorporación de factores múltiples que afectan al nivel del riesgo en un puntaje para dicho nivel.

Limitaciones:

- si el proceso (modelo) y su elemento de salida no se validan bien, los resulta pueden no tener ningún significado. El hecho de que el elemento de salida es un v numérico para el riesgo puede ser mal interpretado y mal utilizado, por ejemplo en análisis posteriores de costo y beneficio;
- en muchas situaciones en las que se usan los índices, no hay un modelo fundame para definir si las escalas individuales para los factores de riesgo son linea logarítmicas o tienen otra forma, ni algún modelo para definir la manera en que deberían combinar los factores. En estas situaciones, el puntaje es por naturaleza confiable y la validación frente a datos reales es particularmente importante.

B.29 MATRIZ DE CONSECUENCIA Y PROBABILIDAD

B.29.1 Información general

Esta matriz es un medio de combinar calificaciones cualitativas y semicuantitativas de consecuencias y las probabilidades para producir un nivel de riesgo o una calificación riesgo.

El formato de la matriz y las definiciones que se le aplican dependen del contexto en el cual se utiliza y es importante que se utilice un diseño adecuado para las circunstancias.

B.29.2 Uso

Una matriz de consecuencias y probabilidad se utiliza para calificar riesgos, fuentes de riesgo o tratamientos para el riesgo con base en el nivel de riesgo. Comúnmente se utiliza como una herramienta de clasificación cuando se han identificado muchos riesgos, por ejemplo para definir cuáles riesgos necesitan mayor análisis o análisis más detallado, cuáles riesgos necesitan primero el tratamiento o cuáles necesitan revisión a un nivel superior de gestión. También se puede utilizar para seleccionar los riesgos que no necesitan consideración adicional en este momento. Este tipo de matriz de riesgo también se usa ampliamente para determinar si un riesgo determinado es aceptable en forma amplia o no es aceptable (véase el numeral 5.4), de acuerdo con la zona en donde se localiza en la matriz.

Esta matriz también se puede utilizar para ayudar a comunicar una comprensión común de los niveles cualitativos de los riesgos en toda la organización. La forma en que se establecen los niveles de riesgo y se asignan las reglas de decisión a estos niveles debería concordar con la apetencia de la organización con respecto al riesgo.

Una forma de matriz de consecuencia y probabilidad se utiliza para el análisis de criticidad en el AMEFC o para establecer las prioridades después de un análisis EPO. Se puede utilizar en situaciones en que existen datos insuficientes para el análisis detallado o en situaciones que no ameritan el tiempo y el esfuerzo de un análisis cuantitativo.

B.29.3 Elementos de entrada

Los elementos de entrada para el proceso son escalas adaptadas para la consecuencia y la probabilidad y una matriz que combina estos dos factores.

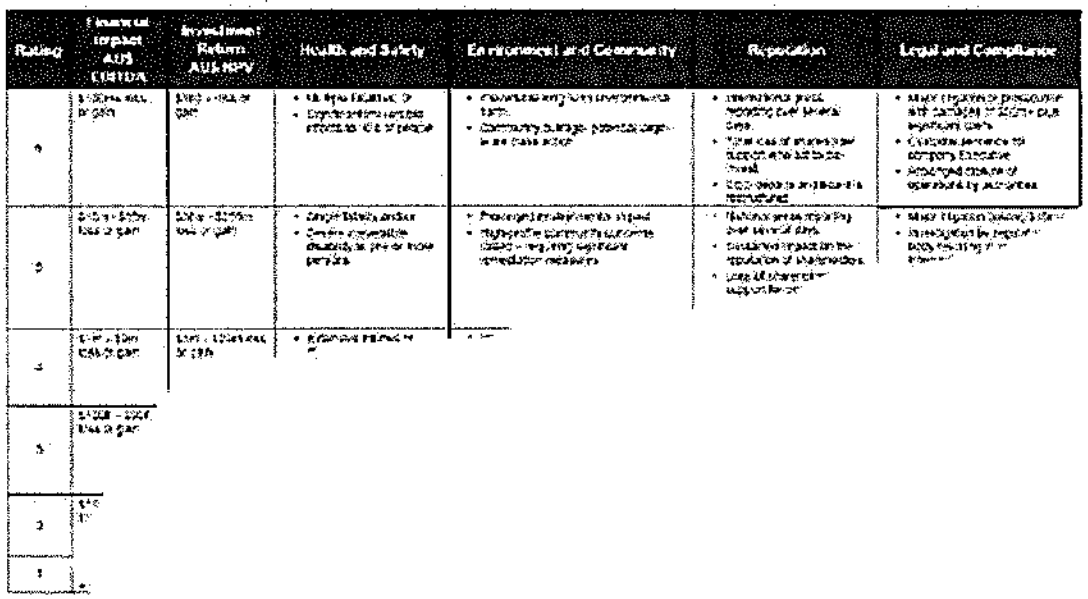
La escala (o escalas) de consecuencia deberían cubrir el rango de tipos diferentes de consecuencias que se han de considerar (por ejemplo: pérdida financiera, seguridad, ambientes u otros parámetros, dependiendo del contexto) y se deberían extender desde la consecuencia máxima creíble hasta la consecuencia de interés mínimo. La Figura B.6 ilustra parte de un ejemplo.

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

La escala de probabilidad también puede tener cualquier cantidad de puntos. Es necesario que las definiciones de la probabilidad se seleccionen de manera tal que, en la medida de lo posible, no sean ambiguas. Si se utilizan guías numéricas para definir las diversas probabilidades, entonces se deberían suministrar las unidades. Es necesario que la escala de probabilidad cubra el rango pertinente para el estudio en cuestión, recordando que la probabilidad mínima debe ser aceptable para la máxima consecuencia definida, de lo contrario todas las actividades con la consecuencia máxima se definen como intolerables. En la Figura B.7 se ilustra parte de un ejemplo.

Una matriz se dibuja con la consecuencia en un eje y la probabilidad en el otro. La Figura B.8 muestra parte de un ejemplo de matriz con escalas de 6 puntos de consecuencia y de 5 puntos de probabilidad.

Los niveles de riesgo asignados a las celdas dependerán de las definiciones para las escalas de probabilidad y consecuencia. La matriz se puede establecer para obtener ponderación adicional de las consecuencias (tal como se ilustra) o de la probabilidad, o puede ser simétrica dependiendo de la aplicación. Los niveles de riesgo se pueden vincular a las reglas de decisión, como por ejemplo al nivel de atención de la gerencia o la escala de tiempo durante la cual se necesita la respuesta.



Calificación	Impacto financiero	Rendimiento de la inversión	Salud y seguridad	Ambiente y comunidad	Reputación	Legalidad y cumplimiento
6	$ 100 m + pérdida o ganancia	$ 300 m + pérdida o ganancia	Múltiples fatalidades o efectos importantes irreversibles para el 10 % de las personas	Daño irreversible en el ambiente a largo plazo. Indignación de la comunidad -- acción potencial con clase de gran escala	Información de la prensa internacional durante varios días. Pérdida total del apoyo de los accionistas que actúan para no invertir. Salida del jefe ejecutivo y reestructuración de la junta.	Litigio máximo con daños de$50m + más costos significativos. Sentencia de custodia para el ejecutivo de la compañía. Se sé prolongado de operaciones ordenado por las autoridades.
5	$ 10 m +$99m pérdida o ganancia	$30m +$299m pérdida o ganancia	Una sola fatalidad y/o Incapacidad grave irreversible para una o más personas	Impacto ambiental prolongado, Se originan preocupación es de alto perfil en la comunidad – se requieren medidas remediales significativas	Información de la prensa nacional durante varios días, Impacto sostenido en la reputación de los accionistas. Pérdida del apoyo de los accionistas ...	Liquidación mayor con un costo de $10m + Investigación por parte de los clientes reguladores ...
4	$1m +$9m pérdida o ganancia	$3m +$29m pérdida o ganancia	Lesiones extensas o			

Figura B.13. Parte de un ejemplo de una tabla de criterios de consecuencia

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distin - could occur within "mon
Unlikely	- may occur but not - could occur in "y
Rare	- occurrence re - exceptional' - only occ
Remote	- theor - fr

Figura B.14. Parte de un ejemplo del ranking de una matrix de riesgo

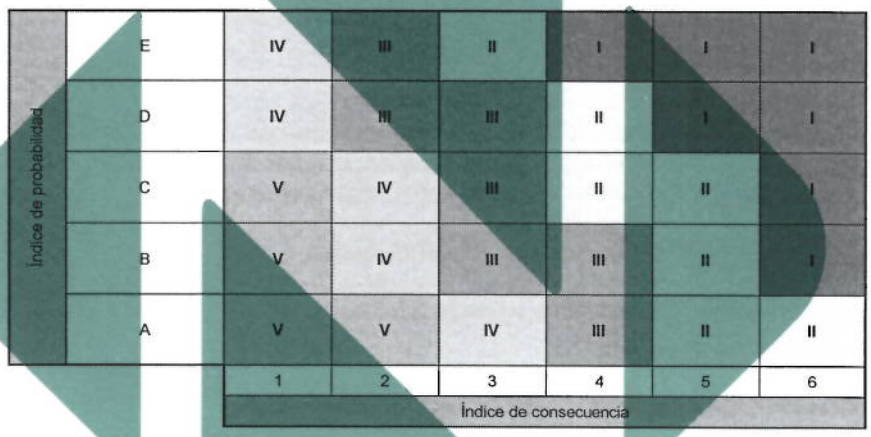


Figura B.15. Parte de ejemplo de una matriz de criterios para la probabilidad

Se pueden establecer escalas de calificación y una matriz con escalas cuantitativas. Por ejemplo, en un contexto de confiabilidad, la escala de probabilidad podría representar tasas de falla indicativas y la escala de consecuencia el costo de la falla en dólares.

La utilización de la herramienta necesita de personas (idealmente un equipo) con la experticia pertinente y los datos que estén disponibles para ayudar en el juzgamiento de la consecuencia y la probabilidad.

B.29.4 Proceso

Para calificar los riesgos, el usuario encuentra primero el descriptor de la consecuencia que mejor se ajuste a la situación, luego define la probabilidad con la cual ocurrirán tales consecuencias. El nivel de riesgo se determina entonces a partir de la matriz.

Muchos eventos de riesgo pueden tener un rango de resultados con diferentes probabilidades asociadas. Generalmente, los problemas menores son más comunes que las catástrofes. Por lo tanto, existe la elección de si calificar el resultado más común o el más grave, o alguna otra combinación. En muchos casos, es adecuado enfatizar los resultados factibles más graves ya

que éstos imponen la amenaza máxima y mayor preocupación. En algunos casos, puede s adecuado calificar tanto los problemas comunes como las catástrofes improbables cor riesgos independientes. Es importante utilizar la probabilidad pertinente para la consecuenc seleccionada y no la probabilidad del evento como un todo.

El nivel de riesgo definido por la matriz puede está asociado con la regla de decisión sobre tratar o no el riesgo.

B.29.5 Elemento de salida

El elemento de salida es una calificación para cada riesgo o la definición de una lista calificac de los riesgos con los niveles de importancia.

B.29.6 Fortalezas y limitaciones

Fortalezas:

- relativamente fácil de utilizar,
- proporciona una calificación rápida de los riesgos en diferentes niveles de importancia.

Limitaciones:

- la matriz se debe diseñar de manera que sea adecuada para las circunstancias, c modo que puede ser difícil aplicar un sistema común a través de un rango c circunstancias pertinentes para una organización;
- es difícil definir las escalas sin ambigüedad;
- el uso es muy subjetivo y tiende a haber variación significativa entre quienes califican;
- los riesgos no se pueden acumular (es decir, uno no puede definir que un núme particular de riesgos bajos o un riesgo bajo identificado una cantidad de veces e particular sea equivalente a un riesgo medio);
- es difícil combinar o comparar el nivel de riesgo para diversas categorías d consecuencias.

Los resultados dependerán del nivel de detalle del análisis, es decir, cuanto más detallado se el análisis mayor cantidad de escenarios, cada uno de ellos con probabilidad menor. Est hecho subestimará el nivel real del riesgo. La manera en que se agrupan los escenarios a describir el riesgo debería ser consistente y estar definida al comienzo del estudio.

B.30 ANÁLISIS DE COSTO-BENEFICIO

B.30.1 Información general

Este análisis se puede utilizar para la evaluación del riesgo cuando el costo total esperado s pondera en comparación con los beneficios totales esperados con el fin de elegir la mejc opción o la más rentable. Es una parte implícita de muchos sistemas de evaluación del riesgc Puede ser cualitativa o cuantitativa, o involucrar una combinación de elementos cuantitativos cualitativos. El análisis de costo-beneficio cuantitativo agrega el valor monetario de todos lo costos y todos los beneficios para las partes involucradas incluidas en el alcance y ajust

diferentes periodos de tiempo en los cuales se acumulan los costos y los beneficios. El valor presente neto (VPN) que se produce se convierte en un elemento de entrada para las decisiones acerca del riesgo.

Un VPN positivo asociado con una acción normalmente implicaría que la acción debería ocurrir. Sin embargo, para riesgos negativos, en particular aquellos que implican riesgos para la vida humana o daño para el ambiente se puede aplicar el principio ALARP. Este divide los riesgos en tres regiones: el nivel superior en el cual los riesgos negativos son intolerables y no se deberían asumir, excepto en circunstancias extraordinarias, el nivel inferior en el cual los riesgos son insignificantes y sólo es necesario monitorearlos para garantizar que permanecen en nivel bajo; y la banda central en donde los riesgos se hacen tan bajos como sea razonablemente factible. Hacia el extremo de riesgo inferior en esta región, se puede aplicar un análisis de costo y beneficio estricto, pero cuando los riesgos se acercan a ser intolerables, la expectativa del principio ALARP es que el tratamiento se producirá a menos que los costos del tratamiento sean significativamente desproporcionados con respecto al beneficio que se obtiene.

B.30.2 Uso

El análisis de costo y beneficio se puede utilizar para decidir entre opciones que implican riesgo.

Por ejemplo:

- como elemento de entrada para una decisión acerca de si el riesgo se debería tratar,
- para diferenciar entre las formas de tratamiento del riesgo y decidir sobre la mejor,
- decidir entre diferentes cursos de acción.

B.30.3 Elementos de entrada

Los elementos de entrada incluyen la información sobre los costos y los beneficios para las partes involucradas pertinentes y sobre las incertidumbres de tales costos y beneficios. Se deberían considerar los costos y los beneficios tangibles e intangibles. Los costos incluyen los recursos agotados y los resultados negativos, los beneficios incluyen los resultados positivos, los resultados negativos que se evitaron y los recursos que se ahorraron.

B.30.4 Proceso

Se identifican las partes involucradas que pueden experimentar los costos o recibir los beneficios. En un análisis completo de los beneficios se incluye a todas las partes involucradas.

Se identifican los beneficios y los costos directos e indirectos de las opciones que se consideran para todas las partes involucradas pertinentes. Los beneficios directos son aquellos que fluyen directamente debido a la acción que se emprendió, mientras que los beneficios indirectos o auxiliares son aquellos que son coincidentes pero que aún podrían contribuir significativamente a la decisión. Los ejemplos de los beneficios indirectos incluyen la mejora de la reputación, la satisfacción del personal y la "paz mental". (Con frecuencia estos factores son ponderados de forma significativa en la toma de decisiones).

Los costos directos son aquellos que se asocian directamente con la acción. Los costos indirectos son aquellos adicionales, auxiliares y costos con pérdidas, tales como la pérdida de la utilidad, la distracción del tiempo de la gerencia o la desviación del capital con respecto a

otras inversiones potenciales. Cuando se aplica un análisis de costo y beneficio a la decisión de si tratar un riesgo, se deberían incluir los costos y los beneficios asociados con el tratamiento del riesgo y con la aceptación del riesgo.

En el análisis cuantitativo de costo y beneficio, cuando se han identificado todos los costos y los beneficios tangibles e intangibles, se asigna un valor monetario a todos los costos y los beneficios (incluyendo los costos y los beneficios intangibles). Existe una variedad de modos normales de lograr esto incluyendo el enfoque de "voluntad de pagar" y utilizando sustitutos. Si, como sucede con frecuencia, se incurre en el costo en un periodo corto de tiempo (por ejemplo un año) y los beneficios fluyen durante un periodo largo posterior, normalmente es necesario descontar los beneficios para convertirlos en "dinero actual" de manera que se puede hacer una comparación válida. Todos los costos y los beneficios se expresan con un valor presente. El valor presente de todos los costos y los beneficios para las partes involucradas se puede combinar para producir un valor presente neto (VPN). Un VPN positivo implica que la acción es benéfica. Las relaciones de costo y beneficio también se utilizan, véase B.30.5

Si existe incertidumbre acerca del nivel de los costos o los beneficios, uno o ambos términos se pueden ponderar de acuerdo con sus probabilidades.

En el análisis cualitativo de costo y beneficio no se pretende encontrar un valor monetario para los costos y los beneficios intangibles y, en lugar del suministrar una cifra única resumiendo los costos y los beneficios, se considera de manera cualitativa las relaciones y los intercambios entre los diversos costos y beneficios.

Una técnica relacionada es el análisis del costo y eficacia. En esta técnica se asume que un beneficio o un resultado determinado es deseado y que hay varias formas alternas para lograrlo. El análisis considera únicamente los costos y la forma más barata para lograr el beneficio.

B.30.5 Elementos de salida

El elemento de salida de un análisis de costo y beneficio es la información sobre los costos y los beneficios relativos de diversas opciones o acciones. Se puede expresar cuantitativamente como el valor presente neto, una tasa interna de retribución o la relación del valor presente de los beneficios con el valor presente de los costos. El elemento de salida cualitativo usualmente es una tabla que compara los costos y los beneficios de diferentes tipos de costo y beneficio, llamando la atención a los intercambios.

B.30.6 Fortalezas y limitaciones

Las fortalezas del análisis de costo y beneficio son:

- permite la comparación de los costos y los beneficios utilizando una métrica sencilla (dinero);
- brinda transparencia en la toma de decisiones y,
- exige la recolección de información detallada sobre todos los aspectos posibles de la decisión. Esto puede tener valor en revelar la ignorancia así como el comunicar el conocimiento.

Limitaciones:

- el análisis cuantitativo puede producir números dramáticamente diferentes, dependiendo de los métodos usados para asignar los valores económicos a los beneficios no económicos;
- en algunas aplicaciones es difícil definir una tasa de descuento válida para los costos y los beneficios futuros;
- los beneficios que se acumulan para una población grande son difíciles de estimar, en particular aquellos que se relacionan con el bienestar público que no se intercambian en los mercados;
- la práctica de descuento implica que los beneficios que se ganan en el futuro a largo plazo tienen influencia insignificante en la decisión dependiendo de la tasa de descuento seleccionada. El método se torna inadecuado para considerar los riesgos que afectan a las generaciones futuras, a menos que se establezcan tasas de descuento muy bajas o cero

B.31 ANÁLISIS DE DECISIÓN DE CRITERIOS MÚLTIPLES (ADCM)

B.31.1 Información general

El objetivo es utilizar un rango de criterios para valorar o objetiva y transparentemente el mérito global de un conjunto de opciones. En general, la meta total es producir una preferencia de orden entre las opciones disponibles. El análisis implica el desarrollo de una matriz de opciones y criterios que se califican y agregan para obtener un puntaje total para cada opción.

B.31.2 Uso

Este análisis se puede utilizar para:

- comparar múltiples opciones para el primer paso de un análisis con el fin de determinar las opciones de preferencia y las potenciales, y la opción inadecuada,
- comparar opciones cuando existen criterios múltiples y algunas veces conflictivos,
- alcanzar un consenso sobre la decisión cuando las diversas partes involucradas tienen objetivos o valores conflictivos.

B.31.3 Elementos de entrada

Uno conjunto de opciones para el análisis. Los criterios, con base en los objetivos que se pueden utilizar equitativamente a través de todas las opciones para diferenciarlas.

B.31.4 Proceso

El general, un grupo de partes involucradas con conocimiento emprende el siguiente proceso:

a) definir el objetivo o los objetivos,

b) determinar los atributos (criterios o mediciones de desempeño) que se relacionan con cada objetivo;

c) estructurar los atributos en una jerarquía;

d) desarrollar las opciones que se van a evaluar frente a los criterios;

e) determinar la importancia de los criterios y asignar la importancia correspondiente a cada uno de ellos;

f) evaluar las alternativas con respecto a los criterios. Esto se puede representar como una matriz de puntajes,

g) combinar los puntajes de atributos sencillos múltiples en un solo un puntaje agregado de atributos múltiples;

h) evaluar los resultados.

Existen métodos diferentes mediante los cuales se puede obtener la ponderación para cada criterio, y diversas maneras para agregar los puntajes de los criterios para cada opción en un solo puntaje de atributos múltiples. Por ejemplo, los puntajes se pueden agregar como una suma ponderada o un producto ponderado, o utilizando el proceso de jerarquía analítica, una técnica de obtención para la ponderación y los puntajes con base en comparaciones por pares. Todos estos métodos asumen que la preferencia por cualquiera de los criterios no depende de los valores de los otros criterios. Cuando esta afirmación no es válida, se utilizan modelos diferentes.

Dado que los puntajes son subjetivos, el análisis de sensibilidad es útil para examinar la extensión hasta la cual las ponderaciones y los puntajes influyen en las preferencias totales entre las opciones.

B.31.5 Elementos de salida

Presentación en orden de rango de las opciones que va desde la máxima preferencia hasta la mínima. Si el proceso produce una matriz en donde los ejes son los criterios ponderados y el puntaje del criterio para cada opción, entonces también se pueden eliminar las opciones que producen criterios altamente ponderados.

B.31.6 Fortalezas y limitaciones

Fortalezas:

- Proporciona una estructura sencilla para la toma eficiente de decisiones y una presentación de las afirmaciones y las conclusiones;
- puede hacer más manejables los problemas de decisión complejos, que no son propensos al análisis de costo y beneficio;
- puede ayudar a considerar razonablemente los problemas cuando es necesario hacer intercambios;
- puede ayudar a alcanzar el acuerdo cuando las partes involucradas tienen objetivos diferentes y por lo tanto criterios diferentes.

Limitaciones:

Se puede ver afectado por el sesgo y la selección deficiente de los criterios de decisión;

La mayoría de los problemas de este análisis no tienen una solución única ni concluyente;

Los algoritmos de agregación que calculan los criterios hacen la ponderación a partir de preferencias establecidas o la agregación de puntos de vista diferentes pueden ocultar la base real de la decisión.