# BASC

# GUIA
# de buenas prácticas en SEGURIDAD en la cadena de suministros

BUSINESS ALLIANCE FOR SECURE COMMERCE

Esta guía fue elaborada con el apoyo de la Organización de Estados Americanos OEA a través de la Comisión Interamericana para el Control del Abuso de Drogas - CICAD.

La guía ha tomado como referencia un sinnúmero de documentos entre ellos la Guía de Implementación de Estándares BASC de la Organización Mundial BASC - OMB y los manuales de seguridad para el transporte aéreo, férreo y marítimo elaborados por el Servicio de Aduanas de los Estados Unidos.

TABLA DE CONTENIDO


**1. Antecedentes** **6**
**2. Objetivos** **7**
2.1. Generales 7
2.2. Especí.cos 7

**3. Alcance** **8**

**4. Administración de riesgos** **8**
4.1. Clasificación de los riesgos 8
4.1.1. Especulativos 8
4.1.2. Riesgos puros 8
4.1.2.1. Robos 8
4.1.2.2. Tráfico ilícito 9
4.1.2.3. Terrorismo 9
4.1.2.4. Piratería 9
4.2. Áreas potenciales a exposición de riesgos 9
4.2.1. Bienes o propiedades 9
4.2.2. Responsabilidades 9
4.2.3. Personal 9
4.3. Metodología para el desarrollo de la gestión de riesgos 9
4.3.1. Identificar el contexto 10
4.3.2. Identificación de riesgos 10
4.3.3. Análisis del riesgo 10
4.3.4. Evaluación del riesgo 11
4.3.5. Tratamiento del riesgo 11
4.4. Auditorías 11

**5. Seguridad física instalaciones** **12**
5.1. Perímetro 12
5.1.1. Muros 13
5.1.2. Mallas (Cercas de Alambre) 13
5.1.3. Barreras 13
5.1.4. Concertinas 14
5.1.5. Fijación de puertas en el perímetro 14
5.1.6. Garitas o casetas para personal de seguridad 14
5.1.7. Guardias de Seguridad 15
5.1.8. Alarmas 16
5.1.9. Iluminación 16
5.1.10. Comunicaciones 16
5.1.11. Áreas Externas 16
5.1.12. La comunidad 17
5.1.13. Inspecciones de Seguridad 17

5.2. Parqueaderos 17
5.2.1. Vehículos propios de la compañía y/o arrendados 17
5.2.2. Vehículos de empleados 18
5.2.3. Vehículos de carga 18
5.2.4. Vehículos de visitantes 19
5.3. Estructuras físicas 19
5.3.1. Instalaciones Administrativas 19
5.3.2. Plantas de Producción 20
5.3.3. Bodegas y Áreas de Almacenamiento 21
5.3.4. Vías 21
5.3.4.1. Resistencia 21
5.3.4.2. Iluminación 21
5.3.4.3. Seguros y control de llaves 22

**6. Seguridad Electrónica 22**
6.1. Centros de monitoreo 22
6.2. Control de acceso 23
6.3. Sistemas de Control e identificación de empleados, visitantes y vehículos 23
6.3.1. Políticas 24
6.3.1.1. Restringir ocupación de zonas 24
6.3.1.2. Controlar entrada y salida 25
6.3.1.3. Sincronizar entrada y salida 25
6.4. Circuito cerrado de televisión (C.C.T.V) 25
6.4.1. Matrix de Control 25
6.4.2. Cámaras 26
6.4.2.1. Cámaras Móviles 26
6.4.2.2. Cámaras Fijas 26
6.4.3. Grabación Digital 27
6.4.4. Monitores 28
6.4.5. Fijación de dispositivos y alarmas 28
6.4.5.1. Páneles de Control Contra Incendio 29
6.5. Control Perimetral 29
6.6. Sistemas redundantes o emergentes 30

**7. Seguridad de Personal 30**
7.1. Proceso de selección 31
7.1.1. Perfil del cargo 31
7.1.2. Requisición 32
7.1.3. Reclutamiento 32
7.1.4. Entrevista jefe inmediato 32
7.1.5. Documentación y antecedentes 32
7.1.6. Preselección 33
7.1.7. Exámenes y Pruebas 33
7.1.8. Selección 33
7.1.9. Contratación 33
7.1.10. Inducción y entrenamiento en seguridad 34

7.2. Identificación en las áreas de trabajo 34
7.3. Mantenimiento y conocimiento del personal 34
7.4. Prevención contra conspiraciones internas 35
7.4.1. Programas de incentivos 35
7.5. Análisis de riesgos por cargo 35

**8. Control y seguridad de documentos 36**
8.1. Documentos no electrónicos 36
8.1.1. Política de firmas 36
8.1.2. Plazos para recepción o trámite de documentos 37
8.2. Documentos electrónicos e información sistematizada 37
8.2.1. Protección de los datos 37
8.2.2. Interceptación 37
8.2.3. Copias de seguridad 38
8.2.4. Protección del hardware 38
8.2.4.1. Acceso físico 38
8.2.4.1.1. Medidas de seguridad 39
8.2.4.2. Desastres naturales 39
8.2.4.2.1. Medidas de seguridad 39
8.2.4.3. Alteraciones del entorno 40
8.2.4.3.1. Medidas de seguridad 40

**9. Seguridad de la carga 41**
9.1. Sistemas, procedimientos durante el almacenamiento 41
9.1.1. Áreas para almacenamiento de desperdicios, desechos y/o basuras en general 42
9.1.2. Facilidades previas para la transferencia de responsabilidad con la carga 42
9.1.2.1. Procedimientos para envío y recepción de carga 43
9.1.2.2. Facilidades de ingreso y salida de carga 43
9.1.2.3. Rutas desde y hacia los puntos de cargue y descargue 43
9.1.2.4. Verificación de la Carga 43
9.1.2.5. Recibo de contenedores vacíos para cargue en planta 44
9.1.2.6. Recibo y entrega de contenedores llenos 44
9.1.2.7. Sellos y Precintos 44
9.1.2.8. Alianzas estratégicas de seguridad 45
9.2. Documentación 45
9.2.1. Documentos de la Carga 45
9.2.1.1. Reporte de faltantes, sobrantes o inconsistencias en documentación 45

**10. Selección de Clientes y Proveedores 46**
10.1. Aplicación de medidas de seguridad 46
10.2. Acuerdos 47
10.3. Calificación de proveedores 47

# 1. Antecedentes

La seguridad es un proceso y como tal se ve sujeto a constantes cambios por su permanente dinamismo, debido a factores externos producto de la globalización, las leyes y exigencias aplicadas por las diferentes naciones en torno al comercio internacional y el creciente desarrollo tecnológico. Siempre se resuelven situaciones que aparentemente son sencillas, pero podrían presentar un riesgo de proporciones inimaginables o de alto impacto para la compañía. Para promover el desarrollo, la empresa se debe mover en un campo donde se requieren nuevos medios, nuevos métodos, nuevas técnicas y nuevas tecnologías. Los factores que en la actualidad afectan a la región, están de una u otra forma ligados al narcotráfico.

Para reducir los niveles de inseguridad y mejorar las condiciones del comercio y fortalecer la cadena lícita de abastecimiento, la Organización de Estados Americanos OEA, a través de la Comisión Interamericana para el Control del Abuso de Drogas CICAD, se ha consolidado por múltiples circunstancias y actividades en la primera entidad del hemisferio en canalizar los esfuerzos colectivos de los Estados miembros para reducir la producción, tráfico y el uso y abuso de drogas en las Américas.

Han quedado manifiestos significativos logros en áreas relacionadas con la problemática de las drogas, tales como el desarrollo alternativo, el control de lavado de activos, el control del movimiento ilícito de armas de fuego, el fortalecimiento institucional y el trabajo sobre estadísticas referidas al problema para dar tratamiento al tema del crimen organizado y el terrorismo.

También hubo un aumento en el uso de las tecnologías más modernas en varios proyectos, y una multiplicación de esfuerzos debido a la sinergia creada por el trabajo de la comisión con otras entidades u organizaciones que tienen similares metas y objetivos de cooperación marítima, seguridad portuaria, cooperación aduanera e inteligencia antidrogas.

Dentro de las recomendaciones que deben seguir los países con dichas problemáticas están:

- La creación de una matriz uniforme de evaluación de riesgo/amenaza para evaluar vulnerabilidades y deficiencias en seguridad portuaria, zonas costeras y medios marítimos.
- El desarrollo de un conjunto de leyes y reglamentos (legislación modelo) de control marítimo que los países pueden utilizar en su examen y actualización de leyes y reglamentos para asegurar una jurisdicción y seguridad marítimas adecuadas.
- La elaboración de una guía de operaciones marítimas modelo para la cooperación y coordinación interinstitucional que los países pueden utilizar para organizar los procedimientos operativos nacionales entre entidades de conformidad con las leyes y reglamentos de cada país.
- El análisis y evaluación de los sistemas actuales de recopilación de datos que se utilizan en los puertos y elaborar una guía de referencia que los estados miembros pueden utilizar para el desarrollo o perfeccionamiento de sus sistemas nacionales.

- La elaboración de una guía de sugerencia de mejores prácticas sobre los métodos para el intercambio de inteligencia antidrogas y de información que se utiliza para los programas de seguridad portuaria.

Con base en lo anterior y dentro de un marco de trabajo conjunto con el BASC, se hace necesario tener una guía de consulta permanente que contribuya a mejorar e implementar los procesos de seguridad requeridos y acordes con las exigencias que impone la globalización al interior de toda la cadena de suministro del comercio internacional.

Esta guía de buenas prácticas de seguridad facilitará el proceso de implementación de los Estándares Internacionales y el Sistema de Gestión en Control y Seguridad BASC en todos y cada uno de los actores de la cadena de suministro, con el objeto, entre otros, de minimizar los riesgos derivados del tráfico de sustancias y elementos ilícitos

# 2. Objetivos

### 2.1. Generales

La presente guía, tiene como objetivo fundamental brindar un asesoramiento integral en materia de seguridad y garantizar que se cumpla con los mínimos elementos y estándares de seguridad internacional dentro de las cadenas productivas y en especial para aquellas involucradas directa o indirectamente con el Comercio Internacional. De esta forma, se contribuye a la protección de la cadena de suministro y se hace una excelente prevención y administración de los riesgos durante la distribución física de mercancías, a la vez que:

- Armoniza y estandariza la empresa desde el punto de vista de la seguridad con los requerimientos que a nivel internacional existen.
- Prepara las empresas respecto de los retos que generen los "TLCs", específicamente en el cumplimiento de nuevos requisitos en materia de seguridad.
- Afianza la credibilidad Internacional.
- Incentiva la diversificación de mercados, facilitando la entrada de los productos nacionales a otros países.
- Incentiva el comercio exterior de una manera segura.
- Fomenta la cooperación internacional contra la utilización de mercados lícitos con fines ilícitos.
- Motiva la conformación de equipos de prevención entre el sector privado y las aduanas nacionales y extranjeras.
- Se obtiene la confianza definitiva en las empresas por parte de las autoridades nacionales y extranjeras, minimizando inspecciones intrusivas.
- Reduce las penalizaciones nacionales e internacionales.

### 2.2. Específicos

Esta guía, de igual forma le permitirá a cada uno de los responsables de la seguridad, tener un texto de consulta para orientar sus esfuerzos en materia de seguridad, de tal forma que les sugiere:

- Implementar procesos no existentes en la compañía.
- Prevenir y administrar los riesgos de una manera eficaz y eficiente.

- Optimizar procesos y operaciones dentro de la cadena de abastecimiento.
- Promover y actualizar la normalización y estandarización de procedimientos de seguridad dentro de la cadena de suministro.
- Mantener un ambiente de trabajo seguro.
- Incrementar la productividad.
- Prevenir actos delictivos.
- Reducir el valor de las primas en pólizas de seguros por la correcta administración de riesgos que hace la compañía.
- Disminuir el trámite administrativo ocasionado por reclamos (control de pérdidas y daños).

# 3. Alcance

La presente guía llega a todos los responsables de la seguridad y protección de las empresas dedicadas a actividades industriales y comerciales, de prestación de servicios al comercio exterior o actividades complementarias y/o conexas tales como: fabricantes, exportadores, comercializadores internacionales, intermediarios aduaneros, transportistas, operadores logísticos, comunidades portuarias, comunidades aeroportuarias, empresas de seguridad y vigilancia privada, es decir, a todos los actores dentro de la cadena de suministro.

# 4. Administración de Riesgos

El riesgo como tal tiene efectos directos e indirectos con la naturaleza y el desarrollo operativo del negocio y de la cadena de abastecimiento.

Según la ORM (Operacional Risk Management) los riesgos han sido definidos como el proceso de tomar decisiones que puedan minimizar los efectos de pérdidas que genera la materialización de éstos. Por eso es importante manejarle, medirle y sopesarle sus consecuencias para que le ayude a tomar decisiones para prevenirlo, de manera que el futuro de la empresa dependa de su elección y no de la elección de otros. Un manejo adecuado del riesgo permite que se generen menos pérdidas, que sea menos severo, menos frecuente y más predecible.

## 4.1. Clasificación de los riesgos

Los riesgos se clasifican en especulativos y puros:

### 4.1.1. Especulativos

Son aquellos que permiten ganar o perder y están relacionados con la parte lucrativa u objeto del negocio.

### 4.1.2. Riesgos puros

Son aquellos en los cuales es posible únicamente perder, en esta clase de riesgos, a los que están más expuestos los participantes de la cadena logística del comercio exterior se identifican:

#### 4.1.2.1. Robos
Se dividen en tres clases: Puntual, es decir que está representado por el robo de un solo producto. Sistémico, signi.ca que son robos menores pero frecuentes y finalmente, Organizados, los cuales generalmente son de gran magnitud.

#### 4.1.2.2. Tráfico ilícito
Se entiende como todo comercio al margen de la ley, de las personas, de las mercaderías o de las sustancias.

#### 4.1.2.3. Terrorismo
Se compone por el sabotaje, atentados masivos o selectivos, secuestros y toma de instalaciones.

#### 4.1.2.4. Piratería
Se define como el término aplicado a los delitos cometidos en contra de los medios de transporte.

### 4.2. Áreas potenciales a exposición de riesgos

#### 4.2.1. Bienes o propiedades
Se consideran aquí los riesgos criminales que tienen que ver con el robo, el hurto, la falsificación y el fraude, entre otros.

#### 4.2.2. Responsabilidades
Tiene que ver con las obligaciones que contrae una persona natural o jurídica, como empresa participante del comercio exterior. Dentro de este marco están las obligaciones laborales, fiscales, contractuales, extracontractuales y en general todas las establecidas por las leyes que rigen el comercio exterior en cada país.

#### 4.2.3. Personal
Comprende las compensaciones que se deben pagar por pérdida (despido) de empleados vitales y empleados generales debido a la influencia que el delincuente pueda lograr en ellos.

### 4.3. Metodología para el desarrollo de la gestión de riesgos
En el desarrollo de las operaciones existen diversidad de riesgos, unos relacionados con el entorno, otros con la gestión misma de la función (responsabilidades), los asociados al efecto del quehacer, sobre el medio ambiente, las personas y los bienes o propiedades, entre otros.

En el caso particular del riesgo inherente a la operación logística, establece las siguientes etapas para el control de riesgos:

#### 4.3.1. Identificar el contexto
Se debe definir la misión del proceso logístico desde el punto de vista estratégico, identificando directamente el nivel de riesgo operacional. Por ejemplo, si la promesa de servicio de la compañía es que sus productos estarán en el domicilio del cliente en una

fecha y hora determinada, se condiciona el nivel de riesgo asociado a que un modo de transporte minimice el riesgo de la no entrega.

Para el caso de las compañías exportadoras, evitar el tráfico de drogas, evitar el terrorismo y contrarrestar los robos, el riesgo se condiciona a que las organizaciones al margen de la ley no utilicen los mercados y productos lícitos de la compañía.

Es obvio que a menor riesgo, mayor será la inversión en el control de éste, por lo tanto, la idea es optimizar la inversión, supeditada a un nivel de riesgo establecido y en un servicio definido.

### 4.3.2. Identificación de riesgos

El primer paso para prevenir los riesgos es la identificación de los mismos. Cada exposición a la pérdida o a la materialización de los riesgos puede ser medida en tres dimensiones: El tipo de valor expuesto al riesgo. El peligro que representa la pérdida y la extensión del potencial financiero que pueda traer como consecuencia la materialización del riesgo.

Se analizan todos los procesos de la operación logística para identificar las fuentes de riesgos y sus áreas de impacto, haciendo referencia concreta al daño de la infraestructura, a la organización, al entorno y a los procesos. Desde el punto de vista financiero, los objetivos del análisis son separar los riesgos aceptables menores de los mayores, así como proporcionar los parámetros que sirvan para su evaluación y tratamiento. Los parámetros que normalmente se emplean para calificar el riesgo son la frecuencia y el impacto (severidad) del evento de pérdida.

### 4.3.3. Análisis del riesgo

Incluye la ponderación de las fuentes de riesgo, sus orígenes, sus consecuencias y la posibilidad que éstas ocurran.

El riesgo se analiza mediante la combinación de cálculos de severidad y probabilidad de ocurrencia (frecuencia) en el contexto de las medidas de control existentes. Dependiendo del cuadrante donde se ubiquen las pérdidas, requerirá de atención inmediata a corto plazo. A continuación se muestra la matriz general de exposición a las pérdidas:

Alta severidad y Alta frecuencia **Cuadrante A**
Baja severidad y Baja frecuencia **Cuadrante B**
Baja severidad y Alta frecuencia **Cuadrante C**
Alta severidad y Baja frecuencia **Cuadrante D**


- Las celdas A y D representan pérdidas catastróficas, por lo que requieren de atención inmediata.
- La celda B puede llegar a representar pérdidas sustanciales, si se incrementa la frecuencia.
- La celda C implica baja posibilidad de materialización de riesgos. Esta combinación da como resultado una calificación cualitativa y cuantitativa del

riesgo. Para el caso, pérdida tiene el mismo significado que materialización de riesgos.

### 4.3.4. Evaluación del riesgo

Requiere la comparación del nivel del riesgo hallado durante el análisis con criterios de riesgos preestablecidos y relacionados con la estructura financiera de la compañía o con la cadena de abastecimiento analizada. Una vez identificado apropiadamente el cuadrante de la matriz de exposición a los riesgos, el próximo paso es identificar y examinar las alternativas para controlar o administrar apropiadamente estos riesgos.

### 4.3.5. Tratamiento del riesgo

El riesgo está asociado a medidas de control como: Prevención, protección, transferencia del riesgo y asumir el riesgo. Para la óptima gestión de riesgos, fundamentalmente debe hacerse una mezcla de los aspectos antes anotados.

Lo anterior, además de ser una buena práctica de seguridad que le ayudará a la protección y desarrollo del objeto social de la compañía en mejor forma, le permitirá tener elementos suficientes para negociar con las compañías aseguradoras, ya que en el cálculo de la prima de riesgo de un seguro influye el grado de implementación de las estrategias de mitigación o prevención.

Evitar la exposición a los riesgos es eliminar la posibilidad para que un riesgo ocurra, es tomar la decisión de eliminar una particular actividad, operación o medio que causaría una muy posible oportunidad para perder.

En algunos casos es necesario cambiar completamente la forma o el procedimiento en que se viene desarrollando una actividad. Las medidas preventivas de seguridad son la estrategia que se debe seguir dentro de las operaciones de administración del riesgo y para lograr esto, los indicadores son el mejor método o factor de medición para tomar las acciones preventivas correspondientes. Afortunadamente la mayoría de indicadores en la compañía, como los de tipo financiero, de productividad, de calidad y de tiempo están relacionados con los de riesgo. Un ejemplo de esto se aprecia de la siguiente forma: Entre más prolongado sea el tiempo de tránsito de una mercancía por carretera, mayor será la exposición y el riesgo de transporte asociado.

## 4.4. Auditorías

Debe elaborarse un plan de auditorías internas y externas para establecer que las políticas, procedimientos y demás normas de control y seguridad establecidas e implementadas se cumplan adecuadamente. Tenga en cuenta que éstas le apoyarán en la detección de vulnerabilidades presentes o futuras. Las auditorías internas deben ser realizadas por personas ajenas a las áreas o dependencias que se están auditando y en el caso de las auditorías externas, tenga en cuenta cumplir las recomendaciones y estándares mínimos, que en materia de seguridad, contemplan los programas como ISPS, BASC, etc.

Tenga en cuenta examinar los planes de respuesta a eventos críticos y aplicarse procedimientos de contingencia y emergencia para el caso de amenazas comprobadas o fallas en las medidas de protección.

## 5. Seguridad Física - Instalaciones

Cuando se habla de seguridad física se refiere a todos aquellos medios (humanos, animales), mecanismos (naturales, físicos, mecánicos, electromecánicos, electrónicos) y medidas (políticas, procedimientos, órdenes permanentes, instructivos de seguridad) que generalmente tienen carácter restrictivo a manera de prevención y de detección destinado a proteger como su nombre lo indica, físicamente todos los recursos disponibles en la compañía.

Todas las medidas que se adopten deben ir unidas, enlazadas y coordinadas entre si, quiere decir, que la seguridad física, debe ser un sistema integrado de protección.

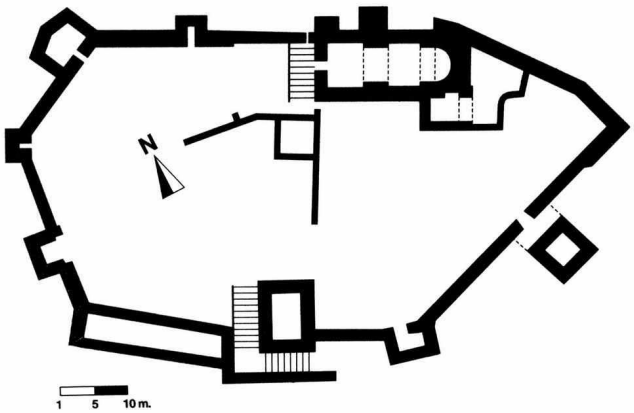
Dependiendo del entorno, de los mismos recursos y de los sistemas a proteger, se aplicarán y utilizarán en mayor o menor grado las medidas y mecanismos de prevención, detección y restricción.

A continuación se mencionan aspectos básicos de seguridad que permiten revisar las acciones de seguridad que debe tener implementadas la compañía y las medidas que se pueden tomar para hacer una excelente administración de los riesgos.

### 5.1. Perímetro

Por ser la línea fronteriza que señala claramente el límite de la propiedad privada, debe gozar de sistemas especiales de construcción que impida el paso de personas y/o vehículos desde y hacia el exterior de la compañía. Así mismo debe tener claramente definidas las vías de aproximación a cada una de sus puertas vehiculares y peatonales.

El principio básico, que se describe a continuación, lo conforman las barreras físicas, los sistemas mecánicos, electromecánicos y sistemas de control electrónico:



### 5.1.1. Muros

Se recomienda que estén construidos en materiales compactos y resistentes, con el fi n de prevenir o retardar el rompimiento ante una posible intrusión, su altura mínima debe estar en los 2,50 metros y superpuesto a éstos, elementos como (Mallas, Concertinas, Estacas) que conlleven a disuadir y dificultar cualquier posible escalamiento; de igual forma, deben evitar la fuga y/o ingreso de productos y/o materiales desconocidos cuando la delincuencia utiliza métodos de lanzamiento. Los muros, deben estar lo suficientemente separados de las edificaciones, de tal forma, que siempre permitan la visualización y reacción oportuna por parte del componente de seguridad humana y/o animal.

### 5.1.2. Mallas (Cercas de Alambre)

De igual forma que los muros, las cercas deben tener las mismas características y condiciones de seguridad; éstas pueden utilizarse también en la parte superior de los muros antes de la concertina.

.

### 5.1.3. Barreras

Cuando se utiliza solamente malla en el perímetro, es posible acondicionar o construir internamente una segunda barrera paralela a la malla principal y pegada a ésta, con árboles frondosos, erguidos y de espinas naturales, o también un segundo cerco a una distancia entre 2 y 3 metros de separación de la malla principal, o en la parte exterior a la malla principal, construir zanjas anchas y profundas.

### 5.1.4. Concertinas

Las concertinas tienen como función disuadir y/o retardar la acción del intruso, éstas se ubican de acuerdo con el estudio de seguridad de la compañía y el análisis de riesgos. Bien pueden ir en la parte media interna del muro o malla, en la parte superior de éstos o en la parte baja cuando encontramos doble malla de zonas de acceso en bajamar como en el caso de los terminales marítimos en los puertos y muelles privados.

### 5.1.5. Fijación de puertas en el perímetro

Sería imposible definir el número de puertas o accesos perimetrales que requiere una compañía debido a la complejidad de las áreas que ocupa cada una, lo que si es seguro, es que deben ser las mínimas necesarias para proveer el adecuado acceso a los parqueaderos internos de la planta, a las áreas de almacenamiento, zonas de cargue y de descargue.

Las puertas construidas en las zonas donde haya concentración de personal deben ser construidas de acuerdo con los principios exigidos de seguridad industrial, de tal forma que permitan la evacuación en caso de siniestros o desastres naturales y de igual forma precisarlo cuando se fije la seguridad electrónica de control de acceso.

Estas puertas deben proveer una defensa contra los accesos de personas y vehículos no deseados, por lo tanto, se recomienda que además de la nave o naves que conforman la estructura de la puerta, también se incluyan otras barreras físicas de seguridad tales como talanqueras o “uñas de gato” entre otras. El proceso de registro e inspección de personas y vehículos debe quedar establecido de acuerdo con los sistemas disponibles en la compañía y políticas de control adoptadas.

### 5.1.6. Garitas o casetas para personal de seguridad

La seguridad perimetral, requiere de garitas en la periferia cuando las instalaciones son extensas y sobre todo, si los límites son alejados de construcciones tales como plantas de producción, bodegas de almacenamiento, talleres o edificios administrativos, entre otros. Previo el análisis de riesgos y el sitio donde serán ubicadas las garitas señalará, si deben ser elevadas o por el contrario, al nivel del terreno, los turnos de labor en que deben ser ocupadas, entre otros, aspectos que se desarrollarán más adelante.

Las casetas se utilizan donde las compañías tienen manejo de grandes cantidades de carga, inventarios costosos, materias primas o sustancias controladas, en todas las entradas y salidas activas para vehículos, especialmente en las horas destinadas para realizar labor de despacho, recibo de carga y en las puertas destinadas para el ingreso y salida de personal.

**5.1.7. Guardias de Seguridad**

Sea la seguridad con personal propio, subcontratado o suministrado y dependiendo del tamaño de la compañía, se debe tener claro que a este personal le corresponde una actividad paralela a las actividades operativas. Su función es proteger las instalaciones y requiere que un representante de la compañía cumpla funciones como responsable de esta seguridad.

En el perímetro, incluyendo los accesos vehiculares y peatonales, se requiere que haya seguridad preferiblemente armada ya que es la línea física que fija la frontera entre la compañía y la comunidad. El número de puestos, turnos a emplear y medios a utilizar lo dará el análisis de riesgos realizado acorde con el estudio de seguridad.


Como recomendaciones especiales, es importante que en grandes compañías tanto por sus instalaciones y/o número de trabajadores, se utilicen los servicios de varias compañías de seguridad, haciendo rotación sobre las mismas funciones y puestos asignados; de este modo, se estimula la calidad, el compromiso con la empresa y los resultados en la prestación del servicio. Exija la correcta uniformidad y diferenciación del personal de seguridad del resto de personal de la compañía, detálleles con claridad las funciones que debe cumplir el personal de seguridad, de acuerdo con cada puesto de trabajo o sitio donde preste su labor, veri. que permanentemente que la compañía que le presta servicios de seguridad, mantenga tan pendiente de su personal, como su compañía lo mantiene de la suya, haga ensayos, simulacros y pruebas de seguridad periódicamente y evitará que el personal de seguridad caiga en la rutina, exija 3 turnos para los puestos que ocupa durante 24 horas, definitivamente usted necesita personal atento y con capacidad de reacción en todo momento.

### 5.1.8. Alarmas

Las alarmas tempranas en el perímetro que acompañan la labor que cumple el personal en puertas, garitas y casetas de seguridad, pueden estar constituidas por medios animales que tienen gran capacidad de detección a través de sus signos vitales tan desarrollados como el oído y el olfato, entre los animales más comunes encontramos los Gansos y los Perros. Adelante se explicarán los medios electrónicos y eléctricos utilizados.

### 5.1.9. Iluminación

La excelente iluminación del perímetro y de las estructuras ubicadas sobre éste, se convierten en el principal factor preventivo y disuasivo de actos ilegales y de conspiraciones al interior de la compañía. Es muy importante la ubicación de reflectores con gran capacidad para proteger tanto áreas externas como internas. Éstos deben contar con sistemas emergentes o redundantes que permitan mantener el fluido eléctrico ante la caída del sistema principal y garantizar un mejor funcionamiento de las cámaras del circuito cerrado de televisión instaladas.

### 5.1.10. Comunicaciones

Las estructuras ubicadas en el perímetro, tales como garitas, casetas de seguridad, puertas, entre otras, deben contar con los recursos apropiados que permitan una fácil comunicación, en ellas se pueden instalar líneas telefónicas, radios portátiles, alarmas sonoras, destellos, etc.

### 5.1.11. Áreas Externas

Las áreas externas al perímetro, son áreas de influencia para el responsable de la seguridad, también debe haber prevención a partir de lo que suceda en extramuros. Se debe procurar y/o controlar que el perímetro externo se mantenga lo menos contaminado visualmente que se pueda y no se convierta en zonas de estacionamiento vehicular permanente, zonas de ventas informales, zonas de depósito de basuras o escombros, zonas de libertinaje, zonas de negocios ilícitos de venta de drogas, etc.

### 5.1.12. La comunidad

La comunidad alrededor de las instalaciones juega un papel importante y debe ser tenida en cuenta entre los aspectos de seguridad, se debe conocer quienes son los vecinos y saber a ciencia cierta a que actividades se dedican. Las compañías no siempre están ubicadas en parques industriales y no todas las que están en los parques industriales asumen la seguridad como un factor determinante en el desarrollo de la empresa.

Incluya la comunidad circundante en los programas de apoyo, desarrollo y mejoramiento de calidad de vida del sector, con esto gana aliados que necesita para prevenir y proteger a la compañía de actividades en su contra.

### 5.1.13. Inspecciones de Seguridad

Las revisiones del perímetro tanto interno, como externo, deben ser permanentes, con el objeto de garantizar que se cumpla lo señalado para el punto 5.1, es decir, que se encuentren libres de escombros, árboles, escaleras, chatarra, basura y/o artefactos que permitan un apoyo para el escalamiento y por ende que sea violada su integridad. De igual forma debe garantizarse que los sistemas de iluminación y alarmas funcionen perfectamente. Muros, cercas, mallas, concertinas y puertas se encuentren en perfecto estado, control de parqueo, trabajos públicos, llegando hasta inspeccionar los sistemas de drenaje del alcantarillado. El responsable de la seguridad debe desarrollar procedimientos, implementar sistemas y formatos de control que le permitan evaluar, anticipar y reaccionar con oportunidad ante cualquier posible evento crítico. Estas inspecciones no reemplazan a las auditorias del Sistema de Gestión en Control y Seguridad que periódicamente deben realizarse.

## 5.2. Parqueaderos

Se ha visto como la organización, el orden, la iluminación, el control, entre otras, juegan un papel importante dentro de la seguridad perimetral, ahora se aplican estos mismos principios y se definen políticas de segregación e independencia, para lo cual se proponen 4 zonas independientes de estacionamiento:

### 5.2.1. Vehículos propios de la compañía y/o arrendados

Por ser parte de los activos de la compañía o por haber una responsabilidad frente a éstos, tienen la prioridad de asignación de espacios en zonas próximas a los edificios administrativos. Generalmente, son vehículos asignados a dependencias de altos ejecutivos y los espacios deben estar debidamente demarcados, señalizados y asignados.

Se recomienda proveer estos vehículos de un distintivo especial suficientemente visible, de tal modo que garantice la labor de control en sitio. En los sistemas de control de acceso debe identificarse claramente su asignación, características del vehículo y el récord de entradas y salidas. Por ser esta una zona especial cerca a los edificios

administrativos, se recomienda mantener espacios sin asignación, para las personalidades que visitan la compañía.

### 5.2.2. Vehículos de Empleados

Son parte del patrimonio del talento humano, por lo tanto se debe resolver su mayor preocupación antes de iniciar labores. Esta zona debe estar ubicada equidistante a todas las dependencias debido a la multiplicidad de labores a realizar. De igual forma, se recomienda proveer estos vehículos de un distintivo especial suficientemente visible que permita la labor de control en sitio. En los sistemas de control de acceso debe identificarse claramente su propietario, características del vehículo, que evitarán entradas fraudulentas y el récord de entradas y salidas del mismo. En caso de no haber espacio suficiente para implementar la zona de estacionamiento de vehículos para empleados, es recomendable hacer convenios con zonas de parqueo seguras, aledañas a las instalaciones, que estén legalmente constituidas y concentrar todos los vehículos allí.

### 5.2.3. Vehículos de Carga

Por lo general, estos vehículos son de fácil reconocimiento e identificación, las empresas con las que se suscriben contratos de transporte regularmente asignan los mismos conductores y los mismos vehículos para que cubran determinadas rutas, los cuales se pueden matricular fácilmente en el sistema de control de acceso.

Lo recomendable es hacer una buena planificación y coordinación de la logística de recibo y despacho de mercancías, garantizando que las plataformas y/o puertas de cargue y descargue, sean únicamente los espacios utilizados por estos vehículos al interior de la compañía, las rutas de llegada y salida a estas zonas deben estar perfectamente definidas y señalizadas, garantizando el tránsito de estos vehículos por sitios específicos dentro de las instalaciones.

Cuando la demanda de vehículos de carga es superior a la capacidad de cargue y descargue, se recomienda que la zona de estacionamiento sea contigua a la báscula, es decir, próxima a la puerta de acceso y salida de suministros, manteniendo la prioridad de ingreso para los vehículos cargados.

Los vehículos que ingresan o se retiran con carga deben ser revisados de acuerdo con las listas de chequeo establecidas para tal .n y acorde con los documentos que protocolizan los hechos.

Los vehículos vacíos que ingresan o salen de la compañía, deben hacerlo con sus compuertas abiertas, carpas recogidas y sometidos a una inspección por parte del personal de seguridad. Recuérdele permanentemente al personal de seguridad que los vehículos vacíos que ingresan a cargar mercancía deben ser previamente verificados con lista de chequeo y de no encontrarse de acuerdo con los parámetros exigidos por la compañía, debe ser rechazado antes de su ingreso, de esta forma, se inicia la prevención y reducción de la siniestralidad de la carga.

### 5.2.4. Vehículos de Visitantes

Casi siempre los visitantes son proveedores de servicios, contratistas, vendedores o entidades de beneficencia. En lo posible el estacionamiento para este grupo debe estar por fuera de las instalaciones, se debe prohibir que vehículos particulares con pasajeros estacionen en zonas de cargue y descargue de mercancías, en zonas inmediatamente adyacentes a los edificios donde se almacena carga.

En lo posible, este grupo de personas debe ser acompañado por el personal de seguridad hasta el sitio donde es solicitado y sus desplazamientos por el interior de la empresa deben estar debidamente demarcados y señalizados.

### 5.3. Estructuras Físicas

Cada edificio, bodega, hangar, taller, vía y/o plataforma construida, ha obedecido a diseños encaminados a satisfacer una necesidad desde el punto de vista logístico, administrativo, operativo y/o de producción, sobre el cual se fija el esquema y parámetros de seguridad.

Cuando se piensa en remodelación, acondicionamiento y/o construcción de nuevas edificaciones, se requiere conformar grupos interdisciplinarios que apoyen la toma de decisiones. No se debe esperar a la terminación de las obras, debe hacer parte fundamental del planeamiento, diseño, ejecución y puesta en marcha de las mismas, puesto que allí serán ubicados activos, nuevos procesos de la compañía y de alguna u otra forma se alterará el esquema de seguridad.

Igualmente, los edificios administrativos, plantas de producción, zonas de almacenaje, bodegas, talleres, etc., reclaman un dispositivo con personal de seguridad que brinde la debida protección, que realice las debidas inspecciones diarias de seguridad y garanticen mantener en forma permanente la integridad de las estructuras. El responsable de la seguridad debe desarrollar procedimientos, implementar sistemas y formatos de control que le permitan evaluar, anticipar y reaccionar con oportunidad ante cualquier evento crítico.

A continuación se enuncian aspectos a tener en cuenta sobre las recomendaciones para el desarrollo de este tipo de obras desde el punto de vista de seguridad.

Con base en los criterios de construcción, el responsable de la seguridad tendrá elementos de juicio suficientes para recomendar el dispositivo de personal de seguridad requerido y orientar el diseño de la seguridad electrónica a utilizar.

### 5.3.1. Instalaciones Administrativas

Por ser espacios exclusivos para concentración de personas, equipo de oficina, documentación, información y comunicaciones es muy importante contar con el aval, decisión y participación de la alta gerencia,

de tal forma que garantice el desarrollo y cumplimiento de los programas, procedimientos e instructivos de prevención implementados y tendientes a garantizar la integridad de las personas que ocupan el lugar, de los activos de la empresa y del secreto profesional manejado a través de los “DOCUMENTOS” escritos y sistematizados.

El responsable de la seguridad, siempre debe disponer de planes y medidas de evacuación los cuales debe ensayar periódicamente de tal forma que estén de. nidos los eventos para cada contingencia y que los líderes de las brigadas de emergencia conozcan perfectamente qué hacer, cómo hacerlo y se utilicen todos los recursos disponibles. Los planes contingentes deben incluir zonas de concentración para la alta dirección y ante eventos terroristas, evacuarlos de la compañía a través de salidas especiales de emergencia.

Los aspectos de seguridad industrial y el plan de evacuación deben contemplar el uso y manejo de llaves, uso de ascensores, escaleras y puertas de salida, de emergencia, señalizadas rutas y pasillos, ubicados gabinetes e instalados los sensores del sistema de riego contra incendio, iluminadas perfectamente las áreas de trabajo de cada edificio, entre otras.

Los activos, deben estar asignados y entregados por actas bajo un responsable directo, marcados e inventariados evitando sustituciones. Deben estar procedimentadas las bajas, altas, traslados y reemplazos.

El manejo y seguridad de la documentación e información, será tratado en capitulo independiente de igual forma que la seguridad electrónica.

### 5.3.2. Plantas de Producción

Son puntos neurálgicos de la compañía, allí se concentra la razón de ser, el objeto social, en esta infraestructura están ubicados los principales activos de la compañía.

Para establecer los planes de seguridad se deben conocer las instalaciones en profundidad y especialmente cada uno de los procesos productivos. Los técnicos de producción serán las personas que apoyen la labor de definición del esquema de seguridad a desarrollar, ellos manejan las normas técnicas aplicables en la elaboración de los productos y las normas de seguridad e higiene industrial. Desde el punto de vista de seguridad física y administrativa es recomendable que las plantas permanezcan operadas con el personal mínimo necesario, se compartimente la información, se establezcan procedimientos de inventario y se mantengan los registros escritos para la recepción de materias primas, empaques y entrega de producto terminado. El manejo de basuras y residuos debe obedecer a un estricto control y debe integrarse de manera eficiente a los medios disponibles de seguridad electrónica.

### 5.3.3. Bodegas y Áreas de Almacenamiento

Los almacenes y bodegas son áreas totalmente restringidas, el uso debe ser exclusivo para quienes operan las mismas.

El control de acceso y blindaje, será de. nido con base en las necesidades y ubicación de la bodega o zona de almacenamiento, las personas que operan las mismas, deben estar comprometidas, con funciones asignadas de seguridad, además de las que les corresponde dentro de la labor operativa.

En el capitulo relacionado con la seguridad de la carga, se retomará el tema por la importancia y alto grado de riesgo que en materia de seguridad representa para la empresa.

### 5.3.4. Vías

El ordenamiento vial de la compañía debe demarcar, definir e identificar claramente el sentido de las mismas, debe poseer señalización informativa, preventiva y reglamentaria que regule y normalice el tránsito, permanencia y estacionamiento de vehículos y personas al interior de la empresa. Se debe evitar el estacionamiento temporal o permanente de acuerdo con las recomendaciones anteriores. En este aspecto, se hace imprescindible incluir las rutas de aproximación desde el exterior hasta el interior de la compañía evitando siempre el estacionamiento de vehículos y proliferación de ventas informales y tránsito de personas en el perímetro externo de las instalaciones.

A continuación se verán algunos aspectos importantes a tener en cuenta durante el desarrollo de cualquier proyecto de construcción:

#### 5.3.4.1. Resistencia

El análisis de riesgos que se elabore debe partir de la destinación que se le va a dar a la construcción, seguidamente pensar en los activos que allí se ubicarán y finalmente en la logística operativa u administrativa que se manejará en el lugar. Las conclusiones deben llevar a determinar la ubicación, vulnerabilidad, exposición al riesgo y las medidas de seguridad que se deben aplicar; obviamente estos conceptos serán tenidos en cuenta por los especialistas encargados del diseño, quienes traducirán estos requerimientos en la calidad de sus estructuras, muros, pisos, techos, ductos, puertas, ventanas, etc.

#### 5.3.4.2. Iluminación

Por tratarse de construcciones que generalmente son cerradas, la iluminación provista debe obedecer tanto a factores de seguridad física, como de seguridad industrial, esta estará determinada por las actividades a desarrollar en cada edificio, por la organización de cada uno de sus espacios, por la cantidad y clase de maquinaria, por la destinación de las mismas dependencias, por la cantidad de personas que laboren y el horario de trabajo asignado. Siempre se debe tener en cuenta sistemas de respaldo que garanticen la continuidad del fluido eléctrico, en especial para puntos de almacenamiento de cargas

valiosas, sustancias controladas, sitios neurálgicos para la seguridad y en áreas de ejecución de procesos vitales para la compañía.

#### 5.3.4.3. Seguros y control de llaves

Los seguros y las llaves utilizadas en cada estructura física y equipo con que cuente la compañía, deben tener la debida protección para impedir accesos no autorizados a éstas. El control debe estar en manos del responsable del área o del personal de seguridad. Se recomienda elaborar y difundir un procedimiento o instructivo de carácter general donde se le indique al personal el manejo de llaves, contar con un armario para el almacenamiento general de llaves, el responsable de la seguridad que se encuentre de turno debe mantener un dispositivo con la llave de la cerradura del armario, contar con un registro y acta de entrega de llaves de áreas de alto riesgo, en lo posible no permitir sacar llaves fuera de la empresa, registrar toda pérdida de llaves, no entregar copias sin el debido control. El capítulo correspondiente a seguridad electrónica retomará aspectos sobre el control de acceso y llaves electromagnéticas y biométricas.

## 6. Seguridad Electrónica

El desarrollo de sistemas y mecanismos electrónicos de seguridad avanza al ritmo de la tecnología informática; cada día se encuentran nuevos avances en sistemas de alerta temprana o sistemas de detección que apoyan y responden eficaz y eficientemente en la labor de seguridad ya que brindan la confianza y certeza que se requiere para tomar decisiones e implementar nuevos procedimientos y mecanismos de control en forma acertada, disminuyendo los riesgos y responsabilidades que recaen sobre el personal de seguridad armada y sobre todo por el papel preventivo, disuasivo e informativo cuando de conspiraciones internas se trata.

A continuación se observarán aspectos importantes en la materia, que contribuyen a mejorar la seguridad de la compañía durante sus operaciones de Importación, Exportación, Almacenamiento, Manipulación e Inspección de mercancías. Se recomienda publicar en áreas de tránsito y de mayor riesgo en la compañía avisos informativos de la seguridad con que cuenta y enunciar su importancia en el cumplimiento de estándares internacionales.

Los sistemas de seguridad electrónicos se utilizaban sólo en grandes organizaciones y corporaciones para proteger objetos de alto valor. Ahora, todo tipo de empresas grandes y pequeñas, deben mostrar un especial interés por implementar estos sistemas debido a que son una realidad alcanzable que ayuda a optimizar y a alcanzar niveles superiores de e. ciencia a menores costos.

### 6.1. Centros de Monitoreo

En los centros de monitoreo se pueden concentrar todos los elementos y aspectos básicos de control y seguridad, centralizando y anticipando la toma de acciones preventivas, disuasivas y correctivas. Desde este sitio se podrán dirigir las acciones a seguir durante el manejo de crisis.

El centro de monitoreo debe ser operado por personal ajeno a las actividades de seguridad armada y operativa. El centro de monitoreo debe manejar políticas duras de acceso y mantener el acceso restringido a sus operadores y de acuerdo con el per. l de cargos a quien el responsable de la seguridad autorice. El centro de monitoreo debe tener los planos actualizados de la ciudad donde se encuentra la compañía, deben estar perfectamente señalizadas en lo posible las viviendas de todos los trabajadores, especialmente, aquellos que de acuerdo con el análisis de riesgo presentan mayor vulnerabilidad. En el plano deben estar perfectamente definidas y señalizadas las rutas de aproximación y de evacuación desde y hacia la compañía. Desde el centro de monitoreo se puede controlar el circuito cerrado de televisión, control de acceso, alarmas de intrusión, robo, incendio, cumplimiento de las normas de seguridad y operativas establecidas, las comunicaciones de la compañía. Los operadores del centro de monitoreo deben estar enterados en forma permanente de la ubicación de ejecutivos, unidades de transporte de carga, escoltas etc.

### 6.2. Control de Acceso

Los sistemas cuentan con módulos integrados de hardware (servidores, redes, paneles de control ISC) y software (Programa de administración) con capacidad para hacer múltiples tareas y múltiples usuarios.


El software se ejecuta sobre sistemas operativos convencionales y se comunica con múltiples estaciones de trabajo sobre la red, donde a través de paneles se registra y almacenan datos que le permiten la toma de decisiones en cuanto a los niveles de acceso, horarios, políticas de control de acceso e identificación. Los sistemas le garantizan el cumplimiento de funciones tales como: El control de acceso, administración de alarmas, instalación de mapas gráficos dinámicos, monitoreo y control de sitios, administración de reportes y Carnetización.

Se pueden integrar al sistema de nómina y se pueden configurar de acuerdo con la estructura y complejidad de la distribución arquitectónica que presente la edificación.

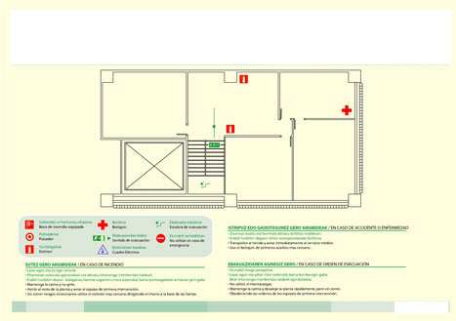
Se observó en el capítulo de seguridad física que el control de acceso debe estar presente en todas las puertas de acceso y salida de la compañía, sitios de alto riesgo de los edificios administrativos, bodegas y zonas de almacenamiento, etc.

### 6.3. Sistemas de Control e identificación de empleados, visitantes y vehículos

Los empleados deben conocer y transmitir a través de sus actuaciones al interior de la compañía las políticas en materia de seguridad adoptadas. Sin duda alguna las restricciones durante el control de acceso conllevarán a disminuir y eliminar riesgos de robo, tráfico ilícito, terrorismo y piratería entre otros.

El control de acceso está configurado para establecer una base de datos con la información necesaria y fotográfica del personal que labora en la empresa, asignándole una tarjeta que posee un número programado, encriptado y almacenado en un chip que sólo identifica la respectiva lectora. También a través de sistemas biométricos que recogen rasgos y aspectos físicos propios de cada persona, como la geometría de la mano, la huella dactilar, el iris, la voz, los cuales asociados a otros elementos de verificación y confrontación como su identificación o un PIN (Número de Identificación Personal) les permite acceder a las instalaciones.

Se recomienda mantener el control sobre las horas a las cuales los trabajadores, visitantes y vehículos acceden a las instalaciones, mantener el control de gestión sobre actividades y tiempo de ejecución de las mismas, no permitir el ocio dentro de las instalaciones, disponer de un mapa donde se muestren las áreas de paso y permanencia prohibidas y restringidas para cada tipo de empleado, implementar la revisión física de las personas, paquetes y vehículos.



Todo el personal de la compañía y en general toda persona que haya ingresado a las instalaciones, deberá estar debidamente identificada, bien sea a través de medios electrónicos o utilizando medios gráficos de identificación ya sea por color, numeración o que sus inscripciones identifiquen y faciliten el control visual a través del circuito cerrado de televisión y garanticen el cumplimiento sobre las áreas a las cuales puede acceder y en cuáles debe permanecer. Se recomienda que la tarjeta de identificación sea portada en lugar visible y lleve como mínimo las características físicas del empleado o visitante, su fotografía a color, su firma y una fecha de vencimiento razonable; el uso de escarapelas, brazaletes o collares deben ir en comunión con las medidas de seguridad industrial para evitar accidentes de trabajo.

### 6.3.1. Políticas

De. nido e implementado un sistema de control de acceso, debe proceder a generar las políticas convenientes para la seguridad de cada una de las puertas y zonas controladas, de tal forma que pueda, entre otras:

#### 6.3.1.1. Restringir ocupación de zonas

Esta política especifica el número máximo de ocupación de una zona. Será útil en parqueaderos y zonas de alta seguridad como bodegas y zonas de alistamiento de producto. Esta política, se considera dura debido a que niega el acceso cuando llega al límite permitido en el lugar.

### 6.3.1.2. Controlar entrada y salida

Se usa en conjunto con lectoras de entrada y salida para monitorear y controlar el paso de los usuarios entre zonas o áreas definidas.

### 6.3.1.3. Sincronizar entrada y salida

Se asigna a una lectora para prevenir reingresos antes de la expiración de un período de tiempo asignado.

Esta política de control de acceso define el tiempo que una persona o un grupo de personas pueden estar en una zona. Si una o el grupo no abandonan la zona en el período de tiempo asignado, el sistema debe generar un mensaje de violación, el cual podrá ser de. nido como una alarma.

## 6.4. Circuito cerrado de televisión (C.C.T.V)

Las condiciones de seguridad y situaciones que a diario se presentan en las compañías, requieren que el esfuerzo
humano sea complementado con sistemas de control electrónico que además de reducir los costos por disminución del dispositivo de seguridad, demuestran y certifican hechos ocurridos al interior de la compañía, garantizándonos la toma de mejores decisiones.

Un sistema de CCTV ofrece la oportunidad de tener mayor cobertura, controlar, obtener evidencia veraz y de primera mano sobre lo que sucede en el perímetro interno y externo, rutas de aproximación y vías internas de la compañía, zonas de estacionamiento, zonas de almacenamiento, zonas de producción y empaque, áreas de trabajo, es decir, se puede llegar a cualquier sitio, logrando resultados más satisfactorios y un mayor desempeño y tranquilidad en la función de seguridad.

En los sistemas de CCTV básicamente se identifican cuatro componentes principales: Matriz de control, Cámaras, Dispositivos de almacenamiento de video y las redes.

### 6.4.1. Matrix de Control

Un sistema matricial cuenta con un software de administración desde el cual se realiza la configuración del sistema, por ser un sistema de configuración modular, se puede adaptar a las necesidades de cualquier compañía y le permite tener el control centralizado de todas las cámaras que se encuentren activas.

Por ser modular, le permite la expansión gradual de cámaras, monitores y/o controladores hasta la capacidad máxima que tenga la CPU.

### 6.4.2. Cámaras

Las cámaras son los dispositivos periféricos de captura de imagen, las cuales se ubican de acuerdo con la evaluación de riesgos establecida en las zonas a controlar y teniendo en cuenta las áreas muertas por barreras físicas y/o naturales que se presenten. Dependiendo de la funcionalidad (Fija y Móvil), características requeridas (Color, Superdinámica y Blanco y Negro), condiciones de luz (Interna y Externa), tipo de luz, se deben considerar varios tipos de cámaras.

#### 6.4.2.1. Cámaras Móviles

Dentro de este tipo de cámaras, se consideran 2 tipos:

(1) las que vienen con su dispositivo autónomo de movimiento conformado por un conjunto de cámara y housing. Estas cámaras operan a color en condiciones normales de iluminación y pueden conmutar a operación en blanco y negro de forma manual o automática cuando la iluminación se hace insuficiente. Estas cámaras, dependiendo de la
marca y modelo, vienen con un zoom óptico desde de 4 a 88 mm (zoom óptico de 22X, zoom digital de 10X para un total de 220X), de igual forma poseen 64 posiciones programables (presets) que se pueden activar en forma manual o automática ante eventos de alarma y una ruta de patrulla programable mayor de 30 segundos.

Estas cámaras giran horizontalmente 360o sin . n y 180o verticalmente.

Al momento de moverse el mecanismo verticalmente de + 90o a -90o, al momento de mirar al piso la imagen se invierte automáticamente en forma digital, es decir, el mecanismo no gira horizontalmente alargando la vida útil del mecanismo.

(2) Cámaras . jas que requieren de un complemento de rotación y control adicional llamados unidades de movimiento, a estas cámaras se les puede instalar iluminadores infrarrojos para tener mejor rendimiento en extremas condiciones bajas de iluminación.

#### 6.4.2.2. Cámaras Fijas

Las cámaras fijas utilizan diferentes tipos de lentes. Entre éstos, encontramos los varifocales auto iris que van desde de 5 - 40 mm hasta 3,8 a 8 mm y se usan dependiendo el área a cubrir. Las cámaras más comunes son:

(1) Cámaras a Color normales: Especiales para operación en condiciones normales de iluminación, éstas no deben ser utilizadas donde haya contrastes de luz marcados, ni presencia de luz amarilla.

(2) Cámaras Superdinámicas: Son cámaras conmutables Color / blanco y negro, especiales para escenas con contraluz, permitiendo que en estas condiciones la imagen se vea claramente tanto en la parte interna (sombra) como en la externa (luz). Estas cámaras operan a Color en condiciones normales de iluminación y pueden conmutar a operación Blanco y negro en forma automática cuando la iluminación se hace insuficiente, por lo cual son apropiadas para uso en exteriores.

(3) Cámaras a Blanco y negro: Especiales para las áreas donde se tengan bajos niveles de iluminación como por ejemplo en áreas perimetrales y bodegas con baja iluminación.

### 6.4.3. Grabación Digital

Los nuevos equipos, combinan la multiplexación de 16 señales de video con grabación digital en disco duro que van desde los 120 hasta de 160 GB y con una amplia capacidad de expansión. Adicionalmente poseen 16 entradas de alarma, zoom digital, grabación de audio y dos salidas a monitor (Spot y Multiscreen). También manejan el sistema triplex, es decir, que permite visualizar, grabar y reproducir simultáneamente.

Permiten definir cuatro grupos de cámaras con el . n de establecer cuatro videograbadoras virtuales, cada grupo de cámaras se puede asignar hasta con cuatro programas diferentes, y cada programa maneja hasta cuatro horarios, los cuales pueden ser programados para grabar de un modo especí. co. En resumen, es posible optimizar el uso del disco duro programando por ejemplo las cámaras de o. cinas a grabar de lunes a viernes de 7 a.m. a 12 m en modo equivalente a TL 2 horas, de 12m a 2 p.m. en modo TL 8 horas, de 2 p.m. a 6 p.m. en modo TL 2 horas y de 6 p.m. a 7 a.m. con grabación ante alarma de movimiento en modo multishot. Las posibilidades son muchas, son equipos diseñados exclusivamente para sistemas de CCTV, poseen interfaces de manejo adecuadas para las labores de los operadores. La selección de las funciones están disponibles desde las teclas del panel frontal y posee un comando circular. Esta disposición de los comandos permite la activación rápida de las funciones.
Este equipo posee un puerto de 16 entradas de alarma para detectores de contacto seco (detectores de movimiento, barreras perimetrales, botones de pánico etc.). La grabación se puede activar por PRE y POST alarma en cualquiera de las modalidades existentes. Además tiene la posibilidad de alarma de detección de movimiento por video. Las búsquedas de grabación se pueden realizar en forma rápida por eventos de alarma, por

hora / fecha y por imágenes, al mostrar pantallas de 8 ó 16 imágenes grabadas. La grabación puede operar hasta 30 imágenes por segundo por multiplexor. Sin embargo, se puede ordenar en cualquier momento modos especiales distintos de grabación tales como grabación de 2, 12, 18, 24, 48, 72, 96, 120, 180, 240, 480, 720, 1.920, 4.320, 8.640 ó 17.280 horas.

La calidad de la imagen depende de la resolución y la compresión. Se puede seleccionar en dos resoluciones: 720x480 y 720x240 campos. Además se permiten diferentes niveles de compresión: Super. no (1/6), . no
(1/10), normal (1/16) y extendido (1/25).

Además de los formatos de visualización convencionales (2x2, 3x3, y 4x4), permite visualizar en pantalla 1, 7, 10 y 13 imágenes simultáneas. Permite el acceso remoto por la red de datos de hasta 16 usuarios simultáneos viendo la misma señal. Este acceso a través de las redes estará protegido mediante contraseña y adicionalmente se pueden definir diferentes niveles de usuarios, lo cual permite definir quién puede modificarla configuración del equipo, quién puede reproducir imágenes grabadas en el disco y quién sólo puede ver el video sin ningún tipo de control sobre las cámaras. El acceso remoto permite visualizar las imágenes actuales de las cámaras o reproducir imágenes grabadas en el disco duro.

### 6.4.4. Monitores

Los monitores permitirán visualizar el video de las imágenes capturadas por las cámaras, en la actualidad en el mercado encuentra software para manejo de cámaras a través de su computador convencional, también encuentra tecnología de monitores en color y blanco y negro, diseñados para manejo exclusivo de circuito cerrado de televisión, monitores en pantalla de cristal líquido, plasma, etc. El número de monitores necesarios, lo dirá la configuración de su sistema de C.C.T.V, en lo posible debe contar con monitor exclusivo para visualizar los eventos de alarma, en sistema multi imagen y sistema secuenciado.

### 6.4.5. Fijación de dispositivos y alarmas

La seguridad física y la seguridad electrónica con sus componentes de CCTV y Control de Acceso, se van integrando; para que todos estos medíos de seguridad den el mayor rendimiento y niveles superiores de seguridad, se requiere que se fijen unos dispositivos físicos, conectados a un sistema de alarmas que permita anticipar hechos delictivos.

En el planeamiento de instalación de los sistemas de alarma se debe tener en cuenta: tipo de protección que se desea, análisis general de las áreas de acceso, zonas de alto riesgo y el área perimetral.

Estos sistemas de detección funcionan como sensores de movimiento, contactos magnéticos y campos sensibles al ruido o la vibración que utilizan microondas, rayos

infrarrojos, campos electrostáticos que darán aviso sobre la presencia de intrusos en la propiedad.

Los accesos peatonales y vehiculares, requieren puertas, tornos peatonales, puertas blindadas, talanqueras, uñas de gato, etc., que estén debidamente conectadas con las lectoras de códigos, lectoras biométricas, lectoras de proximidad, luces estroboscópicas.
El perímetro requiere de muros, mallas, concertinas conectados a sistemas de alarma como: sensores de movimiento, barreras infrarrojas, re. ectores, cable sensorizado subterráneo y/o elevado. Estos crean un campo electromagnético, el cual se activa al pisar sobre el subterráneo. También hay sistemas como el cable sensorizado que se utiliza en mallas y muros y se activa ante el escalamiento, rompimiento, vibración o sonido.

Las bodegas y zonas de almacenamiento, puertas, sensores de movimiento, detectores de humo, excelente iluminación, etc.

Los detectores como los sensores de movimiento, generarán las respectivas alarmas ante cualquier violación o mal uso de equipos y zonas de acuerdo con las políticas adoptadas por la compañía.

**6.4.5.1. Paneles de Control Contra Incendio**
Aunque pueden estar instalados en el centro de control y monitoreo, se recomienda no integrarlas a los sistemas de seguridad electrónica, son dos componentes que actúan independientes y en forma compleja.

**6.5. Control Perimetral**
A lo largo de muros de cerramiento de las instalaciones y sobre la parte superior de este, o en la parte media de la malla que se encuentre superpuesta a este, se puede instalar un sistema de alarmas perimetrales o detección de intrusos mediante la instalación de cable sensorizado. Este cable que de acuerdo a especificaciones del fabricante, puede o no ir protegido por una coraza metálica, van unidos por controladores de dos zonas cada uno.


La medida de cada cable sensorizado depende de la distancia total a cubrir y los recursos disponibles para su implementación debido al número de controladores de zona.

En algunas zonas, el cable tendrá una extensión menor debido a que no necesariamente se encuentra simetría y un largo exacto en el muro de contención.

Este sistema permite la detección de un intruso que corte, escale, mueva o levante la malla y/o la concertina y podrá ser calibrada la sensibilidad del sistema para minimizar falsas alarmas. También se puede instalar barreras de Rayos infrarrojos, que activan una alarma tan pronto como se produzca la interrupción del haz infrarrojo.

Los sistemas de Control Perimetral, se pueden enlazar en el centro de monitoreo con el sistema de control de acceso y con el sistema de CCTV permitiendo monitorear centralizadamente cuando un intruso active una alarma perimetral, la cámara asociada a esa zona será seleccionada automáticamente en el monitor programado, adicionalmente quedará programada una secuencia automática de cámaras y preselección para efectuar el seguimiento de la acción del intruso. Simultáneamente se escuchará una alarma que alertará a los operadores y en la pantalla del servidor aparecerá de manera automática una pantalla que anuncia la alarma, indicando la fecha, hora, evento y zona. Adicionalmente da la posibilidad al operador de escribir un reporte respecto de la actividad desarrollada por el operador para atender la alarma y en el mapa gráfico se indicará el área comprometida en la alarma, siendo posible reconocer la alarma sobre el mismo mapa mediante un clic del mouse.

### 6.6. Sistemas Redundantes o Emergentes

Siempre se debe pensar en sistemas redundantes y/o planes emergentes que respalden la gestión del control de acceso, del circuito cerrado de televisión, del sistema de control perimetral (Iluminación), del sistema de grabación, sistemas de información y comunicación. En general de todos los sistemas para cada contingencia, de tal forma que se pueda garantizar en un alto porcentaje el funcionamiento permanente de los sistemas instalados. En el capítulo de protección de documentos sistematizados, se ampliará la información referente a los planes contingentes.

## 7. Seguridad de Personal

No solamente la integridad física y tranquilidad psicológica de los ejecutivos de la compañía con riesgos externos como el atentado, secuestro, sometimiento, atraco, agresión, extorsión o chantaje deben ser preocupación de la seguridad en la Compañía. Además de éstos estar sintonizados con los esquemas de seguridad (Escoltas, Transportes, Conductores, rutas de movilidad dentro de la ciudad, planes de evacuación o de extracción, coordinación de la seguridad en otras ciudades, aseguramiento de lugares para el traslado parcial o permanente de éstos, etc.), la seguridad debe actuar al interior de la compañía, ya que dependiendo del cargo, posición, área de trabajo y proceso que maneja y funciones del personal dentro de la compañía, estará en mayor o menor riesgo de ser coaccionado o convencido para que colabore en actividades ilícitas, que estén al margen de sus funciones e incluso para participar en actividades como los riesgos sugeridos inicialmente.

De ahí la importancia de hacer el análisis de riesgos por cargos, con el .n de conocer los perfiles de vulnerabilidad del personal.

A continuación se dan algunos parámetros para la seguridad de personal al interior de la compañía desde el mismo momento de la selección, incorporación, el mantenimiento y la

constante evaluación sobre las variables que pueden hacer que un funcionario de una empresa se vea involucrado en conspiraciones internas:

### 7.1. Proceso de Selección

El recurso humano puede llegar a ser el eslabón más débil o más fuerte en la cadena de prevención de riesgos. De los procesos de selección, dependerá en buena parte evitar que el interés primario de éste, no sea trabajar para la empresa, sino, en contra de ésta.

Sí el proceso de selección es lo suficientemente seguro, se debe procurar que los prestadores de servicio (externos) como (escoltas, conductores, operadores portuarios y aeroportuarios, intermediarios, operadores logísticos, etc.), a los contratistas (internos) como (seguridad, servicios de limpieza, recolección de basuras, maquiladores, empacadores, mantenimiento, coteros, etc.) que cumplan con los mismos estándares utilizados por la compañía. Nada se gana con
tener un proceso seguro al interior de la compañía, si los prestadores de servicios, no se acercan o superan los mismos estándares del proceso.

Ya el fólder con un sin número de pergaminos que reflejan idoneidad y recomendaciones personales o laborales, no son prenda de garantía, ni dan la seguridad y certeza que requiere la compañía para incorporar una persona. En la actualidad, se debe investigar a través de los organismos de seguridad del Estado, visitar el sitio de habitación y su entorno familiar, constatar la trayectoria profesional, personal y laboral del aspirante y hacerle seguimiento permanente. Recuerde que hay
tres tipos de aspirantes: (1) Los que colaboran con los delincuentes, (2) los que no colaboran y (3) Los que están dudando; el primero y el tercero, por ningún motivo pueden ser incorporados en la compañía. Un buen proceso de selección y el uso de los filtros adecuados, permitirá detectar estos posibles intentos de infiltración y en la mayoría de los casos, los hace desistir de su intención de incorporarse. En el caso de los segundos, por el contrario, persisten y se acogen a todas y cada una de las actividades y requerimientos que conlleva el proceso de selección que demande la compañía.

Algunos aspectos importantes a tener en cuenta dentro del proceso de selección, el cual debe estar debidamente documentado:

#### 7.1.1. Perfil del Cargo

El responsable de la seguridad de la compañía, está en el deber de acompañar la toma de decisiones relacionadas con el establecimiento de perfiles de cargos en la empresa. Esta labor no debe ser competencia exclusiva del departamento de selección, del jefe inmediato, ni del jefe de personal. Los perfiles del personal, deben resultar y reflejar el análisis de cargos e identificación de posiciones críticas elaboradas por el responsable de la seguridad, buscando disponer de personal no solamente competente sino también confiable.

Actitudes de extrema confianza o la facilidad para concretar relaciones interpersonales, puede ser tan beneficioso, como peligroso. Entonces resulta relevante entender que ciertos puestos de trabajo requieren de este tipo de habilidades, pero tenga en cuenta que otros no. En el caso de puestos de trabajo donde la función es de control y con la

responsabilidad de empacar, almacenar, alistar, entregar carga o documentos, no es recomendable una disposición a hacer amistades con facilidad.

### 7.1.2. Requisición

Es muy importante hacer un buen planeamiento de los reemplazos o apertura de nuevas vacantes, el requerimiento se debe hacer con suficiente anticipación.

Quien hace el requerimiento para cubrir la vacante, debe explicar claramente el cargo y funciones a desempeñar, área de trabajo, procesos que maneja, personas con las que interactúa. El perfil requerido también debe contener aspectos de seguridad acordes con el análisis de riesgos del cargo.

### 7.1.3. Reclutamiento

Dependiendo del perfil y número de personas a incorporar, la oficina de personal hace el llamamiento o solicitud a través de compañías especializadas de caza talentos, oficinas de empleo, avisos de prensa, radio, visita a centros educativos (COLEGIOS, CENTROS TECNOLÓGICOS, UNIVERSIDADES), recomendados por los mismos trabajadores o solicitados a los prestadores de servicio de la compañía, entre otros. Aquí se tiene el primer filtro, donde se pueden descartar, de acuerdo con el perfil requerido, por presentación de la hoja de vida, presentación personal, trayectoria profesional y laboral, lejanía o cercanía con las instalaciones de la compañía, por la información consignada en la hoja de vida, verificación de la información, etc. Cuando el nivel de rotación es alto, se recomienda mantener una base de datos con la información básica, que garantice que un candidato rechazado, no vuelva a pasar por un nuevo proceso de selección de la compañía.

### 7.1.4. Entrevista jefe inmediato

Se maneja este segundo filtro, donde el jefe inmediato dará su percepción y empatía inicial con el aspirante, el concepto general emitido indicará aspectos de presentación personal, dicción, claridad de conceptos, modales empleados,
disposición de horario de trabajo, disponibilidad para iniciar labores, escolaridad, habilidades, conocimiento del trabajo, empleos anteriores, ascensos, motivos de terminación de anteriores empleos, aspiración salarial, aspectos consignados en su formulario de solicitud de empleo etc. El jefe directo debe tener la habilidad para detectar una posible fachada del aspirante.

El concepto emitido por el jefe inmediato, debe terminar en una recomendación que concluye si el aspirante es altamente opcionado para el cargo, si es opcionado con reserva o si por el contrario es rechazado.

### 7.1.5. Documentación y antecedentes

Aquí la compañía hace un tercer filtro y solicita al candidato, que allegue los documentos, registros y certificados legales requeridos por la empresa, los cuales permitirán confrontar la veracidad de la información consignada en su hoja de vida y la transmitida al jefe inmediato. De igual forma, se obtendrán nuevos documentos que permitirán investigar al candidato y solicitar sus antecedentes.

Dentro de la lista solicitada por la empresa, se recomienda incluir copia de la última afiliación al sistema general de seguridad social (ARP, EPS, Pensiones y Cesantías), carta laboral de anteriores empleos, licencia de conducción, tres últimos extractos bancarios.

Debe aprovecharse cualquier sistema que se aproxime a la verdad, olvidando el análisis de personas, los prejuicios y utilizando diferentes métodos para conseguir mayor efectividad y objetividad. En este caso, la compañía le informa y recoge la firma del aspirante en el documento donde acepta voluntariamente someterse antes y durante su vinculación laboral con la compañía, a los exámenes médicos exigidos (general, optometría, audiometría, embarazo, etc.), tests (drogadicción, alcoholemia) y pruebas (polígrafo, grafología, psicológicas, técnicas), entrevista psicológica.

**7.1.6. Preselección**

En el cuarto filtro que es la preselección, se tienen los elementos de juicio suficientes para hacer la visita domiciliaria.

En ésta se amplia y ratifica la información suministrada por el aspirante. Aunque normalmente, ésta visita es practicada por psicólogo o trabajadores sociales y está encaminada a conocer aspectos psicosociales y culturales como el modo y estilo de vida, costumbres, orden, organización, entorno familiar y entorno social, entre otros, se recomienda que el personal que realiza la visita obtenga los registros que indiquen la capacidad de adquisición y nivel de vida tanto del aspirante, como de la familia (fotografías de vías de acceso a la vivienda, fachada de la vivienda, nomenclatura, interior de la vivienda y habitación del aspirante).

**7.1.7. Exámenes y Pruebas**

El aspirante, que ha avanzado hasta este punto dentro del proceso, inicia la presentación de exámenes, tests y pruebas sugeridas en los requisitos indicados en el numeral 7.1.4. De acuerdo con los parámetros y orden establecido por la compañía el aspirante va presentando sus exámenes y pruebas hasta que llega al momento de la selección. Dentro de la pruebas se deben incluir aquellas que reflejen y proyecten los rasgos más importantes de la personalidad.

**7.1.8. Selección**

Ya no es el aspirante, es un candidato a desempeñar el cargo. Este o estos individuos, se han sometido y han superado el proceso. Quien tenga a cargo la decisión, practicará una entrevista final, donde cuestionará la posición de los candidatos frente a aspectos como el robo, tráfico ilícito, terrorismo, piratería, entre otros. Estos aspectos le permitirán al entrevistador determinar el carácter, la motivación, la honestidad de cada uno y escoger el nuevo o nuevos empleados.

**7.1.9. Contratación**

Durante la fase de contratación, se cumplen los aspectos exigidos por la legislación vigente. No olvide antes de formalizar la parte contractual, que se cumpla con todas y cada una de las afiliaciones requeridas por el sistema de seguridad social, incorpore al

contrato de trabajo en las cláusulas adicionales todas aquellas causales de carácter específico que estime convenientes para dar por terminado con justa causa el contrato de trabajo por parte del empleador, entregue una copia del contrato de trabajo al empleado.

**7.1.10. Inducción y entrenamiento en seguridad**

Este es uno de los momentos propicios para hacer el entrenamiento en seguridad, el nuevo empleado tiene grandes expectativas, está ansioso de conocer, está mas dispuesto a recibir información y tiene la motivación suficiente para aprender rápidamente, verifique que el plan de inducción de la compañía, contemple los aspectos de seguridad. Se recomienda que elabore una guía o plan de inducción y capacitación que contenga las políticas y normas generales de seguridad de la compañía, plano de áreas restringidas, tarjetas de identificación, proceso de acceso y tránsito autorizado dentro de las instalaciones, dónde y a quien informar irregularidades, haga un recorrido con el nuevo personal por la planta mostrándole las áreas restringidas, explíquele los motivos de las restricciones. Enséñele a reconocer las señales que indican que sus colegas consumen estupefacientes y/o participan de actividades ilícitas
como el contrabando. Todo el personal que maneja y tramita documentos debe dar a conocer los requisitos de seguridad y las consecuencias de su incumplimiento.

**7.2. Identificación en las áreas de trabajo**

Exija el estricto cumplimiento en el uso y correcta postura de uniformes y escarapelas para identificación en cada área de trabajo; de igual manera, exija el uso de la dotación de seguridad industrial entregada al personal. La indisciplina en el personal es uno de los principales factores de riesgo y genera disminución del compromiso con la empresa.

Utilice colores diferentes de uniformes para cada área criticas de trabajo en su compañía, ejecute las políticas de control de acceso electrónico para cada una de las áreas de trabajo, emita órdenes y tome acciones correctivas inmediatas a través de su personal del circuito cerrado de televisión. Registre permanentemente todas las novedades encontradas y las acciones correctivas tomadas, de tal forma que le permita obtener datos y cifras para encaminar sus esfuerzos a prevenir la siniestralidad.

**7.3. Mantenimiento y conocimiento del personal**

Una charla y revisión periódica sobre aspectos como el comportamiento, cambio de hábitos, las proposiciones que haya recibido de agentes externos, las observaciones que haya hecho sobre otros colegas, su situación social y económica, los compromisos económicos adquiridos, sus nuevos amigos, ayudará para que su empleado se sienta protegido, controlado, tenido en cuenta y a la vez comprometido y responsable con la seguridad de la empresa. Usted demostrará que se preocupa por el empleado, que está pendiente de él, que lo tiene en cuenta y lo más importante, que lo conoce.

Estas actividades se pueden llevar a cabo en la forma propuesta en el punto 7.1.4, con un plan anual de exámenes programados, visitas y reuniones inesperadas a su domicilio, organización de eventos y celebraciones sencillas donde participen sus compañeros, visitas domiciliarias programadas a criterio de la compañía que detecten cambios bruscos en su modo de vida, con un plan de seguimiento selectivo contratado o a través de

personas de confianza pertenecientes a la seguridad o a la red de informantes al interior de la compañía. También puede emplear programas de concientización sobre prevención en el consumo de droga, material de prensa y carteles fijados en cartelera sobre incautaciones y judicialización de personas comprometidas.

### 7.4. Prevención contra conspiraciones internas

Las acciones que realizan un conjunto de personas que trabajan en una empresa, con o sin participación de entes externos y sirven a intereses oscuros y punibles penalmente, se les conoce como "CONSPIRACION INTERNA" y "ASOCIACIÓN o CONCIERTO PARA DELINQUIR".

Recuerde que el recurso humano de su empresa, constantemente está siendo estudiado y analizado por las organizaciones delictivas para explotar sus debilidades y sacar provecho de él.

El principal elemento que las facilita es la OPORTUNIDAD, la cual se presenta en forma subjetiva, que es la probabilidad que tiene el empleado de no ser descubierto y en forma objetiva, que físicamente la falta de control sobre el empleado.

Las personas que laboran, especialmente en áreas con procesos operativos y de responsabilidad en la manipulación y seguridad de la carga, documentos y objetos valiosos, son los más propensos a recibir propuestas por parte de la delincuencia para conformar una asociación delictiva, pues éstos, requieren de conexiones al interior de las compañías que tengan acceso físico a las áreas y conozcan claramente los procesos y procedimientos.

#### 7.4.1. Programas de incentivos

Así como la compañía implementa programas de incentivos para sus mejores trabajadores desde el punto de vista de producción, ventas, calidad, etc., se recomienda también establecer incentivos para aquellos empleados o personas que elaboren y presenten informes sobre actividades relacionadas con aspectos sospechosos o con procesos que presenten vulnerabilidades, de esta forma se crea un ambiente disuasivo que ayudará a impedir y/o neutralizar una acción delictiva y al mejoramiento de los estándares de seguridad.

### 7.5. Análisis de riesgos por cargo

Cuando se elabora el análisis de riesgos por cargo, se debe identificar todas y cada una de las posiciones al interior de la compañía, éstas tendrán su grado de criticidad de acuerdo con la amenaza, riesgo y peligro que represente cada cargo para la empresa. El análisis debe ir ligado a quienes, como personas, ocupan esas posiciones dentro de la empresa, esto quiere decir, que dentro del análisis debe estar presente el perfil de riesgo personal. En cada cargo, se debe observar, entre otros:

Factores laborales que incluya elementos del riesgo tales como: cargo desempeñado, estatus dentro de la compañía, poder de decisión, relación con el poder, notoriedad interna, notoriedad externa, contactos internos, contactos externos, manejo de dinero,

gestión información, actividades externas, manejo conflictos internos, manejo conflictos externos, manejo de agenda, área de trabajo, etc. Factores personales que incluyan elementos de riesgo tales como: bienes que posee, notoriedad económica, notoriedad social, actividad social, diversión y entretenimiento, temeridad, bienes familiares, notoriedad familiar, importancia para la familia, disciplina, vida sentimental. Factores familiares que incluyan factores de riesgo como: área de vivienda, tipo de vivienda, rutas de acceso, conocimiento de vecinos, control de accesos, comunicaciones, vigilancia, iluminación externa, medidas seguridad, observación externa, manejo información, conocimiento de empleados, preparación para emergencias. De ésta forma se puede mantener una alerta sobre los empleados con mayor vulnerabilidad.

# 8. Control y Seguridad de Documentos

Todo documento, escrito o electrónico expedido o elaborado en cualquier área de la compañía debe tener una prioridad (alta,
media, baja, rutina) y un grado de restricción establecida a través de una clasificación (interés general, público, confidencial, reservado), pues es supremamente importante compartimentar la información dentro de cada proceso que desarrolle o adelante la compañía, esto quiere decir, que cada persona tanto al interior (empleados de la compañía y contratistas) y al exterior (prestadores de servicios) deben saber y enterarse de lo estrictamente necesario para el cumplimiento de sus funciones y para la prestación de los servicios. Los empleados de acuerdo con el cargo desempeñado y dentro cada dependencia de la compañía, deben tener claramente establecido el nivel o perfil de acceso a la información, tanto escrita, como electrónica.

## 8.1. Documentos no electrónicos

Un elemento importante en la protección de la información son los elementos no electrónicos que se emplean para transmitirla, fundamentalmente el papel. En las organizaciones se deben controlar los sistemas que permitan exportarla, tanto en formato electrónico, como en no electrónico (impresoras, faxes, teletipos, etc.) Cualquier dispositivo por el que pueda salir información del sistema debe estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos. Cada dependencia debe manejar y ejecutar las políticas de control y archivo de documentos, evitando siempre mantener documentos clasificados a la vista, controlar las copias, disponer de trituradoras de papel para destruir todos los papeles o documentos que no se les quiera dar más uso, evitando que un posible atacante pueda obtener información rebuscando en la basura, se debe, dentro de las posibilidades, impedir que la documentación salga de los edificios para ser revisada o adelantada en las casas de los empleados. Se debe disponer de un lugar adecuado para la ubicación del archivo, que garantice su seguridad física contra sustracción y violaciones y manos criminales, como contra desastres de inundación, incendio, humedad relativa del medio ambiente, etc.

### 8.1.1. Política de Firmas

La política de firmas, generalmente está aplicada a procesos de preparación de documentos, aplicación de sellos, rompimiento de sellos, conteo físico de piezas, revisión de personas, carga equipos, apertura de cajas fuertes, etc.

Se recomienda que los documentos con los cuales se transfiere la responsabilidad sobre la carga o se deja constancia de la prestación de un servicio, debe ser firmado tanto por quien entrega como por quien recibe. Además de la firma, se debe inscribir siempre la fecha y hora con un reloj impresor. Únicamente empleados de nómina de la compañía o que por razón de su cargo y responsabilidad previamente definida, podrán firmar documentos relevantes sobre entrega, recibo o transferencia de responsabilidad de un bien.

### 8.1.2. Plazos para recepción o trámite de documentos

Por experiencia se tiene que la recepción y trámite de documentos de última hora y bajo presión de tiempo, son de gran utilización por organizaciones delictivas para evitar los análisis de riesgos de embarques sospechosos y controles de las autoridades. Se recomienda que se defina una política para recibir con determinada anterioridad los documentos para retiro o ingreso de carga, efectuar un control especial en caso de ser imperativo los embarques de última hora y un proceso para dar cuenta a las autoridades sobre embarques de última hora.

## 8.2. Documentos electrónicos e información sistematizada

Los sistemas informáticos representan una gran ayuda para elevar los estándares de seguridad sobre los procesos administrativos que respaldan las operaciones físicas. Pero si alguien que desee atacar un sistema, tiene el conocimiento y el acceso físico al mismo, todo el resto de medidas de seguridad implantadas se convierten en inútiles. De todos modos, esta premisa válida a la fecha, no puede impedir que se tomen las prevenciones necesarias para proteger la información ubicada en los sistemas. Los delitos informáticos son de dos tipos: Donde el sistema es la víctima real (daños de software y hardware) y donde el sistema sirve como instrumento para llevar a cabo acciones ilícitas. Algunos aspectos importantes a tener en cuenta son:

### 8.2.1. Protección de los datos

Además de proteger el hardware, como se verá adelante, la política de seguridad debe incluir medidas de protección de los datos ya que en realidad la mayoría de ataques tienen como objetivo la obtención de la información y no la destrucción del medio físico que la contiene. En los puntos siguientes se mencionarán los problemas de seguridad que afectan la transmisión y almacenamiento de datos, y se proponen medidas de seguridad para reducir el riesgo.

### 8.2.2. Interceptación

Conocida como ‘’passive wiretapping’’ es un proceso mediante el cual una persona, capta información que no va dirigida a él; esta captación puede realizarse por muchísimos medios: sniffing en redes ethernet o inalámbricas (un dispositivo se pone en modo promiscuo y analiza todo el tráfico que pasa por la red), capturando radiaciones electromagnéticas (muy caro, pero permite detectar teclas pulsadas, contenidos de pantallas, etc.). El problema de este tipo de ataque es que en principio es completamente pasivo y en general difícil de detectar mientras se produce, de forma que una persona, puede capturar información privilegiada y claves que pueden emplear para atacar de modo activo. Para evitar que funcionen los sniffer existen diversas soluciones, aunque al final la única realmente útil es cifrar toda la información que viaja por la red (sea a través

de cables o por el aire). En principio para conseguir esto se deberían emplear versiones seguras de los protocolos de uso común, siempre y cuando se quiera proteger la información. Hoy en día casi todos los protocolos basados en TCP/IP permiten usar una versión cifrada mediante el uso del TLS.

### 8.2.3. Copias de seguridad

Es evidente, que es necesario establecer una política adecuada de copias de seguridad en cualquier organización; al igual que sucede con el resto de equipos y sistemas, los medios donde residen estas copias tendrán que estar protegidos físicamente; de hecho quizás, se deberían emplear medidas más fuertes, ya que en realidad es fácil que en una sola cinta haya copias de la información contenida en varios servidores. Lo primero que se debe pensar es dónde se almacenan los dispositivos, dónde se realizan las copias. Un error muy habitual es almacenarlos en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si se necesita restaurar unos archivos) puede convertirse en un problema serio si se produce cualquier tipo de desastre (como el incendio). Hay que pensar que en general, el hardware se puede volver a comprar, pero una pérdida de información puede ser irremplazable. Así pues, lo más recomendable es guardar las copias en una zona alejada de la sala de operaciones; disponer de varios niveles de copia, una que se almacena en una caja de seguridad en un lugar alejado y que se renueva con una periodicidad alta y otras de uso frecuente, que se almacenan en lugares más próximos (aunque debe ser retirado de la sala donde se encuentran los equipos copiados).

Para protegerla más, se pueden emplear mecanismos de cifrado, de modo que la copia que se guarda, no sirva de nada si no se dispone de la clave para recuperar los datos almacenados.

### 8.2.4. Protección del hardware

El hardware es frecuentemente el medio a través del cual se prepara el elemento más costoso de todo sistema informático, la información, y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización. Los problemas que comúnmente se enfrentan son: acceso físico, desastres naturales y alteraciones del entorno.

#### 8.2.4.1. Acceso físico

Muchas violaciones no tienen un interés manifiesto, ni trascendencia para los sistemas de la compañía, como la denegación de servicio. Si se apaga una máquina que proporciona un servicio es evidente que nadie podrá utilizarlo. Otras violaciones afectan enormemente, si se desea obtener datos, se pueden copiar los ficheros o robar directamente los discos que los contienen. Incluso, dependiendo el grado de vulnerabilidad del sistema
es posible tomar el control total del mismo, reiniciándolo con un disco de recuperación que permita cambiar las claves de los usuarios. Este último tipo de ataque es un ejemplo claro de que la seguridad de todos los equipos es importante, generalmente si se controla el equipo de un usuario autorizado de la red, es mucho más sencillo violar otros equipos de la misma red.

**8.2.4.1.1. Medidas de seguridad**

Para evitar todo este tipo de problemas se deberá implementar mecanismos de prevención (control de acceso a los recursos) y de detección (accesos no autorizados en forma inmediata). En muchos casos es suficiente con controlar el acceso físico a las salas y cerrar siempre con llave los despachos o salas donde hay equipos informáticos y no tener cableadas las tomas de red que estén accesibles.

Se pueden utilizar los medios técnicos de seguridad física existentes en la compañía como son las tarjetas inteligentes, videocámaras, vigilantes, alarmas, etc. y soluciones ofrecidas en el mercado como los sistemas biométricos de analizador de retina, huella dactilar, geometría de mano, entre otros. De igual forma se recomienda que las personas que utilizan los sistemas se conozcan entre si y sepan quien tiene y no tiene acceso a las distintas salas y equipos, de modo que les resulte sencillo detectar a personas desconocidas o a personas conocidas que se encuentran en sitios no adecuados.

**8.2.4.2. Desastres naturales**

Además de los posibles problemas causados por personas, es importante tener en cuenta que también los desastres naturales como terremotos, maremotos y vibraciones, tormentas eléctricas, inundaciones y humedad, incendios y humos. Éstos, pueden tener muy graves consecuencias sobre la documentación e información que se almacenan en los equipos, sobre todo si no se contemplan en la política de seguridad y en su implementación.

Los terremotos y maremotos, son desastres naturales poco considerados dentro de los análisis de riesgos de algunas compañías, ese aspecto se le deja solamente a la compañía de seguros para que los incluya dentro de la prima de la póliza, aunque en la mayoría de las ocasiones queda como una exclusión. Las tormentas, generan subidas súbitas de tensión muy superiores a las que pueda generar un problema en la red eléctrica.

Otro tema importante son las inundaciones no controladas al interior de las oficinas, puesto que cualquier medio (máquinas, cintas, enrutadores, etc.) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido, o bien por los cortos circuitos que se genera en los sistemas electrónicos. En entornos normales es recomendable que haya un cierto grado de humedad, ya que en ambientes extremadamente secos hay mucha electricidad estática. No obstante, tampoco interesa tener un nivel de humedad demasiado elevado, pues puede producirse condensación en los circuitos integrados que den origen a un corto circuito. Por último se menciona el fuego y los humos, que en general provendrán del incendio de equipos por sobrecarga eléctrica.

**8.2.4.2.1. Medidas de seguridad**

La probabilidad debe medirse de acuerdo con la ubicación geográ.ca de las instalaciones, conocer las condiciones climatológicas imperantes y saber si se encuentra en zonas de alto riesgo.

En caso de terremoto, maremoto o temblor, hay varias cosas que se pueden hacer sin un costo elevado y que son útiles para prevenir problemas causados por pequeñas

vibraciones: No situar equipos en sitios altos para evitar caídas, no poner elementos móviles sobre los equipos para evitar que caigan sobre ellos, separar los equipos de las ventanas para evitar que caigan por ellas o que objetos lanzados desde el exterior los dañen, utilizar fijaciones para elementos críticos, colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

En las tormentas, aparte de la protección mediante el uso de pararrayos, la única solución a este tipo de problemas es desconectar los equipos antes de una tormenta (que por fortuna suelen ser fácilmente predecibles).

En el caso de las inundaciones, generalmente no es necesario emplear ningún tipo de aparato para controlar la humedad, pero no está de más disponer de alarmas que avisen cuando haya niveles anómalos y utilizar sistemas de detección que apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados. Hay que indicar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado. En el caso del fuego y humos, se deben emplear sistemas de extinción, que pueden dañar los equipos al apagarlos (actualmente son más o menos inocuos), se evitarán males mayores. Además del fuego, también el humo es perjudicial para los equipos, al ser un abrasivo que ataca a todos los componentes, por lo que es recomendable mantenerlo lo más alejado posible de los equipos.

**8.2.4.3. Alteraciones del entorno**

En el entorno de trabajo hay factores que pueden sufrir variaciones que pueden afectar los sistemas y que se tendrá que conocer e intentar controlar.

Se deberá contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos y/o los cambios bruscos de temperatura.

**8.2.4.3.1. Medidas de seguridad**

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta los equipos; cortos circuitos, picos de tensión, cortes de flujo, etc.

Para corregir los problemas con las subidas de tensión se podrán instalar tomas de tierra o filtros reguladores de tensión. Para los cortes se pueden emplear sistemas de alimentación ininterrumpida que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener por varios minutos los aparatos conectados a ellos, permitiendo que los sistemas se apaguen de forma ordenada (generalmente disponen de algún mecanismo para comunicarse con los servidores y avisarlos de que ha caído la línea o de que se ha restaurado después de una caída). También debemos preocuparnos de la corriente estática, que puede dañar los equipos y para evitar éstos, se pueden emplear aerosoles antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros computadores o por la multitud de aparatos en recintos cerrados, y se transmite a través

del espacio o de líneas eléctricas cercanas a la instalación. Para prevenir los problemas que puede causar el ruido eléctrico lo más económico es intentar no situar el hardware cerca de los elementos que pueden causar el ruido. En caso que fuese necesario hacerlo, siempre se pueden instalar filtros o apantallar las cajas de los equipos.

Las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. En general es recomendable que los equipos operen entre 10 y 32 grados Centígrados, equivalentes a 50 y 90 grados Fahrenheit respectivamente. Para controlar la temperatura se deben emplear aparatos de aire acondicionado que mantengan el medio ambiente de acuerdo con los parámetros señalados.

## 9. Seguridad de la Carga

De los aspectos más sensibles en la seguridad, indiscutiblemente es el tema relacionado con la carga. Para administrar correctamente los riesgos, el responsable de la seguridad, debe tener conocimientos puntuales sobre aspectos relacionados con el Comercio Exterior, Logística durante la Distribución Física Internacional (DFI), Distribución Física Nacional o Interior de Mercancías (DFN). Su labor no llega hasta que la carga sale de la planta, llega hasta que los clientes en destino manifiestan su conformidad al haber recibido completo, en buen estado, a tiempo y en el caso de las exportaciones libre de contaminación.

De un excelente programa de administración de riesgos durante la cadena de distribución física, depende la tranquilidad y confianza que la compañía transmitirá y garantizará a sus clientes, a las autoridades locales, extranjeras y a sus proveedores de servicios. Así mismo tendrá herramientas suficientes para negociar y renegociar las primas de seguros. Recuerde que los seguros son una forma de transferir el riesgo, para mitigar sus efectos. Los seguros, per se, no garantizan que todos los efectos del riesgo estén controlados.

A continuación, se presentan aspectos fundamentales a tener en cuenta dentro de la prevención:

### 9.1. Sistemas, procedimientos durante el almacenamiento

Las zonas de almacenamiento deben ser zonas independientes de otros procesos. De no ser así, se deben construir zonas o áreas de seguridad independientes utilizando cerramientos con muros, mallas, puertas, cadenas, candados, etc. Las zonas de almacenamiento de materias primas, insumos, repuestos, producción, empaque, cargas de alto valor, cargas controladas y cargas peligrosas, deben estar separadas del producto terminado de exportación, del producto terminado de consumo nacional y de zonas de alistamiento de pedidos.

Estos también, deben ser independientes entre si. Cada zona debe estar debidamente demarcada y señalizada. La seguridad electrónica (CCTV, CONTROL DE ACCESO, ALARMAS) además de ser un elemento altamente preventivo y disuasivo, permitirá contar con elementos de juicio y probatorios confiables en el desarrollo de cualquier averiguación.

Cómo se anotó anteriormente, el acceso está restringido única y exclusivamente a quienes cumplen labores específicas de la operación.

Se recomienda eliminar y alejar al máximo posible los casilleros, áreas para cambio de ropas, baños, áreas de descanso, cafeterías y canecas de basura, etc.

Se debe contar en esas zonas con el registro fílmico, fotográfico y documental que permita garantizar la trazabilidad de cada movimiento que se genere al interior de éstas.

**9.1.1. Áreas para almacenamiento de desperdicios, desechos y/o basuras en general.**

Debe existir un adecuado procedimiento sobre el manejo de residuos y basura, permanentemente se deben estar evacuando, evitando acumulaciones considerables e incontrolables en las zonas de almacenamiento de carga.

Las áreas de basura, deben estar ubicadas en zonas de difícil acceso al personal, poco transitadas y en lo posible retiradas de zonas donde se mantengan materias primas y/o productos terminados.

Debe programarse la inspección de estos lugares y los desechos antes de ser recolectados por quienes tienen esta función, ya sea en vehículos o medios especiales utilizados por la compañía. A través de la basura, se producen ilícitos de todo tipo al interior de la compañía.

**9.1.2. Facilidades previas para la transferencia de responsabilidad con la carga**

El proceso operativo es totalmente independiente del proceso de seguridad. Por eso es tan importante que haya una absoluta y total coordinación en las normas de seguridad aplicadas, los procedimientos operativos adoptados y del control de los documentos con los cuales se recibe, se almacena, se alista, se entrega, se embala, se transporta, en general, cuando se transfiere la responsabilidad de la carga de un área a otra área en la misma compañía, de la compañía a otra compañía. Deben estar tan bien de. nidos e identificados, que no generen duda alguna, traumatismos en el desarrollo de las actividades, ni reclamos posteriores.

**9.1.2.1. Procedimientos para envío y recepción de carga**

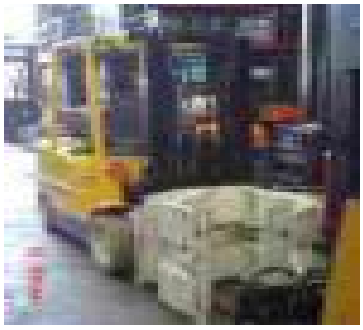
Deben llevarse libros de registro o formatos donde se registre la hora de llegada y salida, las personas que reciben y entregan, la cantidad de carga por tipo de unidad de empaque o embalaje, el estado del empaque o del embalaje, los sellos o precintos de seguridad. En caso que el embalaje presente alguna novedad, se deberá dejar constancia a través de una nota, fotografías y registro de peso en báscula.

**9.1.2.2. Facilidades de ingreso y salida de carga**

Las coordinaciones deben estar acordes con la capacidad de la compañía para almacenar o cargar y la llegada de los transportadores, es decir, haber disposición tanto de espacios físicos, como personal de bodega y zonas de almacenamiento, personal de seguridad y control, operadores de equipo y/o braceros de tal forma que los procesos se surtan de una manera ágil y segura, minimizando el tiempo de espera.

**9.1.2.3. Rutas desde y hacia los puntos de cargue y descargue**

Tanto las rutas internas desde los centros de producción hasta las bodegas o zonas de almacenaje, como las vías de ingreso desde el exterior de la compañía hasta las zonas de cargue y descargue deben mantener lo más despejadas posible, demarcadas y señalizadas correctamente y cubiertas por el sistema de circuito cerrado de televisión.



**9.1.2.4. Verificación de la Carga**

Para hacer esta labor se debe contar con zonas de alistamiento de despachos y plataformas de recepción. Se debe evitar siempre llegar directamente desde la zona de almacenamiento hasta el contenedor o camión, o desde el contenedor o camión hasta el sitio de almacenamiento.

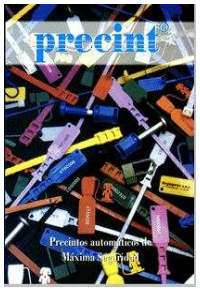

Se recomienda en el caso de carga de exportación que haya una inspección con caninos y revisiones aleatorias de la misma, utilizando inspecciones visuales y/o medios electrónicos como los escáneres, antes de iniciar el cargue en vehículos o en contenedores.

**9.1.2.5. Recibo de contenedores vacíos para cargue en planta**

Dentro de los procedimientos de control de carga, debe efectuarle una inspección rigurosa a todo contenedor y al vehículo que lo porta, antes de iniciar su cargue. Las listas de verificación que estandarizan la actividad son de gran ayuda para evitar novedades posteriores, de igual forma debe implementar listas de chequeo de revisión de los vehículos, para minimizar los riesgos en carretera.

**9.1.2.6. Recibo y entrega de contenedores llenos**

Al momento de ser transportados los contenedores llenos, desde su lugar de almacenaje o desde la fábrica hacia algún destino, deben ser tomados en cuenta los estándares mínimos exigidos. Se recomienda que siempre haya un registro fílmico y/o fotográfico de los sellos y precintos de recepción de estas unidades de carga y con mayor razón, si estos serán violados para cumplir con algún procedimiento o requerimiento de autoridad competente.




**9.1.2.7. Sellos y Precintos**

Una política de sellos y precintos, sobre la documentación, las unidades de embalaje, los vehículos de transporte de carga o áreas que se custodia, determina la responsabilidad de los participantes. Se recomienda que los sellos o precintos estén numerados, controlados uno a uno para evitar que sean usados ilícitamente. Siempre se debe conocer y tener registros documentales firmados, fotográficos y/o fílmicos de quien usó y donde usó el sello o precinto. No se debe hacer entrega de sellos en forma consecutiva y mucho menos hacerlo en esa forma, pues todos los participantes que manejen carga, quedarían notificados de cual será el próximo sello a utilizar y podría prestarse para clonaciones. Se
deben establecer diferentes puntos de chequeo para asegurar que el sello portado, sea el mismo que figura en documentos y que además cumple su función de seguridad. Siempre que haya necesidad de violar un sello, se deben tomar las medidas necesarias para garantizar los registros correspondientes antes de dar la orden de quitarlos. Se debe hacer seguimiento y confrontación a los sellos.

#### 9.1.2.8. Alianzas estratégicas de seguridad

Recuerde que la cadena siempre es tan débil como el eslabón más débil. En la cadena logística del comercio exterior, eso representa que una compañía debe hacer grandes esfuerzos de seguridad, pero si su complementaria o quien subsidia algún servicio no lo es, las oportunidades de que se cometa un acto ilícito con su producto o servicio, está en manos de otro. Para prevenir esto, nada mejor que elaborar acuerdos en materia de controles preventivos a todo lo largo de la cadena logística; estos acuerdos deben contemplar políticas de firmas, sellos, precintos, control de horas, personas responsables, medios de comunicación, transporte, manejo de documentos, inventarios, etc. No olvide hacer partícipe de estas alianzas a las autoridades aduaneras y de antinarcóticos.

### 9.2. Documentación

Para poder manejar adecuadamente los inventarios y ejercer control de pérdidas y daños; además de unas excelentes instalaciones físicas, un adecuado control de acceso y vigilancia, se requiere que haya una adecuada organización durante el almacenaje, claridad en los procedimientos de recepción, alistamiento y despacho de carga. El proceso documental, es sin duda el primer elemento que alertará sobre novedades relacionadas con el recibo o entrega de carga.

Se recomienda restringir al máximo el acceso a la documentación o información, como se vió en el punto 8 SEGURIDAD DE DOCUMENTOS, con procedimientos claros de responsabilidad documental, establecer procesos de cierre y confrontación entre las actividades operacionales y la documentación generada por las mismas, formalizar y protocolizar la entrega y archivo de documentos, contar con áreas seguras para su almacenamiento y archivo.

#### 9.2.1 Documentos de la carga

De acuerdo con las leyes que rijan en cada país, el transporte no es más que el cambio de ubicación de un bien.

Para que se cumpla la actividad de transporte, siempre deben estar presentes tres actores: Un remitente (quien hace el envío), un intermediario (Transportador) y un destinatario (a quien va dirigida la carga) quiere decir, que siempre existirá una remisión y una firma de satisfacción por el hecho cumplido, ya sea durante la entrega o durante le recibo. En este caso todo el personal que tramita los documentos relativos a la carga durante ese transporte, tiene la oportunidad de reconocer las expediciones sospechosas y las inconsistencias, a las que debe negar la recepción o el transporte.

##### 9.2.1.1. Reporte de faltantes, sobrantes o inconsistencias en documentación.

Siempre que se recibe o se entrega carga, por delante va un documento con formalidades plenas. En caso de que ya se encuentre en sus instalaciones documentación sospechosa por que se presentan casos de inexactitud en la información con relación a lo observado físicamente, se deben generar alertas inmediatas que notifiquen a los organismos de

control. Se recomienda un examen cuidadoso de las guías de carga, cartas porte, los contratos de transporte, las facturas, los documentos de aduana y otros. Cada empleado debe llevar la cuenta legible y exacta de la carga que recibe y que tramita. Deben tramitarse solamente los documentos que sean legibles, que tengan las firmas autorizadas, que estén plenamente identificadas esas personas autorizadas y debe estar claramente establecida la forma como se harán los reportes de actividades sospechosas e inconsistencias, sin poner en riesgo la integridad física de los empleados.

## 10. Selección de Clientes y Proveedores

Los conceptos de globalización, virtualización y colaboración aplicados en todo el mundo demandan cambios radicales
en las políticas de seguridad para el aspecto de contratación y negociación con clientes y proveedores. Es importante implementar medidas, mecanismos y procedimientos de prevención, detección y control de actividades ilícitas asociadas con operaciones de comercio exterior, y operaciones cambiarias. Son delitos asociados con el lavado de activos a través del comercio exterior: el contrabando, el favorecimiento de contrabando, defraudación a las rentas de aduana, el testaferrato, fabricación, tráfico y porte de armas y municiones, el tráfico de estupefacientes y otras infracciones como el enriquecimiento ilícito. Existe una clara responsabilidad en todos los actores del comercio exterior que participen de una importación o una exportación, de garantizar la probidad de los prestadores de servicio que contrata y de adoptar las medidas necesarias para evitar tener relaciones comerciales con empresas inmersas en actividades ilicitas.

### 10.1. Aplicación de medidas de seguridad

Se debe adoptar un manual de procedimientos que, además de atender todos los lineamientos mencionados, incluya por lo menos los siguientes aspectos: conocimiento del cliente y del mercado. Se debe conocer a ciencia cierta a quien se le vende y con quien se contrata, ya sean estos habituales u ocasionales, identificarlos y tener conocimiento de sus actividades económicas en aras de establecer la coherencia entre éstas y las operaciones de comercio exterior que realizan.

Lo anterior considerando las características de los diferentes servicios o productos que ofrezcan. Las medidas de seguridad que se apliquen deben garantizar que las negociaciones se hagan con compañías legítimamente constituidas de acuerdo con las normas de cada país, se debe hacer en lo posible la verificación de antecedentes de los accionistas, de sus juntas directivas, de su gerente, de sus representantes legales, cuando se trate de sociedades anónimas, nombre, identificación y dirección de representantes legales, para prevenir, detectar, controlar y reportar operaciones sospechosas que puedan estar vinculadas con actividades ilícitas, nombres y apellidos o razón social del cliente, número del documento de identificación o NIT, domicilio y residencia, actividad económica, capital social registrado, forma de pago de las operaciones de comercio exterior identificando el medio e individualizando el instrumento de pago, entidad financiera emisora o pagadora, ciudad donde está localizada, nombre, identificación y dirección de las personas o empresas beneficiarias de las operaciones de comercio exterior.

### 10.2. Acuerdos

Durante la fase de negociación, deben quedar estipulados y firmados los acuerdos que en materia de seguridad se requieran, siempre se debe procurar en la contratación de servicios que los proveedores pongan en práctica los estándares propios utilizados por la compañía, con el .n de garantizarle a los clientes que el proceso es controlado con los estándares necesarios que aseguran la trazabilidad y control del proceso en forma permanente. Incorpore el lenguaje de la seguridad al interior de sus contratos comerciales con clientes y proveedores.

### 10.3. Calificación de Proveedores

Las personas o empresas que presten servicios inherentes o relacionados con operaciones de comercio exterior se encuentran obligadas a establecer mecanismos de control orientados a conocer las características usuales del mercado propio y el de sus clientes, con el .n de poder compararlos con las operaciones de comercio exterior que, atendiendo el
tipo de servicios que ofrezcan, permita establecer su normalidad o posible anormalidad, o calificación de sospechosa, al compararla con otras operaciones de naturaleza similar efectuadas por clientes que se desempeñan en el mismo ramo de negocio.

Esta evaluación permitirá verificar el cumplimiento de los requisitos de seguridad establecidos a cada uno de los proveedores.

La periodicidad con la cual se realiza la calificación y evaluación de los proveedores debe ser definida previamente por la empresa, al igual que los criterios que utilizará para esta medición. Con base en esta evaluación deberán establecerse acciones correctivas sobre las cuales debe hacerse seguimiento para verificar su cumplimiento.