ESPACIO DE LA PRÁCTICA PROFESIONALIZANTE II

Análisis y Gestión del Riesgo Patrimonial

Lic. Oreste C. Sánchez

01/01/2019

TEMA

ANÁLISIS Y GESTIÓN DEL RIESGO PATRIMONIAL.

TEMA

TEMA

TEMA

1. EL ESTUDIO DE SEGURIDAD PATRIMONIAL.

Es el resultado del examen de aquellos factores que afectan o favorecen la seguridad de una instalación expresado en un documento que debe servir como guía para la elaboración del programa de seguridad y los subsiguientes planes del mismo.

Este estudio comprende el reconocimiento de los riesgos, y vulnerabilidades de la empresa, institución u objeto del estudio. El fin es recomendar las medidas de seguridad necesarias para la protección de los activos y el personal.

Un estudio de detección de necesidades de Seguridad y Protección a instalaciones persigue los siguientes objetivos:

a) Analizar las condiciones de seguridad física que presentan las instalaciones, bienes, personas y operaciones de una organización o comunidad.

b) Evaluar la cantidad y confiabilidad de los medios y equipos de seguridad y protección con que se cuenta para prevenir, detectar y/o reaccionar oportunamente ante las amenazas potenciales, a fin de neutralizarlas o mitigar sus efectos.

c) Analizar las normas, políticas y procedimientos de operación del sistema afectable, para la prevención, auxilio, litigación y recuperación en caso de emergencia, para determinar su nivel de efectividad.

d) Presentar un panorama general de los agentes perturbadores o amenazas a que está expuesto el sistema afectable, evaluando las vulnerabilidades y grado de riesgo estimado.

e) Proponer las recomendaciones básicas para neutralizar o minimizar los problemas que se detecten.

El estudio de seguridad nos dará la oportunidad de realizar un diagnóstico integral, el que podemos conceptualizar como;

> ***"El proceso de elaboración y sistematización de información que implica conocer y comprender los problemas y necesidades de seguridad dentro de un contexto determinado, sus causas y evolución a lo largo del tiempo, las fuerzas y actores sociales involucrados, así como los factores condicionantes y de riesgo y sus tendencias previsibles con el fin de establecer prioridades y estrategias de intervención[1]"***

[1] Adaptada por Aguilar Idañez y Ander-Egg (2006).

1.1. DEFINIENDO LA SEGURIDAD

> ***"La Seguridad es un sistema de combinación de métodos, procedimientos, técnicas y elementos (físicos, lógicos y psicológicos) diseñados para disuadir, detectar, denegar, demorar, aceptar o reaccionar con respecto a la amenaza."***[2]

Por lo expresado, notamos que la seguridad tiene dos formas básicas de verse, la primera es como usuario de la seguridad, que somos todos en una forma u otra, desde el mayor gobernante hasta el más humilde de los ciudadanos o habitantes de un país, tienen necesidad de la seguridad.

La seguridad, como producto, tiene un sentido meramente individual en la mente de cada persona, pero asociada a las personas, adquiere una connotación social que debe ser claramente precisada.

La gente común y corriente, percibe a la seguridad de una manera sumamente distinta que aquellas personas que sus labores o profesión se enfocan a la seguridad de los demás de un modo u otro.

1.2. LA FINALIDAD DE SEGURIDAD.

Los estudiosos de la conducta humana en su fase individual, así como en la colectiva, se han preocupado por analizar esta distinción conceptual, permitiéndonos establecer que la SEGURIDAD, se puede definir de dos maneras: como finalidad o **producto** y como **proceso.**

Como hemos visto, muchas son las definiciones y las mismas son tomadas desde distintos ángulos e interpretaciones.

Los practicantes o profesionales de la Seguridad, debemos entender lo que nuestros conciudadanos, clientes o usuarios esperan o entienden de la Seguridad, ya que de ello pueden depender las estrategias y tácticas para el manejo tanto de los procesos de convencimiento, como del diseño de los productos y servicios que pretendamos brindar.

La seguridad es, desde este punto de vista un sentimiento, es decir un bien intangible y, por tanto resulta en condiciones normales difícil de percibir y apreciar. Normalmente, la seguridad es apreciada más evidentemente cuando falla o cuando se carece de ella.

[2] Definición del consultor didáctico.

Es en virtud de esto que nunca se suele escuchar *"qué bien funciona la policía, no hay delitos en esta zona"*, porque el ciudadano común toma el estado de seguridad como normal, sin sentir ni pensar que hubo acciones disuasivas y/o preventivas que llevaron a ese estado las cosas.

1.3. EL MÉTODO GENÉRICO DE LA SEGURIDAD.

Llegados a este punto, nos parece importante definir qué entendemos por ***actos antisociales:*** Abarca un amplio rango de actos y actividades que infringen reglas y expectativas sociales. Muchas de ellas reflejan acciones contra el entorno, personas y propiedades.

Definición de conducta antisocial: Cualquier acción que viole las reglas y expectativas sociales o vaya contra los demás, con independencia de su gravedad.

y la seguridad contra actos antisociales es:

"La disposición de todas las medidas organizativas, los medios técnicos y personal que coadyuven a evitar, reducir o controlar las acciones delictivas derivadas de la comisión de robos, asaltos, agresiones, sabotajes, espionajes, fraudes, estafas, hurtos, atentados, vandalismos, amenazas de bombas, chantajes, manipulación de datos, tráfico de drogas, lavado de dinero, homicidios, etc." (Diccionario de la seguridad)

El método empleado en este tipo de seguridad es el siguiente:

Fuente: Biblioteca Grupo de estudios técnicos (Reg. 213-A235-08).

En este gráfico queremos explicitar los pasos generales del método genérico que debe aplicarse en la seguridad en todas sus acepciones.

1.3.1. *Contención:* es la primera fase**,** es la acción permanente e inicial de la seguridad, ya que es la utilización de los medios de prevención y protección, que podríamos llamar pasivos.

¿Qué buscamos en esta primera parte del "método genérico"?, obstaculizar con nuestros medios el accionar del delincuente, pero ¿en qué forma? ¿Agresiva?.... NO, ***disuasiva.***

¿Qué queremos decir con este accionar? es algo muy común a todos nosotros, tanto en el medio público como privado, comunicar al posible delincuente o al delincuente, el siguiente mensaje**: *"Aquí estamos, estamos protegidos, estamos preparados..."*,** etc.

¿Cómo plasmamos esto en la vida real? Si lo tomamos desde la Seguridad Pública, serán patrullajes motorizados o a pie, tele vigilancia urbana, CPTED (**C**rime **P**revention **T**hrough **E**nviromental **D**esign: *Prevención del crimen a través del diseño ambiental)*, cartelería, controles en general y otros.

Desde el punto de vista de la seguridad privada, será muy similar; sólo radica la diferencia en que estamos utilizando también esta primera fase del método, pero en un "objetivo" exclusivo y cerrado y no en un ambiente público.

Pero en ambas situaciones (seguridad pública o privada), en esta etapa tendremos, en caso de que sí ocurra un evento de agresión (intrusión, etc.), la misión de:

> ***a).- Disuasión:*** a través de los elementos pasivos y activos, conseguir que una persona cambie su manera de actuar, pensar o sentir.
>
> ***b).- Detención:*** del accionar de él o los agresores, tratando de evitar o demorar el evento delictivo. Incluso, utilizando algunas acciones y/o medios.
>
> ***c).- Restringir:*** la acción de ciertos tipos de agresores.
>
> ***d).- Canalización:*** hacia otros sectores, que cuenten con elementos físicos o técnicos más acordes a la agresión en proceso, que cuenten con mayores, mejores o especiales funciones o sistemas o sub-sistemas de vigilancia, o de detección e incluso capacidad para *intervenir.*

1.3.2. *Detección*. La segunda fase**,** se solapa con la anterior ya que ella será la encargada directa o indirectamente, de comunicar la acción en proceso. Muchos también son los elementos que permiten la detección, desde lo obtenido por la fase 1, llamados a los sistemas tipo 911, otras denuncias, personal especializado, Tele vigilancia urbana, CCTV privados, alarmas, etc.

Todos los elementos antes mencionados, constituyen:

> ***a).- Vigilancia***: es el proceso de monitoreo de personas, objetos o procesos dentro de sistemas seguridad.
>
> ***b).- Alerta***: manifiesta que se ha detectado una irregularidad
>
> ***c).- Reconocimiento***: es la verificación de la alerta que, de ser positiva, se ha convertido en una alarma y pone en movimiento una serie de procedimientos que englobaremos en:
>
> ***d).- Comunicación***: destinada a los encargados de realizar la acción de intervención, por medio de las Fuerzas de reacción (FFSS/FFPP).

1.3.3. ***Reacción*.** Es la tercera fase, es muy vertiginosa, pero requiere su análisis, partiendo de una seria y eficiente:

a).- ***Evaluación;*** que consiste en la clara y práctica dimensión del evento, una identificación lo más detallada posible, destacando tipo, forma de accionar, armamento, vehículos, cantidad de personas, etc. Éstos pueden ser obtenidos por propios medios o con la información que han ido aportando los elementos de las otras dos fases anteriores.

b).- ***Dedición;*** se determinará cómo, cuándo, con quién y con qué se actuará, así como también, si se efectuarán;

c).- **C*omunicaciones*** especiales, o no. Pero todo lo ocurrido en las tres fases, pero muy especialmente en esta última, cada uno de estos eventos debe quedar plasmado en un;

d).- ***Registro;*** de los hechos ocurridos y de todas las acciones realizadas.

1.3.4. ***Intervención:*** (Cuarta fase) Habiendo efectuado en las anteriores, todo en forma correcta y coordinada, lograremos una acción rápida y efectiva para neutralizar el evento en progreso o realizado. El objetivo lógico de esta cuarta fase es ***neutralizar*** al o los agresores o intrusos, acción que normalmente es llevada a cabo por las fuerzas de seguridad/policiales.

1.3.5. ***Normalización*:** (quinta fase) y consiste en volver a la situación de seguridad. Muchas son las tareas que esta quinta fase implica, pero muchas de ellas ya no son específicas de la seguridad, porque hay participación de psicólogos, médicos, asistentes sociales, etc.; por lo tanto es la seguridad la encargada de retrotraer a la situación inicial, que es una situación de equilibrio.

1.4. PREVENCIÓN URBANA.

A la prevención urbana podríamos encararla desde dos ángulos: el Estado y los ciudadanos. El Estado, es el responsable de la seguridad, es una de las funciones primordiales del Estado, irrenunciable, pero claro está que el ciudadano tiene también su gran cuota de responsabilidad como habitante de una ciudad, sea ésta pequeña o grande, en lo que atañe a la seguridad y prevención urbana, la auto protección. Para entender un poco más, presentaremos el cuadrado del delito:

Si tomamos el gráfico podemos darnos cuenta cómo piensa el delincuente, y cuando a cada uno de los lados del cuadrado tomemos alguna medida, le iremos colocando barreras al que quiera delinquir. Pero el primero y fundamental es para el habitante de la ciudad, es el de ***reducir al máximo los motivos*** de robo o delito, por poner un ejemplo simple, no guardar dinero en su domicilio o negocio, depositándolo en bancos.

Si tomamos otro de los lados del cuadrado nos encontramos con el ***menor riesgo y menor tiempo***, significa la posibilidad de fácil acceso y posibilidad cierta de evasión, a esto lo puede reducir o neutralizar colocando barreras de tipo físico y/o electrónico.

El último de los lados del Cuadrado: ***oportunidad de sorprender*** es una ventaja que no se le puede dar al delincuente (criminal) y para ello debemos estar activos en la lectura de los indicios que todo acto delictivo genera, siempre hay indicios previos a un hecho.

A este accionar ciudadano, le llamaremos ***autoprotección*** y debe ser enseñado a todos los ciudadanos y de ser posible comenzar con los niños en las escuelas primarias. Por supuesto que no queremos generar paranoia, pero sí la creación de hábitos que colaboran para facilitar el accionar policial en la represión de los delitos.

1.5. SEGURIDAD FÍSICA.

Muchas veces hemos escuchado y tal vez usado el término SEGURIDAD FÍSICA, pero pocas veces conocemos su aplicación y significado. Su definición según “El consultor didáctico-Diccionario de Seguridad”: organización de elementos tangibles, diseñados con el objeto de detectar, resistir y disuadir los posibles ataques. Este concepto abarca a los PED (siglas en inglés de dispositivos electrónicos portátiles), que transmiten energía electromagnética y estén incorporados a un sistema de protección.

El diseño de un sistema de seguridad física, exige que conozcamos las condiciones, características, especificaciones técnicas, parámetros y criterios de la relación costo/beneficio.

La instalación requiere conocer la estructura, la funcionalidad, los factores críticos y la adecuación al *modus operandi,* la agresividad y la accidentalidad.

La vulnerabilidad de una instalación está en proporción directa con las facilidades que presenta para ser atacada. No se puede generalizar con respecto a los lugares vulnerables de una instalación, pues cada una tiene su peculiaridad.

Como meros ejemplos podemos citar, que los lugares vulnerables de las organizaciones de servicios públicos, que proporcionan medios de comunicación, son las concentraciones de cables y las plantas de generación eléctrica, tanto normal como de respaldo; en los ferrocarriles se consideran críticos los túneles, puentes y patios de distribución; otros ejemplos son los generadores de las plantas eléctricas, los centros de cómputo o procesamiento de datos, almacenes de materiales peligrosos o explosivos para la producción de armamento, por lo tanto es necesario que en cada instalación se determinen los puntos vulnerables, examinando uno por uno los procesos de la cadena de producción u operación, desde la materia prima hasta los productos acabados y su distribución correspondiente.

Derivado del estudio de detección de necesidades, al que se denomina de diferentes formas (Encuesta de Seguridad, Auditoría de Seguridad, Diagnóstico de vulnerabilidad, Atlas de Riesgos, Estudio de Seguridad, Análisis de Vulnerabilidad, Análisis de riesgos, etc.) habrán de hacerse planos y diagramas que indiquen la localización de los lugares vulnerables.

De acuerdo con los textos militares generalmente aplicados, la seguridad física de instalaciones,"... ***son las medidas que se establecen para evitar lesiones o pérdidas de vidas humanas, daño, desorganización o destrucción de una propiedad, así como hacer todo lo necesario para que ésta se mantenga libre de peligros, opere y se desarrolle, cumpliendo los propósitos que le han sido fijados...".***

Por lo tanto el sistema de seguridad física se debe adoptar en toda situación, en todo lugar y en todo tiempo; esta seguridad depende en gran parte, de la adecuada detección de necesidades, la identificación de los riesgos a los que se está expuesto, la disposición de los medios adecuados de operación, el adiestramiento individual y de conjunto de la propia organización de que se trate y su enlace con la comunidad y autoridades competentes.

Existen varios conceptos fundamentales de la seguridad física entre los que podemos señalar:

a.- Protección en profundidad o a fondo (Security in Depth), que consiste en colocar una serie de obstáculos cada vez más difíciles, en el camino de un agresor, de acuerdo a los bienes a proteger y el riesgo del cual nos cuidamos.

b.- Estos obstáculos son las diferentes líneas de defensa que se establecen:

1ª. Línea de defensa: el perímetro de la propiedad.
2ª. Línea de defensa: la conformación exterior de los edificios.
3ª. Línea de defensa: Puertas y controles interiores.
4ª. Línea de defensa: Protección directa a los objetos.

En una instalación muy grande, tal como una mina industrial o un campo agrícola, puede llegar a considerarse poco práctico construir una cerca perimétrica costosa y mantenerla bajo observación; una instalación de este tipo generalmente se establece en un área apenas habitada, su aislamiento y la profundidad de la instalación en sí brindan razonable protección.

En estas circunstancias la colocación de letreros con advertencias, la reducción al mínimo de caminos de acceso y patrullas periódicas en el área entre el perímetro exterior y el área vital convencionalmente protegida puede ser suficiente.
La planificación para la seguridad física implica la definición de la protección para:

1. El Terreno que rodea a las edificaciones.
2. El Exterior de las edificaciones.
3. El Interior de las edificaciones
4. El Contenido de las edificaciones.

Tratando de seguir un marco de referencia que nos proporcione un enfoque más globalizado sobre este tema, lo que nos permitirá un alcance más internacional, se ha divido el presente tema en los puntos de:

1. Barreras
2. Accesos
3. Alarmas y Monitores
4. Comunicaciones
5. Iluminación de Protección
6. Cajas Fuertes y Bóvedas
7. Cerraduras, Candados y llaves
8. Guardias de Seguridad
9. Perros de Seguridad
10. Equipo de Protección Personal
11. Equipo e Instalaciones de Operación

2. ANÁLISIS DE RIESGOS.

El análisis de riesgo, también conocido como **evaluación de riesgos** o **PHA** por sus siglas en inglés *Process Hazards Analysis*, es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

Este tipo de análisis es ampliamente utilizado como herramienta de gestión en estudios financieros y de seguridad para identificar riesgos (métodos cualitativos) y otras para evaluar riesgos (generalmente de naturaleza cuantitativa).

El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar.

Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos[3].

Para el desarrollo de un ***Estudio de Seguridad*** se debe de seguirse un método y fijarse una estrategia.

El análisis de riesgo es un Diagnostico, para tratar de establecer a ciencia cierta ***Cómo estamos***, ***con qué nivel inicial de seguridad contamos***, cuales son las necesidades que presenta el sistema de seguridad.

El análisis es la distinción y separación de las partes en un todo hasta llegar a conocer sus principios o elementos. Es el examen que se hace de cualquier realidad susceptible de estudio.

[3] Fuente: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo

El análisis no busca valorar, sino busca identificar, mostrar y presentar lo que está presente, pero el buen analista, el analista profesional sabe encontrar lo invisible y no debe quedarse con lo simple, objetivo, mesurable y observable.

Podemos decir que a través de este estudio, tómanos conciencia, de las vulnerabilidades de nuestra organización, tanto físicas y electrónicas (estructurales) como de los dispositivos e instrumentos adoptados, (Manual de operaciones, capacidad e idoneidad del personal de seguridad).

De este estudio van a surgir las distintas estrategias a abordar para fortalecer las vulnerabilidades, crear los distintos protocolos de actuación, fomentar la capacitación del personal de seguridad, y el resto de los empleados de la organización, implementando una ***Cultura de Seguridad Integral.***

Una vez finalizado el Análisis de Riesgo y ya con el diagnostico de nuestra situación actual, podremos confeccionar un ***Proyecto de Seguridad***, en el que vamos a destacar, los Procedimientos, el Recursos Humanos, los Recursos Técnicos y Físicos.

Cada uno de estos subsistemas, están estrechamente entrelazados, para conformar un todo, y de esta menara potenciar las medidas de seguridad, eliminando las vulnerabilidades, conteniendo las amenazas.

2.1. PRINCIPIOS DE PLANIFICACIÓN EN SEGURIDAD.-

El principio filosófico de la seguridad, **es el mantenimiento del equilibrio de los bienes y recursos de la Empresa.** La seguridad, para ser eficiente, debe basar su planeación y operación respetando en todo momento tres principios básicos:

2.1.1. El principio de la Información.

El principio de la **INFORMACIÓN,** es el que genera y motiva las acciones de los otros dos principios (el dispositivo y el secreto). Resulta fundamental tener presente y recalcar que la información tiene un significado esencial, ya que sin ella difícilmente podremos efectuar una buena planeación de los sistemas de seguridad y, en todo caso, estaremos expuestos a la insuficiencia de dichos sistemas o a la inadecuada actuación de los mismos.

Es lógico que para determinar cómo y con qué vamos a proporcionar seguridad a los bienes y recursos, requerimos saber contra qué o de qué hemos de proteger a los recursos, es decir que debemos **identificar las necesidades de Seguridad y Protección**.

A esto lo haremos usando el principio de la información que dividiremos en cinco instancias. Las cinco instancias mencionadas son:

a. Detectar y Analizar las amenazas
b. Determinar las vulnerabilidades
c. Establecer el Impacto Consecuencial
d. Evaluar y Jerarquizar el riesgo
e. Retroalimentar

***a. Detectar y analizar las amenazas*:** En este punto es necesario precisar el concepto de Amenaza a la que definiremos como:

> ***Todo acto o condición que por sí mismo o ligado a otro puede ocasionar un daño parcial o total, moral o material a los bienes y/o personas, cualquier peligro potencial. (La amenaza es cualitativa).***

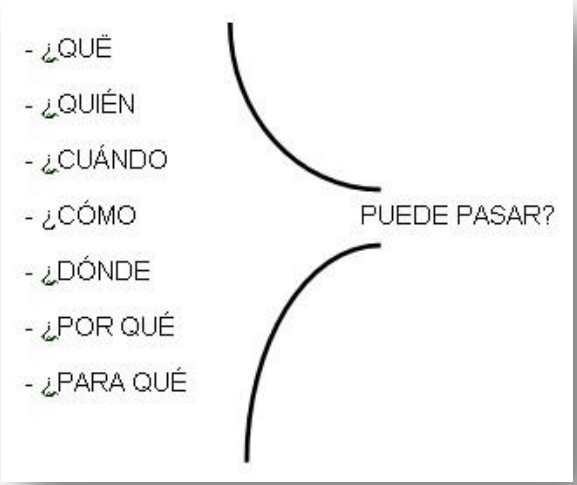
En seguridad, sabemos que no existe amenaza o enemigo pequeño, ya que menos preciar las situaciones de peligro normalmente conduce a grandes desastres.

Algunas amenazas son muy evidentes, pero otras pueden parecer insignificantes; la mente que prevé, es capaz de encontrar el pozo antes de que se ahogue el niño, aún en condiciones en que la mayoría de las personas ignorarían, por ser poco visible el peligro.

De entre la inimaginable lista de actos y condiciones de peligro podemos, enunciativamente, citar los siguientes:

- Robo	- Responsabilidad civil	- Sismo
- Incendio	- Huelga	- Amenaza de bomba
- Inundación	- Tromba	- Terrorismo
- Secuestro	- Asalto	- Desperdicio
- Intrusión	- Disturbio civil	- Ociosidad
- Accidente	- Toma de instalaciones	- Sabotaje
- Corto circuito	- Espionaje industrial	- Fraudes
- Falla de energía	- Fuga de materiales	- Abuso de confianza
- Contaminación		- Guerra o guerrilla
- Fuga de información		- Devaluación

Para la detección de amenazas existen dos vías principales: la **Formal** y la **Informal**. En el primer caso se trata de un estudio de estructura de seguridad, al que se le denomina Auditoria de Seguridad y que también se le conoce como Atlas De Riesgos o Diagnóstico De Vulnerabilidad. Una vez detectada la posibilidad de una pérdida, debe efectuarse el análisis de cada uno de los peligros potenciales para determinar la vulnerabilidad, este análisis parte de aplicar a cada peligro detectado las preguntas clásicas de:



Por su parte, la ***vía informal***, es aquella que no es detectada por el área de seguridad, sino más bien la amenaza es detectada por un empleado, visitante o tercero, quien plantea sus necesidades. *"Conociendo esa denuncia",* se efectúa el proceso de preguntas anteriores a efectos de determinar lo que realmente se constituye en una amenaza.

b. Determinar las vulnerabilidades: Una vez que se ha realizado el análisis de las amenazas detectadas, se determina la Vulnerabilidad, a la que podemos definir como:

> ***"La mayor o menor facilidad que presenta un bien u operación para la ocurrencia de una amenaza en virtud de las condiciones que imperan. Puede decirse que son los puntos o momentos de debilidad que se tienen, y pueden favorecer la ocurrencia de un acto negativo o el aumento en las consecuencias de éste".***

c. Establecer el impacto consecuencial: Otro factor importante es el establecimiento del llamado impacto consecuencial, que definiremos como:

> ***"El nivel y tipo de daño que pudiera resultar en caso de llegar a materializarse una determinada amenaza. Normalmente se distingue el mínimo y máximo de daño posible y probable".***

El impacto consecuencial se identifica en dos vertientes: por **tipo** y por **nivel**, de acuerdo a la siguiente tabla:

Nivel de impacto
- Severidad desconocida
- Leve
- Severo
- Grave
- Catastrófico

Tipo de impacto
- Corporal
- Económico
- Funcional
- Ambiental
- Político/ imagen
- Psicológico

***d. Evaluar y Jerarquizar el Riesgo*:** Muy frecuentemente, la gente confunde al riesgo con la amenaza y erróneamente se expresa diciendo que tiene mucho riesgo, siendo lo correcto decir que tiene muchas amenazas, con distintos grados de riesgo.

Originalmente se decía que existía un riesgo potencial y un riesgo realizado, sin embargo actualmente se ha logrado distinguir a la Amenaza como el factor CUALITATIVO y al riesgo como el factor CUANTITATIVO.

En efecto, la amenaza se refiere a lo que puede suceder y el riesgo a qué tan probable es que la amenaza se materialice, tomando en cuenta el análisis de la misma, la vulnerabilidad y el impacto consecuencial que se ha determinado.

El riesgo puede definirse como:

"El grado de probabilidad de que una amenaza se materialice."

La evaluación de riesgos ha sido objeto de innumerables estudios y existen muy variadas técnicas para determinarlos, sin embargo hemos de mencionar que un factor decisivo para evaluar la probabilidad de ocurrencia de los hechos negativos, es el sistema de registro estadístico y comparativo de incidencias de seguridad, que nos permite estimar nuestra probabilidad de materialización de las amenazas.

Mediante el sistema de registro estadístico y comparativo, aunado a los mecanismos de información o inteligencia con que disponemos, podremos determinar los tres factores que inicialmente se utilizan para la evaluación del riesgo y que son:

- FRECUENCIA
- TENDENCIA
- FACTORES AMBIENTALES (INTERNOS Y EXTERNOS)

Una vez evaluado el riesgo, se jerarquiza, en función de las vulnerabilidades y el impacto consecuencial, para poder darle el tratamiento de acuerdo a la denominada regla de las Cinco ”R” o pirámide de la Administración del Riesgo.

e. Retroalimentar: Pensando en función de la teoría de los sistemas abiertos, la información tiene un ciclo, es decir no basta con hacerla una sola vez, sino que es preciso mantenerla y renovarla, porque resultan situaciones, mucho más frecuentes de lo deseable, en donde el sistema de seguridad se ve rebasado por amenazas que no fueron tomadas inicialmente en cuenta.

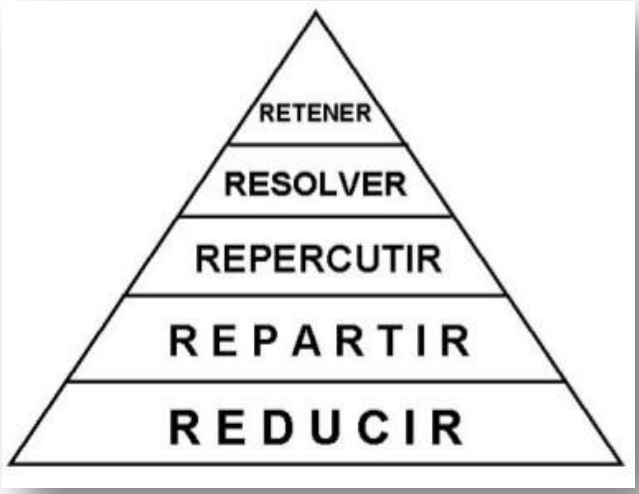
A pesar de que al hacer el estudio no se contaba con indicios de su existencia, por la misma dinámica del sistema, las amenazas aparecieron sin que los responsables de seguridad se hayan preocupado por detectarlas y reportarlas.

Es por esto que se deben mantener mecanismos constantes de monitoreo, a través de vías formales e informales como las inspecciones, la revisión de partes de novedades, las quejas y reportes, revisión de periódicos y noticieros y todo otro medio que nos permita detectar oportunamente la posibilidad de que un acto negativo pueda dañar a las personas, bienes y operaciones de nuestra Organización.

2.1.2. El principio de Dispositivo.

Habiendo revisado el principio de la Información, pasaremos al **dispositivo** y al **secreto**. Para poder establecer el dispositivo requerido de acuerdo a las necesidades detectadas, es menester que la Empresa determine la filosofía básica respecto al tratamiento que se les han de dar a los riesgos evaluados.

Hemos de señalar que ante todo problema o deficiencia de seguridad, se pueden tomar **cinco actitudes básicas**, que se muestran en la denominada PIRÁMIDE DEL TRATAMIENTO DEL RIESGO:



La experiencia ha demostrado que el tratamiento correcto del riesgo debe orientarse de acuerdo a la presentación inicial que nos enseña la pirámide. Es decir que la mejor medida es:

a.- REDUCIR: o sea disminuir la probabilidad de que el hecho negativo se materialice; esto a través de una serie de recaudos como la prevención, disuasión y/o reacción, que tanto administrativa como técnicamente, permitan evitar la ocurrencia de una amenaza y/ pérdida.

b.- REPARTIR el riesgo, que consiste en no tener todos los elementos de valor o críticos reunidos en un solo espacio físico.

c.- REPERCUTIR: A pesar de lo anterior, toda probabilidad de pérdida, en virtud de la imposibilidad de determinarla, ha de ser repercutida o transferida, es decir cubierta a través de

un Seguro, Fianza o Garantía, que minimice el daño en caso de llegar a ocurrir el hecho negativo.

d.- RESOLVER: es sacar el factor de interés para la delincuencia, por ejemplo: no manejar dinero en la organización, todo a través de sistemas virtuales.

e).- RETENCIÓN: Por último, toda repercusión, implica necesariamente un grado de retención ya que en caso de ocurrir un siniestro o presentarse una pérdida, los DEDUCIBLES disminuirán la recuperación y son, en consecuencia, una pérdida de todas formas. Es más, aun cuando nunca ocurra el hecho negativo, el pago de las "primas" es finalmente un margen de disminución en los bienes protegidos.

Lo importante en este concepto es que la administración del riesgo esté en todo momento bajo el conocimiento y dominio del Responsable de Seguridad, para evitarse desagradables sorpresas por accidentes no asegurados, bienes subvaluados o eventos no considerados.

Un **dispositivo** es el conjunto de elementos que materializan las funciones de seguridad. Hace que la seguridad se vea, sienta y se integra de dos elementos que en términos de informática se denominan HARDWARE, es decir los elementos físicos, equipos, instalaciones, etc. y el SOFTWARE, o sea los elementos no físicos, sin los cuales los equipos no tendrían utilidad, ya que de nada sirve contar con una pistola si no se tienen los conocimientos y procedimientos para su uso.

Estos dos tipos de elementos son interdependientes y en ellos se contienen los medios que se usan en la protección de bienes y personas, que a continuación se presentan.

FÍSICOS	NO FÍSICOS
- BARRERAS - ACCESOS - VISIBILIDAD - COMUNICACIONES - EQUIPO DE PROTECCIÓN PERSONAL - EQUIPO E INSTALACIONES DE OPERACIÓN - FUERZAS DISUASIVAS Y DE REACCIÓN	- PLAN INTEGRAL DE SEGURIDAD - OBJETIVOS Y POLÍTICAS - ESTRATEGIAS - ESTRUCTURA ORGANIZACIONAL - PRESUPUESTOS - SISTEMAS (MANUALES) - PROGRAMAS - PROCEDIMIENTOS * Operativos * Especiales * De contingencia - TIEMPO Y ESPACIO

Elementos Físicos:

Respecto a los elementos físicos, realizaremos una descripción de ellos en el anexo I; por el momento únicamente nos limitaremos a señalarlos, ya que debido a la orientación del presente material nos enfocaremos en los elementos no físicos, que son los que en las funciones de un Directivo, resultan su mayor campo de actuación.

Elementos no Físicos:

Así como los programas son la mejor herramienta del supervisor, los **procedimientos** representan la base del trabajo del guardia o del elemento operativo.

El procedimiento es una serie de pasos que lógica y secuencialmente, establecen la forma y tiempo para la realización correcta de una operación o actividad. En seguridad se distinguen 3 tipos de procedimientos:

a) **Operativos:** Estos procedimientos son los de rutina de las actividades diarias para los días Laborales y/o no laborales.

b) **Especiales:** En estos casos es cuando las actividades no son rutinarias, por ejemplo un Evento, día de pago o una actividad de construcción, etc.

c) **De Contingencia:** (Urgencia o Emergencia).

En este marco, es importante mencionar también, que todo procedimiento, para ser efectivo y valioso en el trabajo, debe cumplir con **cinco principios:**

1. **Estar por escrito:** Siempre es conveniente que esté documentado y registrado.
2. **Ser autorizado:** Debe estar autorizado por la máxima autoridad de la organización.
3. **Difundirlo al / los ejecutantes**: Todo el personal involucrado debe tener conocimiento de los mismos.
4. **Supervisar su aplicación**: El control es una actividad necesaria para la implementación y ejecución.
5. **Actualizarlo sistemáticamente**: Como usted sabe, la seguridad es dinámica, por lo tanto, los procedimientos deben ser adaptados a los cambios que se produzcan, a fin de no perder su efectividad.

2.1.3. Principio del Secreto.

El tercer principio de la Seguridad ha sido inadecuadamente interpretado y, por tanto, erróneamente aplicado, ya que no se trata de caer en extremos que rayan en lo irrisorio, sino de entender que existe una serie de disposiciones y medidas de la seguridad que deben ser conocidas y/o controladas por personas seleccionadas y restringidas.

La Seguridad ***siempre debe sentirse y casi nunca verse***, se dan a conocer sólo aquellos factores que nos benefician, manteniendo en confidencialidad los elementos clave que nos permitirán, en caso de una situación de peligro, conservar la libertad de reacción acertada y ordenada, neutralizando el elemento sorpresa que pudiera actuar en nuestra contra.

Aún en el ámbito de la Protección Civil y de la Seguridad e Higiene Ocupacional, existen ciertos dispositivos e indicaciones, que pudieran resultar inconvenientes en caso de difundirse sin un adecuado control.

3.- DETECCIÓN DE NECESIDADES DE SEGURIDAD

Análisis de Riesgos o Diagnóstico de Vulnerabilidades.

Existen dos vías genéricas para la realización del principio de la información, la formal que se materializa a través de una investigación científica, bajo un procedimiento y programa de trabajo. A esta vía se la conoce de distintas maneras como:

- Diagnóstico de Vulnerabilidades
- Atlas de Riesgos
- Estudio de Seguridad

La segunda vía, llamada informal, se realiza cotidianamente a través de las inspecciones, rondines, recorridos, reportes, quejas y cualquier otro medio directo o indirecto que nos permita detectar condiciones inadecuadas que pudieran ocasionar un daño o perdida. La disyuntiva en este AR, es **con quién vamos a efectuarlo:** ¿con personal interno o externo?

A continuación se señalan las ventajas y desventajas en cada caso:

PERSONAL INTERNO	
VENTAJAS	**DESVENTAJAS**
- Bajo Costo	- Parcialidad
- Disponibilidad de tiempo	- Política interna
- Confidencialidad	- Lentitud
- Profundidad	- Baja autoridad Moral
- Accesibilidad interna	- Inaccesibilidad a la dirección
	- Ceguera de taller

PERSONAL EXTERNO	
VENTAJAS	**DESVENTAJAS**
- No compromiso político	- Costo elevado
- Imparcialidad	- Riesgo de superficialidad
- Rapidez	- Bloqueo de personal interno
- Imagen "de expertos"	- Indisponibilidad
- Frescura en la observación	- Riesgo de indiscreción
- Diversidad de criterios	
- Acceso a nivel dirección	

La conclusión que ha dado la experiencia, nos dice que lo mejor es reunir al personal interno con los auditores externos, buscando aprovechar las ventajas que ambos representan y atenuar las desventajas.

Un estudio de detección de necesidades de Seguridad y Protección a instalaciones persigue los siguientes objetivos:

f) Analizar las condiciones de seguridad física que presentan las instalaciones, bienes, personas y operaciones de una organización o comunidad.

g) Evaluar la cantidad y confiabilidad de los medios y equipos de seguridad y protección con que se cuenta para prevenir, detectar y/o reaccionar oportunamente ante las amenazas potenciales, a fin de neutralizarlas o mitigar sus efectos.

h) Analizar las normas, políticas y procedimientos de operación del sistema afectable, para la prevención, auxilio, litigación y recuperación en caso de emergencia, para determinar su nivel de efectividad.

i) Presentar un panorama general de los agentes perturbadores o amenazas a que está expuesto el sistema afectable, evaluando las vulnerabilidades y grado de riesgo estimado.

j) Proponer las recomendaciones básicas para neutralizar o minimizar los problemas que se detecten.

Para el desarrollo del estudio o auditoría de seguridad, debe seguirse un método y fijarse una estrategia. Si bien cada auditor desarrolla su propio estilo de trabajo, a continuación y como una mera referencia, se presenta una lista de verificación sobre algunos de los puntos principales que debe tomar en consideración con fines de auditoría.

3.1. GUÍA DE INVESTIGACIÓN PARA REUNIÓN DE INFORMACIÓN.

a.- Datos Generales

a.1.- Razón social
a.2.- Ubicación
a.3.- Consideraciones previas.

b.- Importancia y Finalidad de la Instalación

b.1.- Centro industrial (tipo de industria)
b.2.- Productos y/o servicios que procesa o presta
b.3.- Oficinas administrativas
b.4.- Almacén
b.5.- Superficie de terreno
b.6.- Niveles
b.7.- Superficie y antigüedad de las construcciones
b.8.- Planos arquitectónicos y especificaciones
b.9.- Población fija y flotante.

c.- Entorno

c.1.- Norte
c.2.- Sur
c.3.- Este
c.4.- Oeste

d.- Amenazas o peligros a los que está expuesta por su ubicación. (Agentes perturbadores).

1) Fenómenos Geológicos
Sismos y Tsunamis
Erupciones volcánicas
Deslaves y Hundimientos de tierra
Otros

2) Fenómenos Hidrometeorológicos
- Huracanes
- Trombas
- Inundaciones
- Tifones
- Sequías
- Otros

3) Fenómenos Químicos
- Incendios
- Explosiones
- Fugas o derrames de substancias peligrosas
- Otros

4) Fenómenos Sanitarios
- Plagas y Epidemias
- Contaminación de los suelos
- Contaminación del aire
- Contaminación del Agua y sus mantos
- Contagios
- Otros

5) Fenómenos Socio-Organizativos
- Disturbio civil
- Asalto
- Accidentes mayores
- Amenaza de bomba
- Sabotaje
- Huelga
- Otros

En la detección de necesidades de Seguridad, se debe tener siempre en cuenta, que **NO HAY** peligro o enemigo pequeño.

Una vez realizada la auditoría, convenientemente apoyada en el uso de fotografías, planos e inclusive video-grabaciones, ya se ha acopiado toda la información del trabajo de campo y es menester proceder al trabajo de gabinete, en donde el auditor tendrá que poner en términos accesibles, mediante una redacción clara, concisa, completa y correcta los resultados obtenidos.

El Informe final de auditoría (análisis de riesgos) es uno de los elementos fundamentales para la planeación del Sistema de Seguridad Integral.

Es imprescindible que la información contenida en el informe sea escrupulosamente revisada y enfocada a la realidad observada para que nos pueda mostrar la "Fotografía o Radiografía" del Centro u Oficina desde el punto de vista de la Seguridad de sus personas, bienes y recursos.

3.2. EVALUACIÓN DE RIESGOS.

Concepto: Es el proceso mediante el cual realizamos la valoración y ponderación de los factores de riesgo.

La ponderación será más eficaz, en la medida que sea más exhaustivo el listado de variables que pueden influir en el riesgo considerado. Con posterioridad iremos eliminando aquellas variables que sean poco significativas. En esta eliminación es necesario tener en cuenta el desplazamiento de las variables en función del entorno y por consiguiente habrá que mantener determinadas variables que se hacen importantes por modificación del ambiente.

La técnica de evaluación cuantitativa de riesgos es bastante reciente, pues sus primeros tratados se remontan tan sólo a 1960, con la aparición del primer método de cálculo y Apreciación del Riesgo de Incendio en diez puntos.

Posteriormente fueron publicados numerosos métodos entre los que podemos destacar los siguientes:

- Cálculo del grado de protección Din 18.230.
- Método Gretener (Riesgo de incendios)
- Método Purt (Riesgo de incendio y grado de protección automática)
- Método de Cruzel y Sarrat. ERIC. Evaluación del riesgo de incendio por cálculo.
- Método de Shibe para instalaciones hospitalarias.
- Método de Aschoff. Métodos de protección en función del riesgo.
- Método de Dow en industria química.
- Método de Trabaud para incendios forestales.
- Método de Stadler para ubicación de parques de bomberos.
- Método de Pou, con la misma finalidad del anterior.

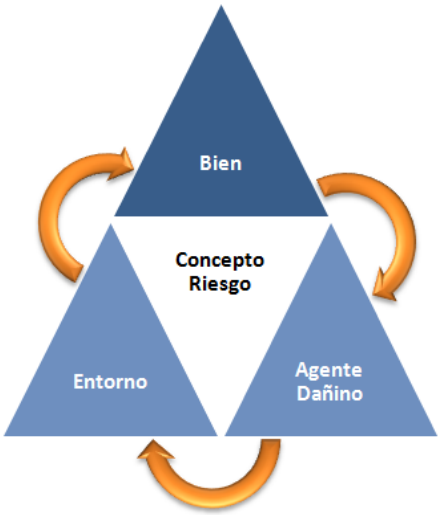
4. ANÁLISIS CUANTITATIVO DE RIESGOS.

4.1. *El Método Mosler*.

La seguridad no ha sido ajena al desarrollo de los métodos científicos. La aplicación de la ciencia a la seguridad, no está restringida al campo meramente tecnológico (alarmas, blindajes, sensores, equipos de video, etc), sino que a medida que se profundiza en la seguridad lógica y psicológica, se han venido aplicando métodos científicos, en forma similar a como lo hacen otras ciencias.

Uno de los desarrollos científicos de mayor difusión, es el de la aplicación de métodos combinados de estadística y probabilidad, mediante los cuales, a través de un esquema de matrices, se miden la frecuencia, la magnitud, y el efecto de un probable siniestro. En un objetivo específico a proteger y por un tiempo determinado, permite diseñar políticas de seguridad para ese objetivo, utilizando aparentemente, una incontrovertible base científica. Lo anterior ha dado origen a métodos como el Mosler, entre otros.

Cuando un experto en seguridad es consultado acerca de sistemas de prevención de riesgos y protección de personas y bienes, debe trabajar metódicamente a fin de llegar a una evaluación correcta.



Empleando el Método Mosler, que se aplica al análisis y clasificación de los Riesgos, y tiene como objetivo identificar, analizar y evaluar los factores que puedan influir en su manifestación, podrá hacer una evaluación ajustada de los mismos.

4.2. CONCEPTOS GENERALES.

Con la finalidad de entender y hacer una buena utilización del Método Mosler, vamos a proceder a definir algunos conceptos de importancia para este trabajo.

4.2.1. El Riesgo:

> ***"Es la Probabilidad de materialización de la amenaza en relacion con el daño que produciria dicha materializacion".***
>
> ***"El riesgo tambien se define como la contingencia que un bien sufra un determinado daño".***
>
> ***"Riesgo de que la cualidad benefica de un bien en unas determinadas circunstancias, pueda sufrir una manifestacion motivada por una causa con resultados de consecuencias negativas"***

La Ecuación sería.

Probabilidad x Consecuencia= Nivel de Riesgo

En realidad se trata, de poner en relación multiplicando la probavilidad de que un daño se manifieste, por las consecuencias de la manifestación que de dicho daño tendría y eso nos da el nivel del riesgo.

El concepto de riesgo comprende tres variables que se relacionan entre si, ***el bien, el agente dañino, y el entorno;*** cuando se conjugan estos tres elementos, estamos ante la probabilidad de la materialización de un riesgo.-

4.2.2. Bienes y Activos.

> ***"El bien es toda persona, animal o cosa que en determinadas circunstancias posee una o varias cualidades benéficas, en virtud de las cuales resulta objeto de valoración".***

Generalmente el bien no tiene un valor absoluto, si no que depende de las circunstancias donde se desarrolla, por ejemplo el valor relativo del agua es distinto en Neuquén, que en el desierto del Sahara. Por lo tanto el concepto de relatividad o del entorno donde se da el bien es fundamental para conocer su valoración.

Desde el punto de vista empresarial, se utiliza el termino de **Activo**, y no de **Bien.**

> ***"El activo es el recurso de la empresa ligado a esta, y necesario funcione correctamente y se alcance los objetivos propuestos por la Dirección".***

Como activos podemos encontrar; Financiacion, el dinero, la informacion, los inmuebles; los bienes intangibles los trabajadores. Entre los activos tambien podemos mencionar; la imagen; el prestigo, la actividad desempeñada y la imagen y confianza generada por el cliente, que pueden verse afectada por la materialización de un riesgo que no hayamos contemplado y valorado.

Importante:

> ***"Cuando realizamos un analisis de riesgo, siempre las personas son la primera prioridad a la hora de evaluarlos".***

Siempre que se trabaje en un análisis de riesgo, y se utilice el Método Mosler, se deberá de identificar el Bien, ver o establecer cuál es su cualidad benéfica, y en qué circunstancias el bien tiene esas cualidades benéficas.

Se confecciona una ficha:

IDENTIFICACIÓN DEL BIEN	
Cosa valiosa:	Bien o propiedad
Cualidad benéfica o Característica:	Que posee o se atribuye al bien
Las circunstancias que delimitan o determinan el bien o la cualidad benéfica.	

***4.2.3. Daño o Impacto*:** Es toda variación que le supone a un bien, una disminución del valor o precio del que era objeto. Ejemplo de daños, pueden ser, incendio, actos antisociales, robos, atentados, enfermedades del tipo biológico que afecten a la salud.-

En términos empresariales a los daños se los denomina IMPACTO: Es una consecuencia negativa producida por la materialización de una amenaza sobre uno o varios activos.

Debemos realizar una ficha de identificación del daño para ver a que nos enfrentamos. En ella debe de constar, cual es el agente dañino y/o la causa que provoca el daño o pérdida.

Se confecciona una ficha:

IDENTIFICACIÓN DEL DAÑO	
Agente Dañino o causa	Que origina el daño
La manifestación del Daño	Como se produce el daño y en qué medida
Las consecuencias negativas o daño	

4.2.4. El Entorno.

Es lo que rodea a un individuo, sin formar parte de él, por ejemplo el clima, otros individuos, el relieve, las normas culturales, religiosas o jurídicas, etcétera. Las múltiples interrelaciones que se presentan en el entorno, dando significación al entorno, y gravitando sobre el sujeto, componen el contexto.

El entorno empresarial son las fuerzas directas e indirectas que condicionan la vida de la empresa, su actuación y sus logros o fracasos. En el entorno directo de la empresa, podemos situar a los proveedores, a los clientes y a la competencia, y en el entorno indirecto; vinculado a la empresa pero con impacto mediato sobre ella: la tecnología, las leyes, la economía, la política, la geografía, las prácticas sociales, etcétera.

***4.2.5. Amenaza*:** Es toda causa previsible de daño a las personas o bienes. Puede ser de distintos origenes origen:

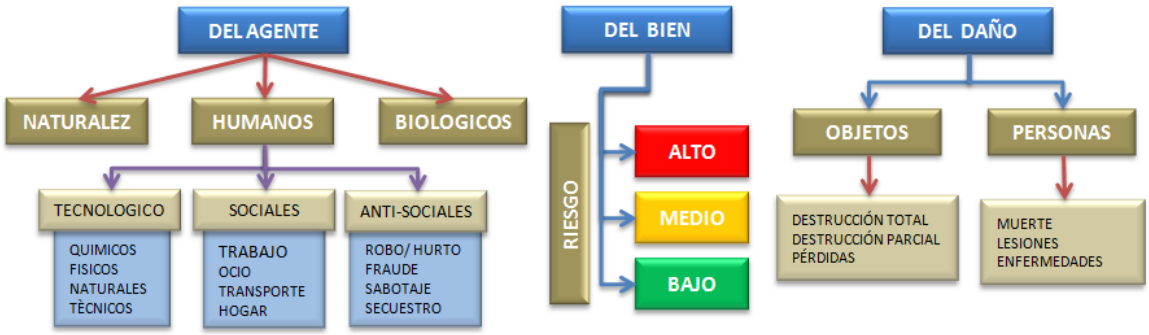
- Antisociailes (intrucion, robo, hurto, sabotaje, etc)
- Naturales (inundaciones, terremotos, tayos, etc),
- Tecnologicas (fallos de hardware o sofware, etc),
- Biologicas (virus, bacterias, epidemias, etc)
- Antròpicas (manifestaciones, huelgas, etc)
- Otras (cortes de suministro, incumplimientos legales, etc).

4.3. LAS CUATRO FASES DEL MÉTODO MOSLER.

4.3.1. Fase 1: DEFINICIÓN DEL RIESGO.

Esta fase tiene por objeto la identificación del riesgo, delimitando su objeto y alcance, para diferenciarlo de otros riesgos. El procedimiento a seguir es mediante la identificación de sus elementos característicos. Estos son: a) El bien. b) El daño

Para llevarla a cabo se requiere definir a qué riesgos está expuesta el área a proteger (riesgo de inversión, de la información, de accidentes, o cualquier otro riesgo que se pueda presentar), haciendo una lista en cada caso, la cual será tenida en cuenta mientras no cambien las condiciones (ciclo de vida).



4.3.2. Fase 2: ANÁLISIS DE RIESGO.

En este método, utilizamos seis (6) criterios de valoración y todos ellos se ponderan en una escala Penta (1al 5) de menor a mayor gravedad.

4.3.2.1. Criterio de Función (F).

Que mide cuál es la consecuencia negativa o daño que pueda alterar la actividad y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde “Muy levemente” a “Muy grave”:

Criterio de Función (F)	
Muy gravemente	5
Gravemente	4
Medianamente	3
Levemente	2
Muy levemente	1

Preguntas:

Los daños a clientes y empleados, ¿Cómo puede afectar?
Los daños en las instalaciones, ¿Cómo puede afectar?
Los daños económicos, ¿Cómo puede afectar?

4.3.2.2. Criterio de Sustitución (S).

Que mide con qué facilidad pueden reponerse los bienes en caso que se produzcan alguno de los riesgos y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde “Muy fácilmente” a “Muy difícilmente”

Criterio de Sustitución (S)	
Muy difícilmente	5
Difícilmente	4
Sin muchas dificultades	3
Fácilmente	2
Muy Fácilmente	1

Preguntas:

El bien a sustituir, ¿se puede encontrar?
Los trabajos de sustitución, ¿serán rápidos?
La actividad en la empresa, ¿continuará?

4.3.2.3. Criterio de Profundidad o Perturbación (P).

Que mide la perturbación y efectos psicológicos en función que alguno de los riesgos se haga presente (Mide la imagen de la firma) y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde “Muy leves” a “Muy graves”.

Criterio de Profundidad (P)	
Perturbaciones muy graves	5
Graves perturbaciones	4
Perturbaciones limitadas	3
Perturbaciones leves	2
Perturbaciones muy leves	1

Preguntas:

Los daños en la imagen de la entidad,
¿Causan perturbaciones en el personal?
¿Causan perturbaciones en los clientes?
¿Causan perturbaciones en el sector?

4.3.2.4. Criterio de Extensión (E).

Que mide el alcance de los daños, en caso de que se produzca un riesgo a nivel geográfico y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde “Individual” a “Internacional”.

Criterio de Extensión (E)	
De carácter internacional	5
De carácter nacional	4
De carácter regional	3
De carácter local	2
De carácter individual	1

Preguntas:

Los daños en la imagen de la entidad, ¿han sido?
Los daños económicos, ¿han sido?
Los daños en los bienes, ¿han sido?

4.3.2.5. Criterio de Agresión (A).

Que mide la probabilidad de que el riesgo se manifieste y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde “Muy reducida” a “Muy elevada”.

Criterio de Agresión (A)	
Muy alta	5
Alta	4
Normal	3
Baja	2
Muy baja	1

Preguntas:

¿Cómo es el nivel de delincuencia en el sector y/o en el territorio?
¿Las instalaciones se encuentran aisladas o en zona de actividad natural?
¿Existen materias peligrosas o gran cantidad de elementos técnicos?

4.3.2.6. *Criterio de Vulnerabilidad (V).*

Que mide y analiza la posibilidad de que, dado el riesgo, efectivamente tenga un daño y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde “Muy baja” a “Muy Alta”.

Criterio de Vulnerabilidad (A)	
Muy alta	5
Alta	4
Normal	3
Baja	2
Muy baja	1

Preguntas:

¿Los daños podrán evitarse con las medidas de seguridad existentes?
¿Existencia de ayuda exterior en la zona?
¿Las perdidas están aseguradas?

Ejemplo de la Valoración de un análisis de Riesgo: En la siguiente tabla, ejemplificamos la valoración del Riesgo, en función de las amenazas (robo/hurto), teniendo en cuenta las vulnerabilidades que presenta determinada organización.

	ANALISIS del RIESGO					
Tipo de Amenazas	**F**	**S**	**P**	**E**	**A**	**V**
Robo	4	3	3	3	5	5
Hurto	3	4	3	3	3	3

4.3.3. Fase 3: EVALUACIÓN DEL RIESGO.

Para ***Evaluar el Riesgo***, vamos a tomar los resultados que hemos obtenido en la Fase 2, del ***Análisis de Riesgo***, y con ello calcularemos la Evaluación del Riesgo, aplicando las siguientes fórmulas:

EVALUACIÓN del RIESGO					
I Importancia del Suceso	**D** Daño Ocasionado	**C** Carácter del Riesgo	**PR** Probabilidad	**ER** Cuantificación del Riesgo Considerado	VALOR DEL RIESGO
F x S	P x E	I + D	A x V	C * PR	

4.3.3.1. *Cálculo del Carácter del Riesgo "C".*

Para obtener el ***Carácter del Riesgo***, la fórmula es:

C = I + D

Con lo cual debemos de realizar dos operaciones previas, en primera instancia debemos de obtener la ***Importancias del Suceso***, y luego los ***Daños Ocasionados.*** Se parte de los datos obtenidos, aplicando:

Importancia del Suceso (I).				
I =	**F**	**x**	**S**
	Criterio de Función		Criterio de Sustitución

Daño Ocacionados (D).			
D =	**P**	**x**	**E**
	Criterio de Profundidad		Criterio de Extensión

4.3.3.2. *Cálculo de la Probabilidad "PR".*

Para calcular la **Probabilidad del Riesgo**, utilizaremos la siguiente fórmula:

PR = A x V

Vamos a proceder a multiplicar el ***Criterio de Agresión*** x el ***Criterio de Vulnerabilidad***, datos obtenidos den la 2ª fase:

Probabilidad (PR).			
PR =	**A**	**x**	**V**
	Criterio de Agresión		Criterio de Vulnerabilidad

4.3.3.3. *Cuantificación del Riesgo Considerado "ER".*

Se obtendrá multiplicando los valores de "C" (carácter del Riesgo) y "PR" (Probabilidad del Riesgo). Obteniendo el valor total de la ***Evaluación del Riesgo***.

ER = C * PR

4.3.4. Fase 4: CÁLCULO Y CLASIFICACIÓN DEL RIESGO

Es importante comprender que, aunque el resultado es numérico, esta escala es CUALITATIVA.
Cálculo de Base de Riesgo se utiliza la siguiente escala:

Puntaje	Riesgo
Entre 1 y 250	**Riesgo muy bajo**
251 y 500	**Riesgo Bajo**
501 y 750	**Riesgo Normal**
751 y 1000	**Riesgo Elevado**
1001 y 1250	**Riesgo muy elevado**

Esta escala se usa en el ejercicio presentado a continuación:
Ejemplo para un edificio: ***"Riesgos causados por Delitos"***

Tipo de Amenaza	ANÁLISIS RIESGO						EVALUACIÓN RIESGO					Valor del Riesgo
	F	S	P	E	A	V	I	D	C	PR	ER	
							FxS	PxE	I+D	AxV	C*PR	
Robo	4	3	3	3	5	5	12	9	21	25	525	**Normal**
Hurto	3	4	3	3	4	4	12	9	21	16	336	**Normal**

4.3.5. 4.3.5. VALORACIÓN Y RESULTADOS.

En cuanto a las amenazas de carácter antisocial, como se puede observar en el gráfico anterior, las amenazas de robo y hurto, tienen una tendencia más elevada en su probable materialización, generando una valoración del riesgo de carácter "Medio".