SOTO & POVEDA ASOCIADOS

INTELIGENCIA Y SEGURIDAD EN EMPRESAS

Cultura de Seguridad

Vicente Soto Pelegrín

Este breve documento va dirigido a personas inexpertas en el campo de la Seguridad o que gestionan departamentos de RRHH, de ventas, o de cualquier otra índole, no relacionada directamente con la Seguridad, con el fin de que adquieran una visión diferente de la Seguridad.

ÍNDICE

INTELIGENCIA Y SEGURIDAD en Empresas[1]

[1] Por extensión entran en la definición de empresas: instituciones, organismos, fundaciones, asociaciones, etc.

1 Cultura de la seguridad

El concepto de **"cultura de seguridad"** nace en los años 80 con el accidente nuclear de Chernóbil, conocido en principio como **"cultura preventiva".** En un principio solo se trataba de prevención de riesgos laborales, pero con el tiempo se extiende a cualquier tipo de actuaciones en Seguridad ante cualquier tipo de riesgos. En este curso nos centraremos en la seguridad a cargo de un Departamento de Seguridad.

Es la cultura preventiva, mejor dicho, las actuaciones preventivas, las que dan sentido a la Seguridad. Las actuaciones se llevan a cabo con normas, protocolos, y la gestión de los medios humanos, físicos y organizativos.

En un país como España, la seguridad no es un elemento que se tenga muy en cuenta en la empresa privada y en algunas instituciones porque se piensa que la seguridad **es un *mal necesario***, porque no se ***ve*** la producción y porque está muy interiorizado el famoso "***a mí eso no me pasa***".

La seguridad siempre es prioritaria, independientemente del tipo de actividad de la empresa, sin embargo en algunos sectores[2] no es que sea prioritaria, es indispensable y eje de la empresa.

Para establecer un Sistema de Seguridad eficaz, tan importante es disponer de medios como la propia actitud pro seguridad de los trabajadores. Los accidentes, las negligencias, la falta de medios, la (falta) de salud, el descontento laboral, la competencia desleal, los delitos patrimoniales etc., merman la seguridad y esto se traduce generalmente en pérdidas económicas, en pérdidas de información o en pérdidas de producción. Las consecuencias afectan generalmente a la empresa pero también afecta a los trabajadores.

El mal endémico es pues, no sólo la falta de nociones en materia de seguridad por parte de los dueños, directivos, responsables de producción, empleados, etc., sino la falta de credo en la Seguridad.

[2] Sectores como el aeronáutico, nuclear, sanitario o alimentario

Ahora bien, ¿qué es la Cultura de Seguridad? Definimos la cultura de la seguridad como el conjunto de valores, actitudes, competencias y comportamientos, tanto del trabajador como de la empresa, desarrollados individual o colectivamente y que van a determinar la gestión de la seguridad diariamente.

En muchas empresas se confunde la seguridad con la prevención de riesgos laborales. Esta situación conduce a que en la elaboración de los planes de autoprotección unicamente los redacta un preventista laboral.

La concienciación de los empresarios y empleados es la mejor manera de llegar a tener un Sistema de Seguridad aceptable. ¿Sólo aceptable? La eficacia de la Seguridad pasa necesariamente por contar con un Departamento de Seguridad con un Director de Seguridad Homologado con titulación.[3]

Entonces ¿Cómo se adopta una Cultura de Seguridad?

– **Concienciar a la dirección o dueño de la empresa:** Que una Empresa, Organismo o Institución comprenda lo necesario que es un Departamento de Seguridad es imprescindible que sus dirigentes crean en la Cultura de Seguridad; que conozcan sus ventajas, que conozcan también los inconvenientes de no invertir en Seguridad. Si los dirigentes no están concienciados, difícilmente se concienciaran los empleados.

– **Concienciación de los trabajadores:** Una vez concienciados los dirigentes es el momento de hacer lo mismo con los empleados. La comunicación de doble sentido, vertical y horizontal, es el pilar básico para un correcto funcionamiento de la Cultura de la Seguridad. La comunicación nos da información, esta información es clave para corregir errores en la producción y para corregir fallos de seguridad.

– **Formación:** Para concienciar a todos los componentes de la Empresa, la mejor manera es dotar a los empleados y directivos de formación en Seguridad. Estos deben ser competentes, sentir que tienen responsabilidades y ser sensibilizados de las consecuencias que tienen sus actividades. En definitiva que interioricen los

[3] Intrusismo

fundamentos de la Seguridad. La formación debe ir de la mano de dotar a los empleados de las herramientas necesarias para realizar su trabajo (Utensilios, protocolos, guías técnicas, material…)

- Implementando un Plan de Seguridad a través del departamento de Seguridad. Ver el último punto.

– Control de las actividades. Es necesario controlar las actividades para comprobar que se realizan correctamente. Esto nos da una visión de la calidad de la implantación de los diferentes planes y protocolos y su seguimiento. Las Auditorías internas realizadas por el Departamento de Seguridad son importantes, pues con ellas detectamos fallos, podemos prevenir mejor.

Premios. Establecer premios para aquellos que, con sus buenas actuaciones, impidan pérdidas de cualquier índole a la empresa, motiva al resto del personal.

La visión que se tenía de la Seguridad hasta hace bien poco era un mal necesario de aspectos retrógrados basada en una operativa tradicional. Su finalidad era tomar mercado. Hoy en día la Seguridad está en posición emergente basada en un sistema integral cuya finalidad es crear mercado. Algunas de sus características y ámbitos de trabajo son la Inteligencia, el Networking, el eCrime, los Planes de Seguridad, los Planes de Contingencia, los manejos de Crisis y situaciones de emergencias…

2 Causas de inseguridad y de los delitos en las empresas

Es la criminología la que se encarga de buscar los factores por los que delinque una persona. Entre las causa de inseguridad encontramos desde, una falta de

planificación en seguridad por parte de la empresa, pasando por un empleado descontento o el crimen profesional. En este epígrafe veremos los factores achacables a la empresa, organismo o institución.

2.1 Causas generales de inseguridad.

Consumo y Tráfico de Estupefacientes: Un gran número de delincuentes son adictos a las drogas y necesitan financiar dicha adicción con los beneficios que le proporcionan sus delitos. Por otro lado, se establece un círculo vicioso: Consumo / Tráfico de drogas, que genera un efecto criminógeno entre consumidores que aspiran a conseguir su dosis y traficantes que tratan de introducir las sustancias estupefacientes a través de redes mafiosas, incluso empresas.

Terrorismo: Los grupos terroristas se han convertido en un mundo globalizado en un fenómeno trasnacional, que genera miedo y angustia a la sociedad. Para financiarse no dudan en extorsionar a empresarios, secuestrar a cambio de rescate o traficar con drogas y armas.

Delincuencia Organizada: La delincuencia organizada, que también podría incluir al terrorismo, hace mención a bandas organizadas profesionales, que se caracterizan por que sus componentes actúan en un grupo jerarquizado, con una importante infraestructura logística y económica, con actuaciones continuadas en el tiempo bien planificadas, con contactos de otras bandas, es decir: Son empresas y actúan como empresas. La diferencia es que, al margen de sus objetivos ilícitos, portan y usan armas de fuego.

2.2 Causas específicas.

Deficiente selección de personal con procesos de reclutamiento obsoletos. Es necesario el uso de herramientas válidas y confiables de selección de personal que midan una serie de variables en la selección de personal. El Dpto. de RRHH está obligado a conocer el grado de honradez, de productividad, de compromiso laboral, del posible consumo de alcohol y drogas Ilícitas, de ludopatías, de posibles enfermedades

del trabajador o de un miembro de su familia, de los posibles antecedentes penales, del grado de madurez, de la situación familiar y de la estabilidad emocional. Pero no basta con esto, lo difícil es hacer el seguimiento al trabajador o directivo que con el paso del tiempo cae en la frustración por no estar motivado o porque sus expectativas no se han desarrollado como pensaba. Esto le puede llevar a cometer una infracción.

Deficientes sistemas de supervisión y control organizativos. La falta de un Departamento de Seguridad con un Director de seguridad al frente hace que haya una vulnerabilidad organizativa espectacular. Son muchos los casos en los que encargan la seguridad a un miembro de la organización (ingenieros, jefes de sección, jefe de compras, jefe de mantenimiento…) con muchas carencias en seguridad. Las empresas piensan que así ahorran costes. No es cierto. Para más señas cometen una infracción a la ley de Seguridad.

Deficiente o nula asignación de responsabilidades. Cuando se detecta un problema es perentorio atajarlo inmediatamente. La inacción puede acarrear pérdidas económicas. La responsabilidad de cada persona que trabaja en la empresa es primordial para detectar posibles pérdidas patrimoniales o de la información. Un ejemplo de ello lo tenemos en el acoso laboral, sea acoso horizontal o vertical, debe cortarse de raíz cuando se detecta. La mayoría de las empresas no lo hacen porque les cuesta terminar con el orden jerárquico implantado. Los resultados pueden ser nefastos: desde el suicidio de la persona acosada, pasando por agredir al acosador o el sabotaje la empresa.

Nulos sistemas de seguridad técnica y administrativa. Aquí hago referencia a la ausencia de sistemas de seguridad técnicos, humanos y organizativos.

Sistemas de seguridad sin evaluar. Los Sistemas de Seguridad Integral de la Organización deben ser auditados de forma periódica, bien con auditorías internas (sin coste adicional) o bien con Auditorías externas realizadas por agencias imparciales (bastante caras). También los planes de autoprotección deben estar sujetos a revisiones cada 3 años y en muchas ocasiones no se cumple. A través del conocimiento del entorno podremos conocer nuestras vulnerabilidades, y de ese modo adelantarnos ante la eventual agresión, asalto, robo, etc.

Software deficiente o nulo. Se estudia en el módulo correspondiente.

Productos de valor mal protegidos. Evidentemente la protección del bien dependerá de su valor. En un hipermercado bastará con añadir una alarma al producto más caro, una botella de whisky, por ejemplo. Pero en una joyería será necesario tener unos bolardos antialunizajes, cristales blindados en escaparates en los que se expongan objetos preciosos, cuyo valor en conjunto sea superior a **90.151,82 euros**.[4] Si no se tiene en cuenta esto, daremos facilidades a los ladrones.

2.3 Formas de comisión de los delitos.

Vamos a exponer algunas de las formas de comisión de delitos

a) Hurtos y Robos

- **Comercios y Grandes Almacenes:**

El carro temático. Se llena el carro hasta los topes de un mismo producto, se escapa con él a la carrera y luego se vende a un intermediario.

Ésta sí, ésta no, ésta sí. Requiere de la complicidad de una cajera. Por cada producto que se pasa por el lector de código de barras se mete otro en las bolsas sin cobrarlo.

Robo por encargo. Ancianos y amas de casa sin fuerzas ni valor para meterse un paquete de arroz en el bolsillo le encargan la lista de la compra a los rateros del barrio, y luego se les pagan por ella la mitad de su valor.

El picnic protesta. Dos docenas de clientes despliegan una mesa y comen de los estantes toda la comida que les apetece.

[4] Fuente: Ministerio del Interior

El truco de la propaganda. Un robo en tres actos: se coge de la entrada el folleto con las ofertas, se mete dentro chopped en lonchas o la bandeja de salchichón y se saca con disimulo.

La mano en la caja. El chorizo llega corriendo, mete la mano en la caja sin reparar en el valor de los billetes y huye.

Con pegatina o sin ella. Lo más fácil es quitar el producto de su envoltorio original o incluso comérselo ahí. Si no, cubrir la pegatina antirrobo con papel de plata.

- **En General**

Resbalón. Consistente en abrir las puertas que no están echadas con llave deslizando una lámina de plástico**,** o una radiografía entre el marco y el resbalón de la cerradura. Es utilizado de forma habitual por cerrajeros cuando no está echada la llave y con práctica puede ser realizada en unos instantes, casi con la misma facilidad de acceso que si tuviéramos la llave. Existen herramientas específicas que aceleran la operación, por lo que es vital para nuestra seguridad cerrar siempre con llave y bajar las persianas para evitar este robo.

Bumping. Esta técnica permite abrir una puerta evitando cualquier signo de apertura de la cerradura, dando la apariencia de que no ha sido forzada si la persona que lo practica tiene práctica. Se lleva a cabo con una llave similar a la que llevamos en nuestros bolsillos, exceptuando que los dientes son más pequeños y de igual tamaño. La llave se introduce en la cerradura y es golpeada repetidas veces, provocando el salto de los pines y la apertura de la misma.

Butrón. Agujero hecho en suelos, techos o paredes con intención de robar. Permite a los delincuentes burlar los sistemas de seguridad que puedan estar instalados en los puntos de acceso de la empresa elegida, a la que acceden desde locales o domicilios anexos que carecen de alarmas

Alunizajes. La técnica habitual consiste en esperar a que el comercio esté cerrado y vacío. En ese momento se utiliza un automóvil, que se lanza directamente contra la

puerta y la luna del comercio. Una vez destrozada la entrada del comercio, los delincuentes roban todo lo que pueden en poco tiempo, tratando de escapar antes de que se presente la policía. Las víctimas más habituales de este tipo de robo suelen ser las joyerías, dado que el delincuente busca poder coger objetos de bastante valor en poco tiempo. Dado que el automóvil suele ser robado, el delincuente comete en ese caso dos delitos: el robo del comercio y el del automóvil.

A mano armada. El robo a mano armada es la forma delictiva más usada para atracar joyerías. El delincuente que atraca joyerías ha evolucionado, ya no es un pequeño ladrón. Ahora son grupos organizados que usan la valencia si les resulta necesario sin ningún miramiento. Usan diferentes métodos para robar en las joyerías, una presa muy fácil y con gran beneficio. No tienen horarios para sus asaltos, pero si éstos deciden actuar mientras el local está abierto, suelen hacerlo a primera hora de la mañana o a última, ya que es el momento en el que tanto la caja fuerte como los expositores con las joyas se encuentran a simple vista y sin apenas seguridad.

Mazas. Muchos ladrones utilizan las mazas para romper el cristal de los escaparates de las joyerías porque es un sistema rápido y muy eficaz. En poco más de un minuto efectúan el robo.

Al descuido. Un grupo de personas entran en el establecimiento y mientras uno distrae a los trabajadores otro aprovecha para robar todo lo posible.

Cogoteros. Los llamados cogoteros son los ladrones que se encargan de vigilar y esperar a los clientes y dueños a la salida del local.

Estranguladores o mataleón. Son ladrones por asalto violento que inmovilizan a sus víctimas por el cuello, cogiéndolas por detrás.[5]

[5] ABC. El Equipo de Investigación del puesto de la Guardia Civil de Illescas (Toledo) ha detenido a los seis integrantes de un grupo criminal al que se acusa, por el momento, de tres violentos asaltos por el método del estrangulamiento a mujeres chinas de Cobo Calleja.
Cinco de los seis encartados por los atracos (tres marroquíes, un argelino y un palestino, además de un cuarto marroquí que ha quedado en libertad con cargos) están ya en prisión. Asimismo, hay otro magrebí y dos españoles imputados por receptación.

Carteristas. Aunque sus objetivos no son las empresas, es posible que entre sus víctimas se encuentre un empresario al que le sustraen documentación, tarjetas de crédito o dinero en efectivo.

b). EL fraude lo define la ACFE[6] como las Actividades o acciones con el propósito de enriquecimiento personal a través del uso inapropiado o la sustracción de recursos o activos de una organización por parte de una persona. Otra definición según The institute of internal auditors: Cualquier acto ilegal caracterizado por el engaño, el ocultamiento o la violación de la confianza.

Los fraudes pueden ser perpetrados tanto por individuos como por organizaciones para: Obtener dinero, propiedades o servicios; para evitar pagos o la pérdida de servicios; o para asegurar una ventaja personal o de negocio. Este tipo de delito es propio del delincuente de cuello blanco.

A continuación se exponen algunos tipos de fraude:

- **Corrupción:** Son aquellas acciones promovidas por los empleados de una empresa u organización (normalmente directivos) para utilizar indebidamente sus influencias o poder afín de obtener un beneficio personal para sí o para un tercero

La investigación Lejano Oriente arrancó a partir del primero caso, el pasado 3 de marzo. La banda utilizaba siempre el mismo «modus operandi»: vivían en Madrid, se desplazaban al polígono de Fuenlabrada, donde es mayoritaria la presencia de empresas asiáticas. Localizaban a una mujer china que saliera de uno de los negocios y subiera en un coche de alta gama. Presuponían que portaban la recaudación del día.

Luego, la seguían, hasta que llegaba a la puerta de su casa, donde, tras aparcar en la calle, las abordaban por la espalda y le apretaban el cuello con el antebrazo, hasta en algún caso hacerle perder la conciencia. Se apoderaban de todo lo que portaba en el bolso de dinero y sus pertenencias, como la documentación y los teléfonos móviles. Estos últimos los vendían luego a los acusados de receptación.

Así actuaron también en la misma urbanización de alto poder adquisitivo conocida como El Señorío de Illescas, el 30 de marzo.

La tercera víctima vive en Paracuellos del Jarama y fue asaltada el 17 de abril. Esta mujer no trabajaba en Cobo Calleja, pero sí fue captada en el polígono. En ese caso, fueron pillados tres de los encartados. Hay detenidos en las zonas de la plaza de Castilla, Méndez Álvaro y Paracuellos. En total, se apoderaron de 8.000 euros en efectivo.

Una de las características de esta banda árabe es la violencia que utilizaban (ver vídeo) y la corpulencia de uno de ellos, que mide 1,98 metros, informaron fuentes de la investigación. Sus iniciales son: S. S., de 37 años; S. B. M., de 31; O. B. L., de 35, y M. L., todos ellos marroquíes. El argelino es J. T., de 37 años, y el palestino es H. K., de 30. Todos tienen antecedentes por causas contra el patrimonio. Se les acusa de pertenencia a grupo criminal y tres delitos de robo con violencia e intimidación.

[6] Asociación de Examinadores de Fraude Certificados

(Ejemplos: Pago de sobornos, extorsión, compra de material a sabiendas que es inservible.)

- **Apropiación indebida de activos**: Son aquellos esquemas de fraude en los cuales la persona que lleva a cabo la acción de fraude realiza sustracciones de activos o utiliza tales activos u otros recursos de la compañía para beneficio propio. (Ejemplos: Desvíos de fondos a través de recibos falsos, robo de bienes y falsificación de cheques de la empresa)

- **Skimming.** (Descremado) Irregularidad anterior al registro contable. También se denomina Skimming al robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta (crédito, débito, etc). Los escenarios comunes en los que se realiza skimming es en restaurantes, bares, gasolineras o en cajeros electrónicos donde un cómplice del criminal está en posesión de la tarjeta de crédito de la víctima o en un lugar en el que se ha instalado un dispositivo que puede copiar la información. En el caso de un cajero automático, el autor del fraude pone un dispositivo, a menudo en combinación con una microcámara, que graba el código PIN (Código de seguridad) del usuario.

- **Fraude por reembolso de gastos**: se produce cuando a un empleado se le paga por gastos ficticios o inflados. Por ejemplo, un empleado presenta un informe de gastos fraudulento y reclama reembolso por viajes personales, alimentos inexistentes, kilometraje extra, etc.

- El **fraude de estados financieros** involucra la inclusión de información falsa como parte de los estados financieros, por lo general sobreestimando los activos o ingresos o subestimando pasivos y gastos. El fraude de estados financieros es generalmente perpetrado por los gerentes de una organización quienes buscan afianzar la imagen económica de la misma. Miembros de la gerencia podrían beneficiarse directamente del fraude al vender acciones, recibir bonos de desempeño, o al utilizar el reporte falso para ocultar otro fraude.

- **Soborno:** es el ofrecimiento, suministro, aceptación o solicitud de cualquier cosa de valor para influir en el resultado. Los sobornos pueden ser ofrecidos a

empleados clave o gerentes tales como agentes de compras quienes cuentan con discreción para adjudicar compras a vendedores. En el caso típico, un agente de compras acepta beneficios para favorecer a un vendedor externo en la compra de bienes o servicios. La otra cara de ofrecer o recibir cualquier cosa de valor que se exige como condición para la adjudicación de negocios es denominada extorsión económica. Otro ejemplo constituye un funcionario de préstamos corrupto quien demanda prebendas a cambio de que se apruebe un préstamo. Quienes pagan los sobornos tienden a ser vendedores que trabajan bajo comisión o intermediarios para vendedores externos.

- **Facturas falsas**.
- **Fraude con cheques.** Fraude por robo o alteración de valores.
- **Nómina.** Irregularidades a través de esquemas en el proceso de nómina.
- **Uso indebido del efectivo de la empresa**.
- **Malversación de activos**: Robo de activos. (Excepto efectivo) Sustracción de activos que no son dinero en efectivo (suministros, inventarios, equipos e información) de la organización. En muchos casos, el perpetrador intenta ocultar el robo incorporando ajustes en los registros.
- **Uso no autorizado o ilegal o el robo de información confidencia**l y de propiedad de la organización para beneficiar equivocadamente a alguien.
- Otros[7]

[7] Estos son algunos ejemplos de fraudes:
1. **Ventas y Servicios no contabilizados** depositándose a cuentas bancarias personales.
2. Ventas y Servicios no declarados en **impuestos**.
3. Créditos recuperados no contabilizados.
4. Pagos autorizados a empresas y bienes no ingresados físicamente, estando únicamente registrados.
5. Pago de **sueldos a personal** que no trabaja.
6. Sueldos pagados a jubilados o personas inexistentes.
7. **Cuentas por Cobrar** en cheques rechazados.
8. Cuentas por cobrar no liquidadas oportunamente
9. Faltantes sin recuperación oportuna, haciendo caso omiso la administración.
10. Ingresos no registrados y pago menor de impuestos.
11. Alteración en **facturas** y registros contables.
12. Anulación de facturas cobradas.
13. Facturas no autorizadas por entes fiscalizadores.
14. Una persona realiza varias funciones de control y registro cobrando cheques a su nombre.
15. **Pasivos** registrados sin documentación soporte.
16. Falta de normas internas que castiguen fraudes.
17. Cheques endosados más de una vez.
18. **Inventarios** registrados sin documentación soporte.
19. Transacciones inusuales a fin de año, ejecutando el gasto y no Recibiendo el bien o servicio.
20. Servicios recibidos en informes y que al ser evaluados no existe el servicio.
21. **Doble facturación**.
22. Doble contabilidad, financiera y fiscal.
23. Pérdida de libro de inventarios para ocultar faltantes de bienes.
24. Clientes y Proveedores sin cumplir requisitos de calidad del bien o servicio y autorizados por la Gerencia para su pago.

Otra clasificación obedecería a la figura que lo comete, entonces tenemos:

Fraudes corporativos. Calificado como el fraude que comete la organización (alta dirección) para ocasionar un perjuicio a los usuarios de los estados financieros, entre ellos, prestamistas, inversionistas, accionistas, el Estado y la Sociedad.

Fraudes laborales. Es el fraude que cometen uno o más empleados para ocasionar un perjuicio a la organización.

Espionaje Industrial. ¿Qué tienen en común el gigante de la industria química Procter and Gamble, Oracle, y el ex cónsul general francés en Houston? La respuesta es que todos ellos han estado involucrados en una de las más grandes industrias contemporáneas: el espionaje corporativo. El espionaje industrial ha acarreado pérdidas de hasta 11.800 millones de euros anuales a la industria alemana, según la consultoría Corporate Trust, con sede en Múnich.

Con frecuencia, los traidores son empleados descontentos con la empresa en la que trabajan y con acceso a información interna sensible que puede ser muy apreciada por la competencia o socios que se largan por sorpresa para montar su propia empresa y que previamente se han llevado toda la información sobre clientes y métodos.

El 90% de los ordenadores conectados a Internet están infectados con spyware. La cantidad de intentos de robo de datos confidenciales ha aumentado en un 50% en un año, y aproximadamente el 45% de las compañías han tenido episodios de acceso no autorizado a datos corporativos por parte de individuos que en razón de su cargo tienen acceso a esta información confidencial.

---

25. Destrucción de documentos legales.
26. Ajustes contables a final de año sin contar con documentación soporte, para ocultar ganancias.
27. Ocultamiento contable en sub cuentas de **gastos ficticios**, pérdidas del ejercicio y ganancias.
29. Transacciones autorizadas por gerencia, sin conocimiento de propietarios.
30. Mermas ficticias en inventarios.
31. Traslado de facturas para ocultar ingresos y evadir impuestos entre empresas relacionadas de socios.
32. Sobrevaloración de servicios y bienes.
33. **Gastos personales** pagados con fondos de la empresa.
34. Contratación de empresas que a su vez sub contratan a otras para prestar el servicio o bien.
35. Bienes trasladados a agencias o unidades internas que se registran dos veces en control de salida y realmente aparece registrado en la unidad únicamente una vez su ingreso.
36. Gastos pagados en teléfono, usándose para otros fines las llamadas.
37. Bienes o servicios pagados, que usualmente no son recibidos.

El problema que tiene los efectos del espionaje es que puede que tarde mucho tiempo antes de darse cuenta que ha sufrido una pérdida de información sensible, ya que no estamos ante material tangible. ¿De qué información sensible pueden apoderarse? De la propiedad intelectual, de avances tecnológicos, de ventajas competitivas, de proyectos para licitaciones públicas, el código fuente de un PC, un software innovador, planes de marketing, secretos corporativos, documentación de investigaciones, es decir, de todo aquello que pueda suponer un beneficio para un tercero.

Pero no sólo queda ahí el espionaje industrial. Es posible que en el transcurso del espionaje obtengan acceso a información privada de cualquiera de los empleados de la empresa, y esto de paso a otro tipo de delito, el chantaje.

La competencia desleal usa personal contratado para realizar este tipo de acciones, sin embargo el principal punto de fuga de la información es el propio empleado. Allen H Beiner, consultor en sabotaje electrónico del FBI, afirma "Podemos colocar cortafuegos en cada una de los ordenadores, pero en realidad todo depende de la persona". Se calcula que en EEUU dos tercios del espionaje se lleva a cabo por los propios empleados. La motivación del empleado espía es de lucro o venganza.

En ocasiones, la tarea de espionaje a una empresa dista mucho de ser sofisticada: basta con buscar en la basura. Son muchos los documentos que van a la basura sin ser previamente destruidos.

¿Cómo nos podemos defender del espionaje industrial y corporativo? A través del empleado capacitado, honesto y eficaz. Éste se puede convertir en la mejor alarma. Para ello hay que mantener al empleado motivado.

Tipos de Espionaje

La infiltración, es la técnica utilizada para introducir unidades propias en las filas del contrario o blanco, para que suministren información de interés inmediato o potencial sobre las actividades, capacidades, planes, proyectos, etc. del contrario. También podría decirse que es la acción que consiste en la utilización de una persona,

denominada topo, cuyo cometido básico es ganarse la confianza de aquellos que poseen la información para tener acceso a la misma.

La Penetración, es la técnica que consiste en lograr la colaboración consciente o inocente de un miembro de la organización o grupo contrario con el fin que proporcione datos e información confidencial del grupo al que pertenece. Generalmente esta actividad se realiza de forma encubierta y emplea personas "reclutadas" que han sido persuadidas de trabajar en secreto en contra de su propia organización por una motivación ideológica, económica, moral, religiosa o personal. A la Penetración, la precede un estudio o selección de personas con acceso a lo que se quiere conocer, sus motivaciones y vulnerabilidades; posterior a lo cual se provoca un acercamiento, a través de terceros, de apariencia casual por parte de un "agente de inteligencia o reclutador" quien inicia un proceso denominado "desarrollo de la fuente", dirigido a cultivar la confianza del futuro informante y prepararlo para la propuesta de colaboración futura.

El soborno es la compra de la información con dinero u otros medios. El soborno es un método muy empleado en la técnica de "Penetración"

Ejemplos de espionaje:

10 grandes casos de espionaje industrial

Caso MacLaren

Coacciones. Las coacciones son el uso de la fuerza o del poder sobre una persona para obligarla a hacer algo que no quiere hacer. Va en dos direcciones. Cuando es el superior jerárquico de la empresa u organización quién la hace, hablamos de acoso laboral, sexual, escolar, moral, psicológico, etc. Si la coacción va del empleado o de un tercero hacia el presidente, directivo, o superior, y no es personal, estamos ante un caso de coacciones por interés patrimonial principalmente, aunque no se puede descartar el interés sexual.

Chantaje. Es una variedad de la coacción en las que el sujeto amenaza al chantajeado con publicar un secreto del sujeto para obtener información de la empresa. Generalmente se obtiene previamente información privada del dueño de la empresa, de un directivo o de un operario que no quieren que se haga pública porque afectaría a su vida particular. Normalmente se pide dinero a cambio de no revelar el secreto. La víctima una vez que paga la primera vez, el criminal volverá a pedirle dinero o documentos de la empresa, y así en espiral hasta que el chantajeado va a la policía o se suicida, en casos extremos.

Amenazas Bomba. Las amenazas de bomba se realizan normalmente para conseguir objetivos políticos por parte de los terroristas. En el caso de las bombas colocadas en empresas privadas, los terroristas buscan un beneficio económico ante aquellos empresarios que no se amedrentan ante ellos. Las pérdidas pueden ser dejar de ingresar en caja las ventas del día por un desalojo de un hipermercado en hora de máxima afluencia. O puede haber una pérdida de patrimonio físico si la bomba es real y explosiona.

Secuestro. Es el acto a través del cual un individuo o grupo privan de manera ilegal a otro u otros de su libertad, generalmente, durante un tiempo determinado y hasta lograr la obtención del rescate, que puede consistir en dinero o algún beneficio político, tecnológico o mediático. El modus operandi que tradicionalmente se sigue en un secuestro implica el seguimiento de la víctima durante varios días previos a la concreción del golpe, qué hace, a donde va, con quien se reúne, entre otras cuestiones y de esta manera tener una acabada idea de cuál sería el momento más adecuado para secuestrarlo, generalmente, en aquellas situaciones en las que la víctima va sola. Son un blanco fácil los empresarios que viajan al extranjero para expandir el negocio e invertir en otro país.

Sabotaje. Si alguien quiere dañar la imagen de una empresa o dañar sus beneficios, el sabotaje es uno de los delitos más socorridos en los últimos años. Consiste en sabotear los productos que oferta la compañía a fin de ocasionar una

pérdida de imagen y consiguiente pérdida de mercado. Un ejemplo de ello lo tenemos cuando se lanza un rumor sobre la nocividad de determinado producto.

Riesgos Sociales. Huelgas. Vandalismo. Las pérdidas para las compañías por este tipo de riesgos es enorme. En el caso de las huelgas (legales o ilegales) las horas de trabajo perdidas por huelgas en España ascendieron a 6.633.454 en los cinco primeros meses del año, como consecuencia de las 459 huelgas contabilizadas, en las que participaron 210.729 trabajadores, según los datos de conflictividad laboral, analizados por los servicios técnicos de CEOE. En cuanto al vandalismo, las puertas selladas con silicona, las pintadas en las paredes y persianas, la rotura de ventanas, camiones de empresa quemados, etc. ocasiona en las compañías un gasto adicional que en las que muy pocas veces se atrapa al culpable y se hace pagar por ello.

Riesgo de Incendio. El control de los incendios comienza en las fases de diseño de la empresa, local y/o almacenes; así, si la instalación es de tipo industrial tendrá que cumplir con los requisitos marcados en el RD 2267/2004, si la instalación es de otro tipo se adaptará a lo marcado por el RD 314/2006, donde se incluye el Documento Básico de Seguridad en Caso de Incendio. Sus causas más corrientes. La principal causa de incendios fortuitos en la industria está en fallos eléctricos.

Según un estudio realizado en Gran Bretaña sobre individuos procesados por delitos de esta naturaleza reveló que: un 17% padecían trastornos mentales; un 19% se habían visto impulsados por sentimientos de venganza, frustración e ira; un 17% habían bebido mucho antes del incendio o eran alcohólicos y un 17% no mostraban más motivo que un irracional vandalismo destructivo. Un 9% estaría realizado con fines lucrativos: cobrar el seguro o similar.

En otros estudios se estima que el incendio fraudulento representa un 20% del total de incendios provocados en el Reino Unido y en algunos otros países europeos se percibe con una proporción incluso mayor.

Riesgos Naturales. Es la probabilidad de que un territorio y la sociedad que habita en él, se vean afectados por episodios naturales de extremos. Es necesario distinguir entre:

- **riesgos actuales**: un volcán en erupción, un deslizamiento activo, un acuífero contaminado que se está explotando. Los Riesgos actuales suelen ir acompañados de daños, aunque no hayan desarrollado todo su potencial
- **riesgos potenciales**: son un volcán transitoriamente inactivo o una ladera en equilibrio estricto.

2.4 Responsables

En una encuesta realizada en el año 2011 a los empresarios españoles por los responsables de los delitos económicos sufridos, el 82,5% señaló que se habían dado dentro de su empresa, es decir, **por el personal propio.** Más concretamente, el 61% señalaba a la alta dirección y el 39% a los mandos intermedios. El perfil que daba este estudio sobre el autor del delito era el siguiente: hombre, maduro, con trayectoria en la empresa y bien posicionado, lo que permitía que el montante del fraude fuera mayor.

En España, el 50 % de la pérdida desconocida corresponde a hurtos de clientes, el 27 % a hurtos de empleados, el 5 % a proveedores que "sisan" y el 18 % a errores administrativos.

El estudio reveló que los pequeños negocios son más vulnerables porque no tienen los recursos o los procedimientos apropiados para detectar o evitar el robo.

En 2008 desaparecieron de los comercios españoles artículos por valor de 1.200 millones de euros (1% de su facturación), según los datos de la patronal Aecoc.

Clientes/ usuarios/ Proveedores. España ocupa la segunda posición entre países europeos y la quinta mundial en robo a minoristas. Por delante, México, China, Estados Unidos y Finlandia.

Esto se traduce en unas pérdidas de unos 2.574 millones de euros, el 1,36% de las ventas. Pero el coste de estos robos y hurtos también lo soporta el cliente honesto, puesto que se traduce en un encarecimiento de los productos para compensar estos delitos. Se calcula que supone unos 259 euros anuales a cada hogar español. Entre los productos más codiciados por los *ladrones* encontramos complementos de moda, joyas, herramientas eléctricas, pilas, accesorios para móviles, *smartphones*, vinos y licores, cárnicos frescos, productos de maquillaje y cremas faciales. El nexo común a todos es la facilidad para ocultarlos entre las ropas y su posible reventa.

http://www.elperiodicoextremadura.com/noticias/extremadura/comercio-pierde-30-millones-euros-robos-clientes-empleados_80742.html

Empleados[8]**.** Los empleados de las empresas manejan dinero, mercancías, suministros, información y todo ello es susceptible de robo. Dependiendo de la posición en el organigrama de la empresa, el acceso a estos bienes será más o menos fácil. Un reponedor en un supermercado puede llevarse un Cd de música; un policía, la prueba de un delito; un directivo, información privilegiada; o un albañil, herramientas.

Algunos empleados roban dinero físicamente sacándolo de la caja fuerte (en algunos sitios es el cajón del director o empresario) o sacando dinero de una caja registradora. Otros son facilitadores del delito.

Otra forma de robo de dinero se produce cuando los empleados cobran a un cliente y luego se quedan con la diferencia o devuelven el cambio incorrecto y se quedan con la diferencia. Los empleados de contabilidad o algún gestor pueden modificar las nóminas, los pagos, los vencimientos y desviar dinero a sus cuentas bancarias. Hablamos en este caso de malversación de fondos.

Al igual que el robo de nómina en la que alguien crea empleados fantasma y recoge cheques de pago para estos empleados inexistentes. Esto generalmente ocurre solamente en las grandes organizaciones, donde hay numerosos empleados eventuales o que trabajan a tiempo parcial. El empleado que participa en este tipo de robo es

[8] *Según el Departamento de Justicia de EEUU , cerca de un tercio de los empleados roban a su empresa.*

generalmente un miembro del departamento de contabilidad o algún gerente que se encarga de la contratación ya que tiene que crear un empleado falso y cobrar el sueldo de esa persona.

Otra forma de robo que puede realizar el empleado es el robo del tiempo. La forma más extendida es que otro trabajador fiche por el infractor, el cual no ha ido a trabajar. O que el propio infractor fiche y se marche. Esto está muy extendido en la Administración pública.

Robo de suministros. A priori el hurto por un empleado de un paquete de bolígrafos no supone un descalabro para la empresa. Pero si son varios los empleados quienes realizan este acto (papel, cartuchos de tinta o grapadoras) y además prolongado en el tiempo, el resultado cambia. De estos pequeños robos con impunidad pasamos a un objetivo más suculento: los portátiles y ordenadores, tabletas, y otros componentes electrónicos.

Directivos. Según la Asociación de Examinadores de Fraude Certificados, la ACFE en sus siglas inglesas estiman de media, unos 578.000 euros que son escamoteados por los directivos de las empresas.[9] El dueño defrauda a su compañía porque en ocasiones la tiene con un socio al que escamotea dinero o bien porque se hace con sumas de la compañía como si fueran propias y no de la sociedad.[10] Los mandos intermedios sustraen unos 220.000 euros. Y a medida que se tienen más estudios, se roba más. Y en tiempos de crisis se detectan más casos.

Según un responsable de la firma i2 Integrity (consultoría de negocios) "Los defraudadores tratan de mantener un nivel de vida que ya no pueden permitirse", "En los casos en los que hemos trabajado así lo hemos visto. Y casos de directivos que cobran unos sueldos indecentes, que tratan de aparentar un estatus que no se corresponde ya con su nivel". Los robos de los directivos se explican ahora con la crisis porque han perdido pluses. Pero antes de la crisis, ¿por qué un directivo bien posicionado hurtaba a su compañía? La ambición es la única respuesta, o no. Es

[9] http://www.conclusion.com.ar/2015/07/citaron-directivos-del-banco-municipal-por-repetidos-robos/
[10] Caso Urdangarín

necesario mirar cada caso y preguntarse, si tiene algún familiar de primer grado con alguna enfermedad cuya curación es inasumible en términos monetarios; o le están chantajeando y extorsionando; o tiene alguna alteración del lóbulo frontal; o como apuntamos al principio, tiene una ambición sin límites.

Los delitos económicos a los que recurren suelen ser apropiación indebida, como realizar cargos a la tarjeta de empresa, la manipulación contable (alterar las cuentas para que aparenten lo que no son, disimulen inversiones fallidas o gastos excesivos) o cobrar a los proveedores por adjudicarles contratos de la compañía. El pago de bonificaciones a los directivos por alcanzar los objetivos puede suponer una motivación para delinquir.

Un profesor de Psicología criminal de la Universidad de Alicante, entró a una clase de Criminología y dijo tras las buenas tardes: "el 70% de vosotros sois delincuentes". Tras el asombro inicial aclaró la rotunda afirmación. Hablaba de la población media que se ha llevado algo alguna vez de un hipermercado, de su empresa. Se refería a la sustracción de algún Cd debajo de la ropa, o de alguna grapadora o cosas menores; naturalmente en alguna etapa pasada de la vida, normalmente en la adolescencia temprana y tardía. Esto no quiere decir que todos seamos delincuentes, sino que podríamos llegar a serlo con la motivación adecuada.

El fraude se comete tanto en pequeñas como en grandes empresas pero con una diferencia: En las pymes los fraudes son más frecuentes porque su gestión se basa en la confianza, aunque de menor cuantía. En las grandes hay menos fraudes porque hay mayor control, en estos casos es mayor el importe defraudado.

Este tipo de conductas generan muchas pérdidas en las compañías. Algunas asumen el coste del pequeño hurto, no así el coste del fraude que se puede disparar pudiendo suponer la quiebra de la Empresa.

Pero no sólo estos dos delitos producen pérdidas, las conductas anti productivas también, y es posible que ocasionen mayores pérdidas. Situaciones de preferencias dirigidas en la rotación laboral en los cuadrantes, los accidentes laborales, el absentismo o el sabotaje llevan a una situación de falta de productividad.

Actualmente se estima que de promedio, las empresas pierden aproximadamente el 3% de las ventas totales netas, producto de la merma desconocida, del hurto de empleados, del hurto de clientes y de errores administrativos[11].

Error de Gestión. El error de gestión no es un hecho que venga producido por un acto delictivo, a priori.

Criminalidad profesional. La **delincuencia organizada** es la actividad delictiva de un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves para obtener, directa o indirectamente, un beneficio económico, político u otro beneficio de orden material. Tiene las siguientes características: Las actividades que desarrollan no están concentradas en un solo objetivo, sino que sus actividades atienden a todos los campos en los que es posible obtener una rentabilidad adecuada, que no tiene por qué ser económica. Su ámbito de actuación es trasnacional. En tercer lugar, usan una extrema violencia ejercida en cualquiera de sus formas.

Schneider apunta diez criterios característicos de la criminalidad organizada:

1) Satisface necesidades de una parte de la población en cuanto a bienes y servicios ilegales que son prohibidos por las leyes.

2) Escoge sus actividades ilegales pretendiendo minimizar el riesgo adecuando sus esfuerzos y gastos a tal fin.

3) La criminalidad organizada es nuclear respecto a otras formas de criminalidad.

4) El grupo delictivo se forma con el fin de producir, distribuir y ofrecer servicios y mercancías ilegales.

5) En su actuación domina la planificación estratégica y táctica, racionalidad y distribución de roles.

6) Seguimiento de normas subculturales, convenios tácitos de absoluta lealtad al grupo y anonimato social.

7) Uso de la violencia como último recurso con el fin de mantener la cohesión del grupo.

[11] Las empresas incluyen en errores administrativos las conductas anti productivas.

8) Se mantienen estrechas relaciones entre actividad legal e ilegal aprovechando la zona gris de la economía.

9) Utilización de protectores, consejeros y patrocinadores de la policía, justicia y economía necesarios para el desempeño de sus actividades criminales.

10) Operatividad a nivel internacional con una gran movilidad haciendo uso de los medios de comunicación y transporte, la tecnología y la más moderna infraestructura económica y social.

Se puede observar que el funcionamiento es similar al de una empresa convencional.

Consecuencias de las pérdidas patrimoniales y de la información en la empresa

- Daños a los valores tangibles de la empresa
- Manipulación maliciosa de los productos
- Daños a la propiedad industrial
- Daños a los archivos, informes y documentación
- Daños a las personas.- Ejecutivos, personal laboral
- Daños a la imagen de la empresa
- Posible quiebra

3 Departamento de Seguridad

Necesidad del Departamento de Seguridad

La creación del Departamento de Seguridad está contemplada en el Reglamento de Seguridad Privada, aprobado por el Real Decreto 2364/1994, de 9 de diciembre como una medida de seguridad de carácter organizativo, para la protección de las personas del patrimonio de la empresa o institución, y ha de ser de carácter obligatoria o voluntaria, según las circunstancias.

Distinguimos pues tres formas de creación:

a) Obligatorios por disposición expresa: cuando concurran las circunstancias recogidas en la letra b) del apartado segundo del artículo 96 del Reglamento de Seguridad Privada: centros, establecimientos e inmuebles que cuenten con un servicio de seguridad integrado por veinticuatro o más vigilantes, y cuya duración prevista supere un año; o a los que hace referencia el apartado primero del artículo 119 de dicho Reglamento: Bancos, Cajas de Ahorro y demás Entidades de Crédito.

b) Obligatorios por orden gubernativa (artículo 112 del Reglamento): Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean, o cualquier otra causa lo hiciesen necesario, el Secretario de Estado de Seguridad para supuestos supraprovinciales, o los Delegados y Subdelegados del Gobierno, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, una serie de servicios o sistemas de seguridad, entre los que se encuentra la creación del Departamento de Seguridad.

Cuando lo disponga la Dirección General de la Policía y de la Guardia Civil para supuestos supranacionales, o el Subdelegado de Gobierno para la provincia, atendiendo al volumen de medios personales y materiales, al sistema de seguridad de la entidad o

establecimiento, así como a la complejidad de su funcionamiento y el grado de concentración de riesgo.

c) Voluntarios (artículo 115 del Reglamento): hace referencia a las entidades, públicas o privadas, que, sin estar obligadas a la creación del Departamento, pueden crearlo de forma voluntaria, con todos o alguno de los cometidos establecidos en el artículo 116, poniendo al frente del mismo a un Director de Seguridad habilitado.

Al frente del mismo habrá siempre un Director de Seguridad, con las funciones contempladas en los artículos 95, 97 y 98 del Reglamento de Seguridad Privada. En este sentido, el artículo 18.3 de la Orden INT/318/2011, dispone que deberán desempeñar sus funciones "integrados en su **departamento de seguridad**".

El artículo 95.2 del vigente Reglamento de Seguridad Privada, sólo exige que el Director de Seguridad sea "designado" por la entidad, empresa o grupo empresarial. Según la Secretaria General Técnica del Ministerio del Interior, en informe del 12 de febrero de 2009, concluyó que resultaba admisible la posibilidad de externalización de la figura del Director de Seguridad, así como del departamento, al entender que la norma no exigía, necesariamente, una vinculación contractual directa entre el **Director y la entidad**, sino que tal vinculo podía ser sometido a negociación contractual, pacto o acuerdo entre las partes. Siguiendo otras opiniones, el director de seguridad que esté al frente de un Departamento de Seguridad, **deberá formar parte de la plantilla de la empresa**. Es decir, no se podría realizar esa labor de dirección del Departamento de Seguridad de manera externa, mediante contrato mercantil, como una prestación de servicio. No podría hacerlo ni un director de seguridad como trabajador autónomo, ni tampoco una empresa de Seguridad Privada, que cediera a alguno de sus directores de seguridad para hacerlo. Sin embargo, la Secretaría General Técnica del Ministerio del Interior, ya en informe del 12 de febrero de 2009, concluyó que resultaba admisible la **posibilidad de externalización** de la figura del Director de Seguridad.

En un informe de la Secretaría Técnica 2015/021 se concluye lo siguiente:

De todo ello se desprende que el Departamento de Seguridad, ya sea obligatorio o facultativo, con su Director de Seguridad al frente, desarrollará sus cometidos para la entidad, empresa o grupo empresarial para el que fue creado y se encuentra incardinado.

El Director de Seguridad habrá de estar integrado en la plantilla de las empresas de seguridad y en aquellas obligadas a disponer de esta figura según determine la normativa de desarrollo de la vigente Ley de Seguridad Privada.

En cuanto al asesoramiento en materia de actividades de seguridad privada, se encuadran dentro de las actividades que pueden ser prestadas, o no, por empresas de seguridad, y será el titular de la entidad, empresa o grupo empresarial quién designe al responsable de la gestión de las actuaciones encaminadas a la prevención y control de riesgos.

En relación con la viabilidad legal de las posibles formulas planteadas en las consideraciones de este informe, únicamente reiterar lo en ellas manifestado.

Estas actuaciones, es decir, la elaboración y desarrollo de los planes de riesgo, estarían encuadradas en las funciones que el artículo 36 de la Ley les atribuye a los Directores de Seguridad, por lo tanto, nada impide que los realicen para terceros, ya que la normativa no obliga a que sean realizados por empresas de seguridad, al ser actividades compatibles que quedan fuera de su ámbito de aplicación.

Problema práctico: en los casos en los que el Director de Seguridad no pertenece a la entidad, éste tiene menos posibilidades de ejercer sus funciones con eficacia debido a que precisamente no va a tener independencia funcional. Tendría una relación contractual, sometido a las órdenes del cliente.

Lo que se deja claro es que la carencia de Departamento de Seguridad cuando su existencia obedece al cumplimiento de una medida de seguridad obligatoria, así como la carencia de los mismos en los establecimientos obligados, pudiera dar lugar a una

infracción muy grave o grave, según los casos, de las tipificadas en el artículo 155 del mencionado Reglamento.

Creación

Lógicamente, el presupuesto es el primer escollo con el que nos encontramos con lo cual, es posible que el Departamento tenga que ser proporcionado al coste de creación, al menos para ponerlo en marcha. Otros aspectos a tener presente son las dimensiones de la Organización, la actividad que desarrolla y los peligros o riesgos potenciales.

De este Departamento nace a continuación el Plan de Seguridad.

Los Departamentos de Seguridad deben convivir por necesidad y sentido común con otros Departamentos como pueden ser los de Mantenimiento o Infraestructuras (dependiendo del volumen de la Empresa u Organismo) o los de Prevención de Riesgos Laborales o con la Entrada de Mercancías, etc. Pero en modo alguno debe estar subordinado a ellos. En las Empresas donde se ha decidido que la Seguridad está subordinada a otros departamentos, ésta, simplemente no funciona. El Departamento de Seguridad debe ser independiente funcionalmente y tener dependencia orgánica con la gerencia o con el Director General. Con esto se evitará la lentitud que supone la gestión de pasos intermedios, sin claridad, sin toma de decisiones, y sobre todo la sensación de vacío y responsabilidad, lográndose por el contrario la aceptación de la normativa general en materia de seguridad y garantizando así el respaldo por parte de la dirección en todo lo referente y que afecte a la seguridad de la propia empresa. También debe contar con una relación fluida con el Departamento de Recursos Humanos.

Relaciones con otros departamentos[12]

- **Con RRHH.** Es indudable que se necesita una estrecha colaboración con este dpto., ya que es el que contrata al personal y el que conoce los problemas que pueda tener el empleado. Cualquier anomalía debe ser comunicada al Dpto. de Seguridad.
- **Con Dpto. Jurídico.** A través de este dpto. se inician acciones legales contra aquellos sujetos que atentan contra los interese de la Organización. El Director de Seguridad trabajará en estrecho contacto con sus componentes y consultará que las medidas de seguridad a adoptar cumplan con la Leyes y la LOPD
- **Con Dpto. de Compras y Recepción.** El material que entra y sale de la Organización o empresa, lo hace a través de recepción. Cuando se trate de material sensible se habrá de comunicar afín de tomar medidas adicionales si cupiese.
- **Con Dpto. de Mantenimiento.** Los operarios de este departamento pueden detectar de primera mano los posibles actos de sabotaje, lo que deberán comunicar inmediatamente al director de seguridad.
- **Con Dpto. de Riesgos Laborales.** En España existe la creencia y la equivocación de que este departamento se debe encargar de las medidas de emergencia y protección. Nada más lejos de la realidad. Los delitos, sabotajes, vandalismos, robos, etc. son competencia del departamento de Seguridad. Este departamento está para asuntos de salud de los trabajadores.

Un Departamento de Seguridad se crea para obtener una Seguridad Integral de las instalaciones, sin embargo, éste fin queda condicionado por el presupuesto y por la capacidad para establecer y aplicar el Plan de Seguridad. Hay que tener en cuenta que la Seguridad no se puede garantizar al 100% aunque contemos con un presupuesto extraordinario, no obstante a mayor inversión en seguridad mayores resultados. Pero la inversión se debe realizar después de realizar un estudio de seguridad con su correspondiente análisis de riesgos; con esto tenemos visibles las vulnerabilidades y amenazas potenciales.

[12] Sólo en grandes corporaciones encontramos una estructura presente con todos los departamentos. Lo normal en Pymes es encontrar los departamentos aunados, o no existir.

¿Por qué un estudio de Seguridad? Para evitar gastar más de lo necesario y contar con un recurso de mayor coste que aquello que se quiere proteger. Por ejemplo, poner 250 cámaras para proteger una universidad y dejar el 50% de la superficie ciega sin tener siquiera en cuenta las zonas más sensibles o conflictivas es poco o nada profesional.

Uno de los hándicaps que encontramos a la hora de establecer un Plan de Seguridad son los propios dueños de las Empresas o los directores Generales porque piensan que pierden el "control" del Ente. No es así. Lo que se gana es un mayor potencial en prevención y aseguramiento del lugar usando un CCTV, controles de accesos y con un responsable de Seguridad que marca las pautas, órdenes de puesto y protocolos a seguir.

Relaciones con organismos externos

La relación del Dpto. de Seguridad y por extensión de todos sus componentes con los servicios de emergencia debe ser correcta y fluida. En el punto que en ocasiones dependemos de ellos, debemos tenerles informados de las características de la empresa. Por ejemplo con el plan de autoprotección actualizado para los bomberos en la entrada de la Empresa.

- Policía
- Bomberos
- Protección Civil
- Ambulancias

El Plan Integral de Colaboración del CNP con el Sector de la Seguridad Privada se llama "Proyecto RED AZUL". Se asienta en la colaboración CNP/SP, trascendiendo el modelo actual de exigencia legal para llegar a un modelo de colaboración profesional de complementariedad y corresponsabilidad, en una puesta en común de recursos entre la Seguridad Privada y el CNP.

Ventajas de contar con un Dpto. de Seguridad con un Director de Seguridad al frente

- Reducción de pérdidas y retorno de la inversión al contratar director de seguridad
- Eficacia
- Reducción costes
- La contratación de un director de seguridad ajeno a la empresa de seguridad subcontratada supone un mejor control y fiscalización de los gastos y de la operatividad. Control de los presupuestos destinados a seguridad.

5 Detección y Análisis de riesgos. Amenazas. Vulnerabilidades. Riesgos

En el análisis de riesgos o diagnosis de seguridad se trata de detectar los niveles de riesgo de un centro, analizando las amenazas potenciales. Se elabora un informe donde se plasma los niveles de riesgo que puede ser, alto, medio o bajo. Con el análisis de riesgos conocemos las medidas de seguridad correctas a implantar; creamos los planes de contingencias en previsión de las amenazas detectadas; y además podemos implantar un SGSI.

5.1 Componentes del Riesgo

El **riesgo** se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

RIESGO = AMENAZA x VULNERABILIDAD

Amenaza: es un evento o incidencia que puede ocasionar daños en las personas o en las organizaciones o en la propiedad.[13] La amenaza corresponde a un fenómeno de origen natural, socio-natural, tecnológico o antrópico en general, definido por su naturaleza, ubicación, frecuencia, probabilidad de ocurrencia, magnitud e intensidad (capacidad destructora). La amenaza se determina en función de la intensidad y la frecuencia.

- Degradación: Nivel o grado de perjuicio del activo.
- Frecuencia: Cada cuánto tiempo se materializa la amenaza

[13] la pérdida de medios y de servicios, trastornos sociales y económicos, o daños ambientales

Valor 1/4	degradación	frecuencia
1	Escasa	Anual
2	Normal	Mensual
3	Frecuente	Semanal
4	Asiduamente	A diario

AMENAZAS	accidentales	intencionadas	Personal propio	Personal externo
humanas	0/1	0/1	0/1	0/1
naturales				
Robo		0/1	0/1	0/1
Sabotaje		0/1	0/1	0/1
Vandalismo		0/1	0/1	0/1
Incendio	0/1	0/1	0/1	0/1
Agresión				

Vulnerabilidad: es una debilidad en un sistema que permite a un atacante violar la integridad de una empresa, organización o comunidad y que los hacen susceptibles a los efectos dañinos de una amenaza.

Los factores que componen la vulnerabilidad son la exposición, susceptibilidad y resiliencia.

VULNERABILIDAD = EXPOSICIÓN x SUSCEPTIBILIDAD / RESILIENCIA

Exposición: es la condición de desventaja debido a la ubicación, posición o localización de un sujeto, objeto o sistema expuesto al riesgo.

Susceptibilidad: es el grado de fragilidad interna de un sujeto, objeto o sistema para enfrentar una amenaza y recibir un posible impacto debido a la ocurrencia de un evento adverso.

Resiliencia: es la capacidad de un sistema, comunidad o sociedad expuestos a una amenaza para resistir, absorber, adaptarse y recuperarse de sus efectos de manera oportuna y eficaz, lo que incluye la preservación y la restauración de sus estructuras y funciones básicas.

Impacto: Consecuencia de la materialización de una amenaza sobre un activo

5.2 El riesgo

Una correcta identificación del riesgo pasa por un detallado conocimiento de la empresa, del entorno físico, legal, social, político, cultural y económico. Esta gestión del riesgo sirve para minimizar las pérdidas y proporcionar una seguridad e integridad del Ente razonable. Para calcular el riesgo hay que tener en cuenta una serie de factores que detallo a continuación:

- Ubicación física de la empresa.
- Posicionamiento en el mercado, competencia.
- Estadísticas criminales de la zona.
- Datos accidentes en la zona, vecinos. (Bomberos y protección civil)
- Datos del INE.
- Datos del INS (instituto sismología)
- Datos AEM (Agencia meteorología)
- Catálogos generales de amenazas (Proveído por aseguradoras)

A1) Activos o inventario

- (Recursos necesarios para que la organización funcione correctamente)
- Información o datos
- Servicios prestados (internos y externos)
- Aplicaciones y equipos informáticos (hardware y software)
- Redes de comunicaciones (telefonía, internet, etc.)
- Instalaciones y equipamiento.
- Personal

A2) Valor de los activos

Los activos son todos aquellos elementos que forman parte del Sistema de Información. El valor de los activos de la empresa, vienen caracterizados por los siguientes elementos:

Disponibilidad.- Alude a la reserva de tiempo de la que podemos disponer del recurso. Por ejemplo, en menos de una hora, menos de un día, menos de una semana, más de una semana. A la hora de calcular el impacto de una amenaza, debemos tener presente tanto las vulnerabilidades como las soluciones inmediatas que disponemos. Si tenemos una solución de alta disponibilidad, ante una amenaza alta el riesgo sería medio. Esta lectura la haremos a la inversa. Si tenemos una solución de baja o nula disponibilidad, una amenaza baja la trataremos como alta.

Integridad.- La integridad de los activos es la capacidad de un activo para cumplir su función de manera eficaz y eficiente, protegiendo al mismo tiempo la vida de las personas de la empresa y los bienes protegidos. Las acciones de gestión relacionadas sirven para garantizar que durante todo el ciclo de vida del activo existan en la empresa las personas, sistemas, procesos y recursos necesarios y adecuados para su correcto funcionamiento. Se clasifica en bajo, normal, alto, crítico.

Confidencialidad.- Esto hace referencia al nivel de privacidad del activo, es decir: libre, restringida, protegida, confidencial…

B) Gestión de riesgos

Se debe determinar si el riesgo es aceptable para identificar y aceptar el riesgo residual o decidir sobre la forma de gestionar el riesgo

Forma de gestionar el riesgo:

- Evitarlo: suprimir las causas del riesgo: Activo, Amenaza, Vulnerabilidad
- Transferido: cambiar un riesgo por otro: Outsourcing, seguros, etc.
- Reducirlo: reducir la amenaza, vulnerabilidad, impacto
- Asumirlo: Detectar y recuperar (Statu quo).

5.2 Análisis del riesgo. Método Mosler.

Cuando un experto en seguridad es consultado acerca de sistemas de prevención de riesgos y protección de personas y bienes, debe trabajar metódicamente a fin de llegar a una evaluación correcta. Entre otros, se emplea el Método Mosler, que se aplica al análisis y clasificación de los riesgos y tiene como objetivo identificar, analizar y evaluar los factores que puedan influir en su manifestación, entonces podrá hacer una evaluación ajustada de los mismos

Consta de cuatro fases concatenadas:

Fase 1: DEFINICIÓN DEL RIESGO

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

Fase 2: ANÁLISIS DE RIESGO

Se utilizan para este análisis una serie de coeficientes (criterios):

✓ Criterio de Función (F)

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

- Muy gravemente (5)
- Gravemente (4)
- Medianamente (3)
- Levemente (2)
- Muy levemente (1)

✓ Criterio de Sustitución (S)

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

- Muy difícilmente (5)
- Difícilmente (4)
- Sin muchas dificultades (3)
- Fácilmente (2)
- Muy fácilmente (1)

✓ Criterio de Profundidad o Perturbación (P)

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

- Perturbaciones muy graves (5)
- Graves perturbaciones (4)
- Perturbaciones limitadas (3)
- Perturbaciones leves (2)
- Perturbaciones muy leves (1)

✓ Criterio de extensión (E)

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

- De carácter internacional (5)
- De carácter nacional (4)
- De carácter regional (3)
- De carácter local (2)
- De carácter individual (1)

✓ Criterio de agresión (A)

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

- Muy alta (5)
- Alta (4)
- Normal (3)

- Baja (2)
- Muy baja (1

✓ Criterio de vulnerabilidad (V)

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

- Muy alta (5)
- Alta (4)
- Normal (3)
- Baja (2)
- Muy baja (1)

Fase 3: EVALUACIÓN DEL RIESGO

En función del análisis (fase 2) los resultados se calculan según las siguientes fórmulas:

Cálculo del carácter del riesgo "C":

Se parte de los datos obtenidos, aplicando:

I. Importancia del suceso

I= F x S daño que pueda alterar la actividad x facilidad para reponer los bienes

D. Daños ocasionados

D= P x E afectación a imagen de la firma x alcance daños geográficos

C= I + D Carácter Riesgo= Importancia suceso + daños ocasionados

Cálculo de la Probabilidad "PR":

Se parte de los datos obtenidos en la 2ª fase, aplicando:

A. Criterio de agresión

V. Criterio de vulnerabilidad

Probabilidad PR= A x V probabilidad de que el riesgo se manifieste x daño efectivo

Cuantificación del riesgo considerado "ER":

Se obtendrá multiplicando los valores de "C" y "PR".

ER = C x PR Riesgo considerado =Carácter riesgo x cálculo de probabilidad

Fase 4: CÁLCULO Y CLASIFICACIÓN DEL RIESGO

Calculo de Base de Riesgo:

Entre 2 y 250 Bajo.

251 y 500 Pequeño.

501 y 750 Normal.

751 y 1000 Grande.

Ejemplo para una empresa:

Riesgos causados por delitos

TIPO DE RIESGO	ANÁLISIS RIESGO						EVALUACIÓN RIESGO					RIESGO
	F	S	P	E	A	V	I	D	C	PR	ER	
							FxS	PxE	I+D	AxV	CxPR	
Robo/hurto	4	3	3	3	5	5	12	9	21	25	525	**Medio**
Atraco	3	4	3	3	4	4	12	9	21	16	336	**Medio**
Fraude/Estafa	3	4	3	3	3	5	12	9	21	15	315	**Medio**
Atentado/Agresión	3	2	3	3	2	3	6	9	15	6	90	**Bajo**
Vandalismo	4	2	3	3	2	3	8	9	17	6	102	**Bajo**
Secuestro	4	3	4	4	1	3	12	16	28	3	84	**Bajo**
Amenaza de bomba	2	2	2	2	1	4	4	4	8	4	32	**Bajo**
Sabotaje	3	2	3	2	2	3	6	6	12	6	72	**Bajo**
Disturbios	2	1	2	2	2	3	2	4	6	6	36	**Bajo**
Espionaje industrial	2	2	3	4	2	3	4	12	16	6	96	**Bajo**
Chantaje/Extorsión	3	3	3	3	2	3	9	9	18	6	108	**Bajo**
Manipulación Datos	4	3	4	3	3	4	12	12	24	12	288	**Medio**
Robo Datos	4	2	3	3	3	4	8	9	17	12	204	**Medio**

Una vez conozcamos a través del análisis de riesgos, las vulnerabilidades, las amenazas y los activos, podremos crear un plan de contingencia o un plan director de Seguridad, establecer responsabilidades y medidas a adoptar.

5 Medios de protección

La protección: Es el conjunto de sistemas que garantizan la integridad de una instalación frente a las agresiones internas o externas, sean éstas de carácter fortuito o intencionado".

Los tipos de protección se pueden dividir en:

- Protección Física o pasiva
- Protección Electrónica o activa

O cuando se refiera a protección de personas:

- *Protección Estática*
- *Protección Dinámica*

Las medidas de protección constan de:

a) Medios técnicos: Pasivos y Activos.
b) Medios humanos
c) Medios Organizativos

a) *Medios técnicos.* Son los distintos equipos usados por la Organización para protegerla. A su vez, se dividen en: (CNI)

- *Medios Técnicos Pasivos*: Puertas, barreras, alambradas, esclusas, cristales blindados,
- *Medios Técnicos Activos*: Alarmas, CCTV, detectores...

Medios Pasivos. Son elementos diseñados para impedir o retardar la materialización exitosa de una amenaza y por tanto la primera línea de seguridad. Pueden tratarse de barreras externas (muros, vallas) o internas (paredes, techos de una habitación, una caja fuerte).

- **Barreras perimetrales**

Muros[14]. De infinidad de materiales, desde pladur hasta hormigón armado, pasando por acero. Pueden estar diseñados para impedir el paso de personas, para protección contra explosiones (no producen metralla), para emanaciones de señales electromagnéticas, etc.

Otro tipo de barreras son las vallas, cercados, verjas, espino, concertinas. Éstas últimas, provistas de cuchillas que debido a la torsión del alambre salen disparas en cualquier dirección en caso de cortarlas (muy útiles para curar cualquier mal a base de sangrías típicas de la edad media). Este tipo de barreras son **menos robustas**, por lo general, que los muros pero más económicas, rápidas y fáciles de instalar, suelen verse en instalaciones militares. Pueden estar electrificadas y protegidas contra sabotaje e intrusión mediante sensores.

Los muros y vallas pueden estar terminadas en su parte superior por bayonetas de espino, concertina, etc. en diversas formas, (en oblicuo simple –hacía el exterior de la amenaza es más complejo de sortear-, doble -en V-, etc.).

- **Barreras Periféricas**

Puertas, las hay de todo tipo (manuales, automáticas, basculantes, enrollables, giratorias, correderas, extensibles, etc.).

Puede ser de acceso “directo” o con protecciones contra vehículos cargados de explosivos. En este caso, se instalan obstáculos accionables de forma automática, remota o manual, que impiden o dificultan el paso de un posible vehículo proyectado contra las instalaciones a proteger.

[14] El muro de Cisjordania que erige Israel a lo largo del territorio de Cisjordania, llega a levantarse hasta 7 metros de altura y tiene planificado alcanzar una longitud de más de 700 km y los hay subterráneos para impedir la construcción de túneles (bypassing the wall :P), llegando a una profundidad de 20 a 30 metros como es el caso del Muro de Egipto.

Las puertas pueden ser comunes, de seguridad, blindadas o acorazadas. Pueden ser tipo esclusa (unidireccional, bidireccional, lineales, angulares, etc.). Pueden ir "aderezadas" con detectores de metales, muy usadas en sucursales bancarias.

Ventanas, mostradores, respiraderos, claraboyas, etc. pueden estar protegidos con rejas, cristales blindados (diseñados para diferentes amenazas, -armas ligeras, pesadas, vandalismo, etc.

- **Protección del bien**

Cajas fuertes y cámaras acorazadas. Los tipos varían en función del tamaño, método de apertura, fortaleza, etc. Como ejemplo de cámara acorazada, la del Banco de España, construida a base de hormigón armado y cemento fundido, se encuentra sita a 35 metros de profundidad y cuenta con una superficie de 2500 m2 (algo más que los "minipisos" de Trujillo), además cuenta con un foso y su puente levadizo.

Como curiosidad indicar que por encima se canalizan aguas subterráneas que en caso de robo inundarían la cámara y ésta quedaría sellada. Por último decir, que no todo el oro de la reserva se encuentra en el propio banco, puesto que una importante parte en Fort Knox, el Banco de Inglaterra y Banco Internacional de Pagos de Basilea.

Medios Activos. Los elementos activos se encargan de monitorizar y/o alertar de una posible intrusión o sabotaje. Éstos se pueden clasificar como sigue:

1. Detección de intrusos en el interior y en el exterior.
2. Control de accesos personas/objetos.
3. CCTV.
4. Avisos.

- Detección de intrusos en el interior y en el exterior. **Sensores.**

Los hay de todos los colores y sabores. Se pueden dividir en cuatro categorías en función de la cobertura de detección.

a. *Puntual*. Sensor magnético. Se colocan en puertas, ventanas o similar.

b. *Lineal*. Láser, infrarrojo. Ideales para zonas angostas.

c. *Superficie*. Presión. Se instalan en suelos, vitrinas con objetos valiosos, etc.

d. *Volumen*. Microondas, infrarrojos, etc. Cubren amplios espacios, habitaciones, salas, etc.

A continuación se muestra un ejemplo de la tecnología utilizada.

• **Magnéticos**. Sensores muy simples. Dos puntos están en contacto, pasa corriente eléctrica. Cuando se produce una intrusión (abertura de una ventana, por ejemplo), se produce una diferencia de potencial que activa la alarma. Son sencillos de sabotear.

• **Láser**. Se suelen colocar en zonas de detección muy determinada, como pueden ser ventanas, puertas, cajas fuertes, pasillos, etc. A mayor número de sensores mayor cobertura de detección. Es común ocultar este tipo de sensores porque su inhabilitación es relativamente sencilla. Son utilizados tanto en interior como en exterior. Requieren de visibilidad entre el transmisor y receptor y por tanto no puede haber obstáculos entre ellos. Le afecta las condiciones climáticas que puedan dificultar la visión entre el transmisor y receptor, como hemos comentado anteriormente.

• **Inducción**. Este tipo de sensores mide la alteración de un campo de inducción (o magnético). Detectan el paso de un objeto metálico. El tamaño de dicho objeto irá en función de la calibración del sensor. Estos pueden presentarse en forma de arco de detección, como el que hay en los aeropuertos o pueden instalarse en el suelo, de tal forma que al pasar un vehículo o persona puedan detectar su presencia. Se han utilizado a modo de radar y cuenta la leyenda que los israelíes tiene todo el perímetro de sus fronteras (al menos las más "calientes") rodeado por este tipo de sensores. De tal forma que cualquier persona con un mínimo objeto metálico es detectado de inmediato (mínimo = clavos de los zapatos). Este tipo de sensores, muy a groso modo son dos cables que crean un campo magnético entre ellos. Como se puede observar no sirve ante objetos no metálicos. No les afecta la climatología (exceptuando tormentas eléctricas).

• **Microondas**. Basados en el efecto doppler. Suelen cubrir un entorno en forma de óvalo. Se suelen instalar en el interior de zonas cerradas. Sensores muy efectivos

pero que se han de calibrar correctamente porque puede llegar a traspasar paredes o muros y provocar falsos positivos al detectar "intrusiones" en zonas aledañas. En el exterior les puede afectar la climatología (niebla densa, lluvia intensa, etc.).

- **Infrarrojos**. Miden la radiación electromagnética infrarroja que irradian los cuerpos. Son sensores que se adaptan mejor en estructuras internas porque les afecta, como es lógico las condiciones climáticas. Cuidado al orientar este tipo de sensores hacia ventanas, puesto que la exposición directa del sol puede provocar falsos positivos.
- **Ultrasonidos**. También basados en efecto doppler. Capaz de atravesar obstáculos físicos. Les afecta en menor medida los elementos climáticos (comprobar) y pueden cubrir grandes distancias.
- **Vibración**. Todos conocemos su utilización a la hora de medir terremotos. También son muy utilizados en cajas fuertes, detectan movimiento (perforación, taladro,…) sobre una superficie.
- **Otros**. Temperatura, posición, presión, lumínicos, acústicos y un gran etc.

Un error habitual en los dispositivos sensores es no eliminar u ocultar el típico LED que se enciende cuando se activa. Por ejemplo, el volumétrico qué cuando una persona pasa por delante se activa (detecta a la persona) y podríamos conocer su alcance porque se ilumina el LED. Esta es una información que debería ocultarse. Hay circunstancias que pueden no haberse tenido en cuenta a la hora de instalar y "configurar" los sensores. Un ejemplo, volumétrico (infrarrojos) apuntando a una ventana puede verse afectado por la exposición directa del sol, o en puestas, etc. Por último, nos podemos encontrar sensores de doble tecnología (microondas+infrarojos, por ejemplo), que sólo en caso de que ambas tecnologías detecten, envían la señal de alarma. De esta forma se minimiza la posibilidad de falsos positivos.

- **Sistemas Control de Acceso**.

Son sistemas que en función de un criterio definido permiten o impiden el acceso a determinado lugar. Tornos (manuales o automáticos), esclusas, barreras, puertas, lectores de proximidad, biométricos, electromagnéticos, etc.

- **CCTV.**

Muy asociado a la defensa perimetral. Las cámaras pueden ser de color (mayor realismo) o en blanco y negro (mayor definición), alta definición. Las hay adecuadas a la luz diurna, luz artificial, nocturnas, etc. Incluso con la luz de las estrellas pueden obtener imágenes de calidad (made in Israel). Las hay motorizadas o estáticas (las primeras tienen la ventaja de cubrir más amplitud pero a su vez es una desventaja).

Pueden detectar movimiento, mediante el software adecuado, de la imagen y alertar al operador o disparar alguna acción. Como cualquier sensor se ha dimensionar correctamente para no obtener falsos positivos.

Un fallo muy común son los ángulos muertos, zonas que las cámaras no cubren. Esto ocurre cuando dos cámaras puestas en un mismo punto apuntan a dos direcciones diferentes. Lo ideal, es que una cámara cubra el perímetro y a la vez a la siguiente cámara (en fila) de esta forma, podremos eliminar los puntos muertos así como cualquier manipulación directa sobre la cámara. Por supuesto, normalmente detrás de una cámara deberá haber un operador, si no, como que el sistema no funciona igual (excepto las cámaras con sensor de movimiento). Es interesante ocultar las cámaras por cubiertas opacas, con objeto de no revelar información sobre qué puntos "vigilan" dichas cámaras.

- **Avisos.**

Es importante poseer un sistema de avisos ante intrusiones o anomalías, para poder dar aviso (en caso necesario) a la amenaza o para coordinar la seguridad de las instalaciones. Para ello existen sistemas de megafonía para dar avisos y/o instrucciones a “gran” escala, interfono, para comunicaciones puntuales y precisas. Otros sistemas acústicos son sirenas, bocinas, silbatos (muy utilizados en la mar). También se pueden contar con señales lumínicas, iconos, pictogramas, etc.

b) *Medios humanos*. Compuesto por el personal de seguridad de una organización como los vigilantes de seguridad y los directores de seguridad. Aquí es importante

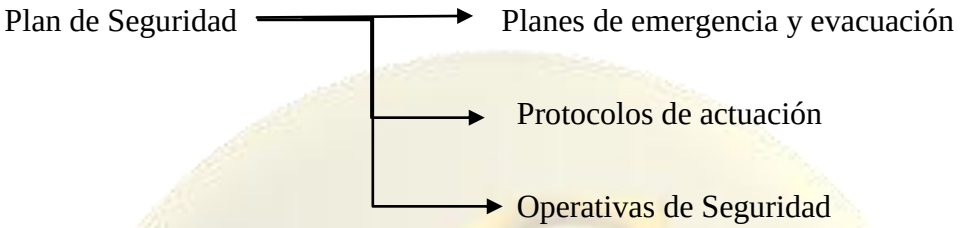
añadir que el gerente o dueño, forma parte de esta cadena como responsable de los bienes a proteger. También es necesario considerar a cualquiera que esté en contacto con los bienes a proteger.[15]

c) *Medios organizativos*. Estos medios están constituidos por los planes directores de seguridad, los planes de contingencias los protocolos, los planes de autoprotección y emergencia y, atención, por las instrucciones específicas recibidas para un periodo concreto, sea de una hora o de un mes. La finalidad de estos documentos es hacer frente a las hipotéticas situaciones de vulneración de la seguridad que se puedan dar. En estos planes quedará perfectamente asignado la función de cada uno de los integrantes de un Sistema de Seguridad Integral (SIP)

[15] Un técnico de laboratorio que tenga bajo su cargo isotopos radioactivos, por ejemplo

6 Estudio e Informe de Seguridad

En primer lugar se debe establecer la situación actual de la empresa en relación a los riesgos. A continuación hay que identificar y evaluar las posibles amenazas, ya visto en el epígrafe 6.5. Con este análisis de riesgos trataremos de eliminar o reducir los efectos que pueda desencadenar esas amenazas potenciales. Por supuesto, el Plan resultante debe ser objeto de control y supervisión y mantenerlo actualizado.[16]



El Plan Director de Seguridad es el documento principal sobre el que deben sustentarse el resto de documentos que utilice el Departamento de Seguridad. Su extensión debe ser lo suficientemente amplia para profundizar en todos aquellos aspectos que pudiesen ser relevantes para el organismo, y deben tenerse presentes los siguientes aspectos y por este orden:

a) Fase de toma de datos. Tarea de campo que si bien en principio pueda resultar la parte más tediosa, es la fundamental para una correcta elaboración de un Plan de Seguridad sin fisuras. Para la toma de datos es necesario contar con el libre acceso a toda la información relativa a la actividad de la empresa, ya que si un aspecto no es incluido, es susceptible de provocar un fallo en los procedimientos a implantar.

b) Identificación de riesgos potenciales. Con toda la información, ya se está en disposición de identificar los riesgos potenciales, los cuales habrán de jerarquizarse en orden de importancia para priorizar y/o aplicar las medidas de forma proporcionada.

c) Identificación de vulnerabilidades. Una vez identificados los riesgos, y con la información obtenida en la fase de toma de datos, se está en disposición de identificar los puntos vulnerables de la organización.

[16] Hay empresas que no revisan nunca su plan de Autoprotección o sus Protocolos de Seguridad

d) Acciones a emprender para eliminar o atenuar vulnerabilidades. Lo que se culmina con la elaboración de un Plan de Seguridad, o con la mejora del existente.

El Plan de Seguridad no deben conocerlo en su totalidad los empleados de la Empresa, Organización o Ente. Ni siquiera todos los componentes del Departamento de Seguridad deben ser conocedores del Plan de Seguridad General en su totalidad; basta con que conozcan la parte del mismo que le pudiese afectar en sus labores cotidianas.

De esta manera se evitan filtraciones accidentales o interesadas. Al administrativo del Departamento de Seguridad no le aporta nada el ser conocedor de la operativa nocturna. Evidentemente si el Departamento de Seguridad lo constituye un reducido número de personas esta consideración no tiene sentido.

Una de los documentos que más se elaboran son los protocolos. Cuanto más protocolos menos relevancia del Plan de Seguridad; es decir la redacción abusiva de protocolos viene dada por las lagunas del Plan Director de Seguridad.

Está demostrado que un protocolo excesivamente extenso no resulta útil en la práctica; a menos que su sola misión sea la de depurar responsabilidades, pero de ser así, el planteamiento inicial estaría desvirtuado, donde la confianza en todos sus componentes es cuestión de vital importancia para el buen funcionamiento del equipo de Seguridad.

Este tipo de documentos, está especialmente indicado para el personal subcontratado que trabaja para el Departamento, y si bien, la parte fundamental es el relativo a las Instrucciones de Puesto específicas, se pueden complementar con otros documentos dependiendo del puesto concreto, como puedan ser:

- Listados de entradas y salidas de personal autorizado
- Listado de entradas y salidas de proveedores y visitas
- Listado de control de llaves
- Informes de amenaza telefónica de artefacto explosivo
- Informes vehículos sospechosos

- Informes descripción de sospechosos
- Listados de accesos a salas restringidas
- Informes de averías (cualquier caso de avería debe quedar documentada)
- Informes del dinero físico en caja (Confidencial)
- Informes del material a proteger (joyas, bonos, material laboratorio tóxico…)

7 Prevención

Las conclusiones del estudio de Seguridad nos aportarán las soluciones a desarrollar, las cuales irán en función del tipo de riesgo a combatir.

7.1 Robos realizados por empleados

a) Selección de personal

Si la amenaza es interna, se está implementando en los países anglosajones la *Honesty Profile o el* ***perfil de honradez*** *del empleado.* Es un examen que se aplica vía electrónica previa contratación del trabajador, con independencia del puesto a desarrollar,[17] y que nos permitirá conocer cómo piensa el candidato, cuáles son sus valores y principios, cuáles fueron los motivos por los que actuó de una manera determinada en el pasado, y conocer si es una persona de riesgo para la organización.

Esta prueba mide tres parámetros:

1. Confiabilidad
2. Integridad
3. Compromiso Organizacional

Según datos internacionales, el 90% de los trabajadores ha estado involucrado en conductas deshonestas, por ejemplo, en una empresa normal, el 25% de los empleados roba habitualmente, otro 25% no robará bajo ningún concepto y el 50% restante robará si tiene la oportunidad de hacerlo. (Bryan Hylans, ex inspector general del Ministerio de Trabajo de EE.UU.).

En la selección de personal se debe filtrar en la medida de lo posible la elección de aquellos trabajadores que tengan un perfil cercano a la conducta lesiva e irresponsable.

[17] No podemos olvidar los delitos de cuello blanco.

En trabajos en los que hay una clara oportunidad de apropiación (material o intangible) será conveniente subir un poco el nivel de las pruebas. Por ejemplo en empleados de caja, oficinistas, mandos intermedios, etc.; pero este nivel exigido varía en función del tipo de empresa u organización. Si planteamos la seguridad de una central nuclear, un edificio de laboratorios con productos tóxicos o sensibles, una farmacéutica, o cualquier tipo de infraestructura crítica, las pruebas de selección de personal deben endurecerse.

Pida referencias profesionales y académicas

Pida teléfonos de contacto de los encargados o supervisores de anteriores empleos. Direcciones y teléfonos de los centros de enseñanza a los que asistió, indicando cuál fue la graduación exacta.

Certificado de penales: Es un certificado de antecedentes penales que ha de solicitar el propio candidato. Debe comprobarlos todos los empleados independientemente del puesto o cargo a desempeñar. Atención, un sujeto con antecedentes por robo hace 20 años no es suficiente motivo para no contratarlo.

Consulte las redes sociales. Le ayudará a conocer un poco al sujeto a contratar. No prejuzgue.

Compruebe las referencias y otros datos escritos en el curriculum

Es conveniente preguntar por los periodos de inactividad laboral para saber qué se han debido.

Entrevista personal. ¿Qué espera el solicitante del puesto de trabajo?: Comuníquele qué puede esperar del trabajo y en qué consistirán sus funciones, para evitar frustrar aspiraciones. Uno de los secretos que más contribuyen a la satisfacción personal de los empleados consiste en seleccionar y colocar en cada puesto de trabajo al empleado cuyas características personales mejor se adapten al mismo, cumpliendo con los requisitos de aptitud y predisposición necesarios para el puesto.

Realice preguntas abiertas: Realice preferentemente preguntas abiertas. Las preguntas cerradas pueden responderse a menudo con pautas aprendidas para este tipo de pruebas.

Riqueza de matices: Las respuestas a este tipo de preguntas le proveerán de datos más matizados y espontáneos, a la vez que marcarán mucho más las tendencias de la personalidad del candidato. Evite respuestas cortas.

Estas pautas deben ser realizadas por un experto en RRHH:

- Analice la expresión no verbal: El análisis de la expresión no verbal sirve para saber lo que está pensando realmente el entrevistado:
- Escuche con atención: Hay que escuchar atentamente sin interferir demasiado.
- Análisis de reacción a preguntas: Mientras se preguntan datos laborales clave, observe la expresión del entrevistado para así entrever la ocultación o cambio de información. A menudo no es lo que el empleado dice, sino cómo lo dice, por ello fíjese también en el tono de voz.
- Lenguaje del cuerpo: El idioma del cuerpo puede esconder ciertas pistas: Fíjese en la duración de las expresiones. Hay que ser un experto para detectar e interpretar el lenguaje corporal. A no ser que el entrevistado se ponga a bostezar continuamente durante la entrevista.
- Detección de drogadicciones: Averigüe mediante los síntomas percibidos si el candidato es adicto a algún tipo de droga. Un empleado drogodependiente va a necesitar a menudo fuertes sumas de dinero para mantener su adicción.

b) Política de la empresa

La política de una empresa queda reflejada en sus objetivos, normas y procedimientos. A la hora de dirigir la Organización es interesante considerar los siguientes aspectos:

- Realizar una selección de personal con procedimientos donde se consideren tres factores: profesionalidad (actitud y aptitud), ética y valores.
- La Empresa debe tener una buena planificación de proyectos y objetivos con una organización, dirección y control bien asentados capaz de detectar problemas en el seno del grupo. Por escrito.
- Asignación de responsabilidades bien definidas de acuerdo a las actividades a desempeñar. Por escrito.
- Asignar el personal a niveles de gerencia y mandos, con alta capacidad y conocimientos amplios.
- Establecer reglamentos, códigos y políticas organizativas
- Establecer protocolos de actuación.
- Establecimiento de sistemas de supervisión y control
- Revisión, corrección o establecimiento de unas normas de trabajo. (Normas empleado)
- Supervisión de personal
- Supervisión de la red informática
- Fomento de valores éticos y morales dentro de la plantilla. Contribuye al desarrollo de un clima general de honradez.
- Mayor participación del área de gestión de proyectos en estos conceptos
- Control de inventario
- Instrucciones eventuales siempre por escrito.

c) Recomendaciones para evitar el robo de información.

Evitar el hurto de información

https://www.youtube.com/watch?v=yHOymwvbX1U

Usted, como responsable de la Empresa, debe prestar atención a:

- ✓ Una escasez de artículos de inventario más frecuente o en mayor cantidad.
- ✓ Empleados que se nieguen a tomar vacaciones o ascensos.
- ✓ Patrones de negocio que cambien cuando cierto empleado está ausente.
- ✓ Empleados que se muestren incómodos antes preguntas rutinarias sobre procedimientos.
- ✓ Asegúrese de tener sus papeles en orden. Evite dejar documentos sobre el escritorio o post-its con palabras clave, contraseñas o cualquier otra información sensible a la vista.
- ✓ Guarde siempre sus claves de acceso en un lugar seguro. Si las tiene dentro de su ordenador, que sea en una aplicación encriptada, y nunca las lleve anotadas en papeles en la cartera. Tampoco las anote en su móvil.
- ✓ Controle quién tiene acceso a su lugar de trabajo, y trate de limitarlo lo posible.
- ✓ Evite proporcionar sus datos a terceros. Dejar la contraseña del ordenador a un empleado, por mucha confianza que tenga presenta riesgos. Recuerde que muchos de los robos de información se deben a empleados descontentos.
- ✓ Evite que el personal administrativo, ingrese medios de almacenamiento masivo como USB, Ipod, etc., ya que el 66% de la información robada se realiza por este medio.
- ✓ Acceso a la información. Indique como cláusula del contrato la prohibición de divulgar información confidencial. Establezca una política escrita acerca de quién, cuándo y bajo qué circunstancias puede acceder a la información clasificada. Prohibida la divulgación de información confidencial de la compañía.

- ✓ Controlar el inventario y activos a través de la instalación de cámaras de circuito cerrado es una de las formas más eficaces para prevenir el robo hormiga.
- ✓ Disponer de áreas restringidas, donde solo podrán acceder los usuarios autorizados; preferentemente con un sistema electrónico de control de acceso, que lleve un registro detallado de las horas de ingreso y salida.

d) ¿Cómo evitar descuadres de caja o robos de dinero por parte de trabajadores?

La mayoría de los robos en un comercio son por parte de personal de la empresa. Esto provoca que, cada vez más, las empresas busquen soluciones para paliar este mal que afecta a un elevado número de negocios, aunque dónde más se produce es en el sector de la hostelería.

En este tipo de negocios se dan una serie de circunstancias que facilitan los descuadres en caja:

- Alta rotación de trabajadores que acceden al efectivo de caja durante la jornada.
- Elevado ritmo de trabajo y stress.
- Bajos sueldos del personal.
- Contrato de tipo temporal de los trabajadores.

Estas circunstancias crean un contexto ideal para favorecer los descuadres de caja tanto por robos como por errores humanos.

Otros propietarios de negocios de hostelería optan por designar un trabajador de confianza (o ser ellos mismos) quien accede al efectivo de caja. Esta solución puede generar ineficiencias en la gestión de cobros ya que si el trabajador está ocupado en otros menesteres, el cliente deberá esperar para pagar y recibir su cambio y no quedará satisfecho con el servicio. Si no queremos que suceda esto último, deberíamos inmovilizar un trabajador en caja con el coste que ello supone.

Otros dueños de negocios, asumen un descuadre diario en sus cuentas debido a errores y continúan con su negocio mientras este sea rentable.

Según Hollinger y Clark, dos investigadores que estudiaron a 9,000 empleados de EE.UU., es el descontento en el trabajo y no la búsqueda directa de dinero, la razón principal que lleva al hurto.

Los sistemas utilizados para combatir el hurto interno son en primer lugar el CCTV, el uso de personal interno de confianza y la contratación de una empresa de seguridad y asesoramiento. Son parte de los mismos medios que ante el hurto y robo externo.

El efecto disuasión se puede conseguir con la instalación de una simple cámara de seguridad; estaríamos ante la disuasión explícita. Si aprehendemos a un empleado tras hurtar, o le castigamos (despido, suspensión de sueldo) el efecto disuasión es implícito. La finalidad de la disuasión es disuadir del delito, no recuperar la mercancía o el dinero robado. Además desmonta la racionalización del delito del sujeto. La correcta utilización de medidas preventivas como la disuasión, evitará gran parte de las medidas correctivas, siempre más desagradables de aplicar.

e) Normativa del empleado

La normativa del empleado es una de las expresiones más importantes derivadas de la política de la empresa. Es la implantación de una serie de normas que servirán de guía de referencia para todos los empleados. Una normativa es un documento que recomienda una acción concreta para cualquier situación en la que se puedan encontrar los empleados durante el desempeño de su trabajo. Las Consecuencias de la falta de normas claras y explícitas sobre la función del empleado y sobre la penalización de la figura del delito, ayuda a que aparezca la racionalización. Se verá al final del tema.

Notificación de controles: Los empleados deberán estar informados de la aplicación de medidas electrónicas, humanas y organizativas contra el hurto. Por supuesto dando la información estrictamente necesaria.

Notificación de sanciones: El procedimiento de sanción por quebrantar las normas ha de constar claramente en la normativa. El mero hecho de comunicar las posibles sanciones de los delitos contribuye a eliminar comportamientos nocivos.

Aplicación real de la normativa: Los empleados deben saber que cualquier violación de la normativa tendrá la correspondiente sanción. Ello ayudará a crear un efecto de no-impunidad. La inmediatez en la aplicación del castigo aumentará su efecto ejemplificador. Las notificaciones tienen como misión corregir cautelarmente la conducta de los empleados cuando existan desviaciones de la conducta. Han de seguir un criterio progresivo: Advertencia oral, Advertencia escrita, Entrevista, Despido disciplinario.

Defina qué es delito[18]: La normativa indicará al empleado qué es considerado como delito en la compañía. La normativa del empleado tendrá una importante función disuasiva al determinar explícitamente los comportamientos que no serán tolerados, acabando con posibles excusas de desconocimiento.

Implicación. Pregunte al empleado, hágale partícipe del negocio.

Previsión de situaciones habituales: Es una guía que permite la toma de decisiones en situaciones repetitivas. Englobe todos los aspectos y situaciones que puedan plantearse en el devenir diario del negocio, informando al director de seguridad.

Previsión en situaciones de emergencia: Esto se realiza a través del documento plan de autoprotección y emergencia.

Formación. Es conveniente, no sólo desde el punto de vista del negocio, sino desde la visión de la seguridad, formar habitualmente al empleado con cursos eficientes; esto es una motivación.

Salvaguarda de responsabilidades. Tener una normativa escrita constituye una salvaguarda en las responsabilidades del funcionamiento del negocio. También

[18] No me refiero a la definición legal de delito contemplada en el Código Penal

ha de tener en cuenta que el cumplimiento de la normativa exculpará a los empleados que la apliquen correctamente y sin mala fe de cualquier consecuencia derivada de su cumplimiento.

Periodo de prueba. Antes de poner en vigor la normativa del empleado, es necesario someterla a un periodo de prueba. Las normas han de demostrar su efectividad sobre el terreno. Este periodo de prueba servirá para determinar las modificaciones necesarias.

Requisitos de las normas

- ✓ **Sencillez:** Las normas han de ser de fácil aplicación.
- ✓ **Equidad:** No mida con diferentes raseros un mismo delito. La falta de equidad puede fomentar la sensación de injusticia, agravando así la propensión al hurto. Cualquier empleado debe ser consciente de que lo que se persigue es el delito y no a las personas.
- ✓ **Conocimiento obligatorio**: Puede especificar dentro del contrato una cláusula en la que se exprese el compromiso de conocer los contenidos de la normativa del empleado, una vez pasado el periodo de formación. La empresa ha de entregar la normativa a cada uno de los empleados, incluyendo un acuse de recibo mutuo. De lo contrario, podría encontrarse con veredictos exculpatorios del empleado deshonesto por falta de información de las acciones consideradas como contrarias al funcionamiento de la empresa.
- ✓ **Objetivos realistas**: Las normas están para ser cumplidas. Una normativa poco realista quedará pronto en papel mojado.
- ✓ **Integración de normas:** La normativa del empleado ha de tener en cuenta la integración de procedimientos para hacer factible su cumplimiento. Ej.: Un empleado de caja presencia el hurto cometido por un cliente en la superficie de ventas. La normativa del empleado indica que cualquier empleado que presencie un acto delictivo cometido en el establecimiento deberá informar al departamento de seguridad; pero la misma normativa también indica que un empleado de caja no podrá abandonar su puesto hasta no ser relevado de su función.

Política de autorizaciones. La normativa del empleado ha de expresar claramente cuál será la política de autorizaciones y cuáles serán sus requisitos, así como las actividades sujetas a tales autorizaciones.

f) Otras consideraciones generales

Autorización de cheques: Haga una lista de las personas autorizadas a firmar cheques. Informe al banco cuando una persona autorizada deje la empresa.

Prohibición de firma en blanco: No dejar nunca cheques en blanco firmados por una de las partes, porque entonces desaparecerá la doble responsabilidad. La doble firma cumple una función de control que evita falsificaciones y desfalcos.

Autorizaciones canceladas o caducadas: Los documentos desechados deben ser cancelados por el director de seguridad. Cuando se hayan caducado se estudiará si se debe prorrogar la autorización

Prohibición de entrega de llaves: Indique las personas que pueden tener acceso a cada una de las llaves. Limite su entrega, en la medida de lo posible, sólo a los jefes o encargados. Si detecta duplicidad de llaves debe comunicarlo inmediatamente al Departamento de Seguridad.

Dietas y gastos. Incluya la prohibición de cubrir gastos que no puedan justificarse. Especialmente en comerciales y representantes.

Vacaciones. La forma de distribución de los periodos vacacionales ha de expresarse explícitamente en la normativa del empleado. Fomente la rotación.

Cuadrantes. La distribución del cuadrante de trabajo debe ser equitativa y rotativa.

Supervisión de devoluciones: En tiendas, cualquier abono de una devolución debe cumplir con la firma del encargado y cajero.

Anotación de datos del cliente: Deben anotarse los datos del cliente que realiza la devolución, en vista de posibles comprobaciones.

Recepción y expedición de mercancías. Los proveedores deben saber las normas por las que se rige la empresa, así evitará excusas de malentendidos por su desconocimiento. Establecimiento de horario de recepción: Establezca un horario para el envío y la recepción de mercancías. Así podrá prever la supervisión por un empleado autorizado.

Firma de albaranes de recepción: Sólo los empleados autorizados podrán firmar albaranes de recepción o envío. Para evitar confusiones, marque las facturas con el sello de "Pagado" inmediatamente después de abonarlas.

Acceso de empleados, usuarios y proveedores fuera de horas. Indique las restricciones de autorización para acceder al establecimiento fuera de horas. El conserje o la seguridad deben anotar el objeto de la visita, así como la hora de entrada y de salida, y debe de acompañar al empleado o proveedor en todo momento. (Este punto depende del número de efectivos que tenga la empresa)

La aceptación de regalos por parte del personal de recepción de mercancías o representantes puede suponer indirectamente una compra de favores por adelantado y una tentación hacia el retorno del favor por parte de los agasajados.

GPS. En el caso de representantes, comerciales, repartidores es conveniente el Seguimiento de vehículos. Puede instalar GPS en todas las unidades móviles, de esta manera podrá conocer las rutas y la localización de su flotilla.

Compras de empleados.

Asigne una caja tutelada por un encargado para tales compras. Dichas compras deben realizarse en un horario restringido, fuera del horario de trabajo.

Rebajas a los empleados: Permita que los empleados compren, para uso personal, productos del establecimiento a precio de coste. Debe especificarse por escrito la política concreta de rebajas para empleados. Ha de indicar los productos rebajados y su importe.

Beneficios del descuento a empleados: Esta posibilidad reduce considerablemente el peligroso sentimiento de ingratitud o de abandono por parte de la compañía. Cuando un producto se puede comprar más barato que el precio que pagan los clientes, es más difícil que los empleados consideren su hurto, además, las compras de los empleados fomentan la rotación de productos.

Caja registradora

Retirada de llave: Indique la obligatoriedad de retirar la llave de acceso a apertura ante cualquier ausencia del empleado.

Registro escrito de retiradas de efectivo: Tanto quien hace la retirada de efectivo como quien la recibe deben firmar la transacción.

Cuadre y firma tras finalización de cajero: Con cada finalización de jornada, cada cajero ha de cuadrar caja y firmar los registros y facturación correspondientes en la hoja de contabilidad. Si falta dinero habrá de abonarlo. El empleado encargado de recoger los rollos internos ha de meterlos en un sobre en el que conste: Día, cajero y firma como sello de cierre. Guarde los rollos en un lugar de acceso restringido a cajeros.

Bolsos junto a caja: Prohíba la entrada de determinados objetos personales al puesto de trabajo. Instale taquillas para empleados y consignas para clientes y visitantes.

Para evitar no registros en línea de cajas.

Entrega de ticket de caja: El ticket o la factura son pruebas verificables del registro y garantía de una compra, por ello siempre deben entregarse al cliente junto con el cambio.

Entrega de ticket de cargo a tarjeta: El ticket de cargo a tarjeta es la prueba verificable de la extracción bancaria hacia el establecimiento, por ello siempre debe entregarse al cliente.

Destrucción de tickets: Los tickets no entregados por los clientes deben ser destruidos para evitar su posible entrega posterior tras un no registro.

Prohibición de dejar pasar: Prohíba explícitamente que se deje pasar compras con importe justo en medio de otra compra.

Prohibición de delegación de anulaciones: Prohiba la delegación del nivel de acceso que permite la anulación del producto sin la verificación del encargado.

Registro de anulaciones: Lleve un registro de anulaciones y los motivos que las causaron. Ej.: El cliente se quedó sin dinero, Cambió el producto por otro.

Registro obligatorio de traspasos de caja: Regule las suplencias momentáneas de un cajero dejando una identificación exacta de cuáles han sido exactamente los momentos de suplencia y quién los ha cubierto, con el fin de evitar vacíos de responsabilidad.

Reparto de funciones

El reparto de funciones permite delimitar claramente las atribuciones de autoridad y responsabilidad.

El reparto de funciones debe constar dentro de la normativa del empleado. De esta manera se evitarán las dudas de quién es el responsable de cada una de las tareas de la empresa.

Publicación del organigrama de la empresa y de cada departamento haciéndolo llegar a todos los empleados.

Evite el vacío de poder. En todo momento debería de haber una persona de guardia responsable de todo el establecimiento en todos los sentidos.

Turnos alternativos: Es por ello conveniente establecer turnos alternativos en las vacaciones de los encargados.

Responsabilidad. El reparto de funciones significa que cada empleado sepa sobre qué es responsable, ante quién, y cuando es responsable.

Responsabilidad individual: Es la asignación o fijación de funciones a cada empleado. Cada empleado debe conocer exactamente cuál es su función dentro de la empresa, así como su responsabilidad individual, para lo cual debe de establecer y delimitar de forma clara su autoridad y responsabilidad.

La persona coordinadora es importante ya que donde todos tienen el mismo poder, nadie se responsabiliza de nada.

Responsabilidad / autoridad: “A los trabajadores del taller, a los encargados de compras, a los ingenieros, hay que darles la autoridad necesaria. Deben sentir que son propietarios de lo que hacen. Las empresas que no acepten lo que viene de abajo van a la catástrofe”. López de Arriortúa, exdirectivo de General Motors y Volkswagen, del libro “Superlópez, más allá de sus memorias” (mayo de 1993).

Si delega la responsabilidad, delegue también la autoridad necesaria para cumplirla.

Segregación de funciones: La acumulación de funciones facilita un hurto hasta el punto de poder cometerse sin dejar el más mínimo rastro. La segregación de funciones ayuda a que se forme algo tan imprescindible como el control mutuo. Ninguna persona o departamento controle los registros contables relativos a sus propias operaciones

Forma de segregación de responsabilidades: Un empleado que observe irregularidades y no quiera hacerse responsable o firmar la situación dejada por otro empleado es más probable que tome las medidas necesarias para corregir los hechos.

En establecimientos pequeños es más difícil realizar la segregación, por la propia configuración del negocio. En este caso es preferible que determinadas funciones susceptibles de malversación sean realizadas directamente por el propietario del negocio.

Alternancia de tareas: Cambiar periódicamente las tareas de los empleados permite un control de responsabilidad mutua entre empleados porque la realización del control del propio trabajo supone un control del trabajo del compañero con quien se intercambia la tarea. Con ello se consigue:

**Cambia la rutina: Se evita que el trabajo se haga monótono y aburrido, con lo que disminuye el descontento que es uno de los factores favorecedores de la deshonestidad.*

**Mejora el conocimiento mutuo: Los empleados conocen las funciones de los demás empleados, favoreciendo así la flexibilidad de la plantilla hacia las diferentes tareas.*

**Evita control exclusivo: La alternancia de tareas evita un control exclusivo de determinadas áreas por parte del trabajador.*

**Intercambio revelador: Al hacerse cargo un determinado empleado de la totalidad de las funciones que normalmente corresponden a otro, pueden descubrirse fallos y deshonestidades.*

Normalmente los cambios de tareas no suelen gustar a los trabajadores porque deben adaptarse (implica esfuerzo) a una nueva situación tras estar acomodados en su puesto. Y por otra parte pueden encontrarse un problema en el nuevo puesto (implica delación o "comerse el marrón"

La mayoría de los empleados que hurtan lo hacen tras racionalizar sus conductas y aprovechar la oportunidad y tras tener una necesidad. La necesidad no es económica necesariamente, puede ser física, psicológica, social o individual, en definitiva es emocional, simplemente es una justificación. La oportunidad es el momento en el que "nadie mira" para hurtar algo. Las medidas preventivas para evitar los robos están sustentados en eliminar la oportunidad (las cámaras de seguridad, los vigilantes y los controles) Pero es el proceso psicológico de la racionalización el que hace que el empleado deshonesto busque las formas de burlar los sistemas de seguridad. Como ejemplos de racionalización encontramos:

- ✓ "La empresa gana demasiado", "lo que tomo es insignificante"
- ✓ "Es como quitarle un pelo a un gato"
- ✓ "Todos lo hacen, es algo normal llevarse cosas de la empresa"
- ✓ "Todos son deshonestos, partiendo por los políticos, los empresarios, esto es algo normal"
- ✓ "Nos pagan muy poco", "tenemos que arreglar nuestro salario"," es hacer justicia"
- ✓ "Lo necesito, la empresa no"
- ✓ "Me explotan en esta empresa, es una forma de justicia"

7.2 Recomendaciones de seguridad en comercios

Empleados atentos. Avise a la policía. Jamás, jamás haga frente usted **sólo** al ratero, en momentos de desesperación por verse atrapado puede usar cualquier arma blanca oculta.

Asegúrese de poder ver todo lo que pasa en la tienda. Los mostradores deben estar a una altura menor de la cintura. Instale espejos en las esquinas para que no haya puntos ciegos.

Arregle los mostradores y las mesas de exhibición de la mercancía de manera que no haya vía directa hacia la salida de la tienda. Algunas tiendas instalan barreras rotatorias en las entradas para que la única manera de salir sea a través del área de la caja registradora. Coloque los artículos caros en el centro de la tienda, lejos de las salidas.

Arregle la exhibición de mercancía de manera que se note con rapidez si falta algo. Coloca los artículos pequeños en filas ordenadas o patrones claramente definidos

Los ladrones de tienda generalmente visten ropa abultada: abrigos, pantalones y atuendos de maternidad y llevan consigo mochilas y bolsas que pueden servir como lugares de escondite y algunas veces hasta pueden tener fondos falsos, procura vigilar a tus clientes con discreción.

Se debe adaptar la prevención al tipo de establecimiento y debe optarse por una selección ponderada de los medios o medidas de seguridad lógicas.

Un estudio de seguridad es imprescindible para conocer y aplicar las medidas de seguridad aconsejables y saber qué puntos débiles tenemos para poder eliminarlos. Consulte con un director de seguridad.

El uso evidente y habitual de medidas de seguridad hace desistir al delincuente en gran medida de cometer el delito.

La instalación del sistema de seguridad no es, en sí misma, suficiente. Además, es preciso que, tanto el propietario del establecimiento como los técnicos de la empresa de seguridad, lleven a cabo comprobaciones periódicas así como el mantenimiento y revisión adecuados de sus componentes, para garantizar su buen funcionamiento.

A mayor dificultad para el delincuente, mayor probabilidad de detención.

Un director de seguridad puede diseñar un proyecto de seguridad o mejorar el sistema existente.

Se debe avisar mediante carteles de la existencia de medidas de seguridad.

Se debe tomar precauciones extraordinarias si el establecimiento funciona en horarios no habituales.

Los teléfonos de emergencia, bomberos y policía deben estar siempre al alcance.

Es aconsejable instalar un timbre y un sistema de apertura remota de la puerta de acceso al establecimiento.

Proteger las lunas contra alunizajes e impactos.

Las lunas deben ser antirotura

Buena visibilidad desde el exterior hacia la tienda

Puede ser conveniente instalar rejas y/o persianas antipalanca y anticorte en puertas, ventanas y otros accesos del establecimiento (respiraderos, conductos de ventilación, tragaluces, aberturas de los sótanos, etc.). Las persianas no deben ser macizas para permitir la visualización del interior cuando estén echadas.

Es necesario instalar cerraduras de seguridad en puertas, ventanas y otros accesos al establecimiento y reforzar los marcos y las bisagras.

En caso de pérdida de llaves, cambiar la cerradura inmediatamente

Si pierde el mando de la persiana proceda igual.

Cuidado con las obras en la calle o en el mismo inmueble. Los andamios facilitan el acceso al establecimiento.

Comprobar la iluminación, que debe ser adecuada, el estado de las puertas y ventanas.

Las puertas deben ir dotadas de cerraduras anti¬atracos, bulones de seguridad y, si es posible, barras metálicas interiores que eviten los apalancamientos

Prestar atención a la parte exterior del local y cuidar que no haya marcas exteriores. Algunos delincuentes marcan los locales en el exterior y luego realizan butrones sobre los locales marcados.

Instale una alarma antiintrusión conectado a una Central receptora de alarmas (asegúrese de que la empresa instaladora esté homologada y que la respuesta que vaya a dar a la alarma sea eficaz)

Del mismo modo instale un sistema antiincendios.

En la apertura y el cierre se debe tener presente:

• Según la naturaleza del negocio puede ser recomendable tomar medidas de seguridad desde la salida del domicilio. Comprobar que no haya movimientos sospechosos, o desconocidos con conductas extrañas, y en caso de duda ponerse en contacto con la Policía.

• Hay que procurar que la persona que abra o cierre el establecimiento comercial esté acompañada.

• En el cierre, dejar la caja registradora vacía y visiblemente abierta para evitar que la fuercen en caso de robo.

• Evitar crear posibles escondites por almacenamiento de material y comprobar siempre que todas las instalaciones han quedado vacías (cuartos, baños, armarios, etc.).

• Asegurar siempre de que puertas y ventanas queden cerradas y el sistema de alarma conectado.

Alarmas exteriores:

Una buena forma de evitar robos en su negocio es contar con un sistema de alarma conectado a una Central Receptora de Alarmas.

El funcionamiento de las alarmas es posible dividirlo en cuatro fases:

1. Disuasión: la simple presencia de la placa indica a cualquier intruso que su negocio cuenta con un sistema de alarma, lo que puede traducirse en un aviso inmediato a las Fuerzas y Cuerpos de Seguridad del Estado en caso de intento de intrusión.

2. Detección: los detectores volumétricos se activan si registran movimiento y/o aumento de temperatura. Cualquier intento de intrusión hará que la señal de alarma llegue a la Central Receptora.

3. Recepción: las alarmas están conectadas a una Central Receptora. Cuando ocurre algo, los profesionales de la empresa de seguridad contratada contactan al instante para comprobar si se trata de una falsa alarma. De no ser así, proceden a llamar de inmediato a la Policía.

4. Intervención: es posible contratar con las empresas de seguridad un servicio de acuda inmediata, mediante el cual al activarse la alarma de su local le envían un vigilante.

Así, se puede decir que:

• La instalación de un sistema de alarma sonora adecuado al establecimiento y conectado a una central receptora de alarmas con una línea telefónica protegida, no visible y separada del resto de líneas es una medida de seguridad de gran importancia.

• En esta línea es conveniente revisar periódicamente los detectores volumétricos del sistema de alarma. Los delincuentes, en horario comercial y con el establecimiento abierto al público, colocan de forma discreta, una lámina de plástico transparente encima de los detectores, difícil de detectar a simple vista. Esto hace que los detectores no funcionen correctamente y que los delincuentes puedan aprovechar el horario de cierre del establecimiento para acceder sin ser detectados por el sistema de alarma. En estos casos no hay que tocar nada ni comentarlo con nadie y se debe avisar a los agentes de seguridad.

• Anunciar de forma bien visible que su establecimiento está protegido por un sistema de alarma.

• Asegurarse de que el personal conoce el sistema para eliminar los riesgos de falsas alarmas.

• Notificar un teléfono de contacto o el de la empresa instaladora a la Policía para que puedan avisar en caso de que suene la alarma.

Videovigilancia exterior:

La videovigilancia exterior conlleva el uso de cámaras con acceso a la vía pública. Se debe de recordar que la legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados. Por tanto la regla general es la prohibición de captar imágenes de la calle desde instalaciones privadas.

No obstante, en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas.

A veces también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta. Por todo ello el artículo 4.3 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, dispone:

"Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida."

Para que esta excepción resulte aplicable, no deberá existir una posibilidad de instalación alternativa. Debe tenerse en cuenta que:

• La utilización de instalaciones de videovigilancia en la vía pública se reserva a las Fuerzas y Cuerpos de Seguridad por la Ley Orgánica 4/1997, de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos.

• El artículo 4.3 de la Instrucción 1/2006 no constituye una habilitación para captar imágenes en espacios públicos.

• El responsable del fichero adecuará el uso de la instalación de modo que el impacto en los derechos de los viandantes sea el mínimo posible.

• En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

• La señalización garantizará en todo caso los derechos de los afectados.

• Las indicaciones de uso y seguridad facilitados al personal contendrán de modo expreso instrucciones específicas que garanticen un uso adecuado y proporcional de los recursos.

Ingresos de efectivo en entidades financieras

• La persona que realice los ingresos debe de proceder siempre con la mayor reserva posible. Evitar compartir información sobre estos movimientos.

• Escoger una oficina bancaria próxima al establecimiento.

• Variar la ruta de acercamiento a la oficina de la entidad financiera procurando ir por vías concurridas.

• También es conveniente no realizarlos siempre el mismo día a la misma hora. Hay que evitar rutinas y se debe ir variando para que los delincuentes no dispongan de pautas a seguir para cometer el delito.

• En caso de hacer el traslado en coche, cuidar de que esté siempre en buenas condiciones y con el depósito suficiente, evitar hacer paradas dejando el dinero en el vehículo y llevar éste, en un lugar que no sea accesible desde la ventanilla.

• Cuando se trasladen grandes sumas de dinero encima evitar, en la medida de lo posible, el trato con desconocidos.

• Durante el trayecto mantenerse alerta para detectar la presencia de posibles delincuentes que observen o tengan una actitud sospechosa.

• Si se sospecha de que puedan estar siguiendo, dirigirse a una comisaría o a un Policía.

• Evitar llevar mucho dinero en una única entrega a las entidades bancarias.

• No llevar el dinero en bolsas de mano o bandoleras colgadas del hombro. Se deben llevar en bolsillos interiores de la ropa. De esta manera evitaremos tirones.

• Considerar la posibilidad de contratar el servicio de alguna empresa de seguridad para realizar la recogida de la recaudación comercial.

7.3) Prevención en instalaciones varias

Bancos, cajas de ahorro y entidades de crédito

Departamento de seguridad

En todos los bancos, cajas de ahorro y demás entidades de crédito, existirá un departamento de seguridad, que tendrá a su cargo la organización y administración de la seguridad de la entidad bancaria o de crédito.

Asimismo, dichas entidades deberán conectar con una central de alarmas propia o ajena los sistemas de seguridad instalados en sus establecimientos y oficinas, salvo que dificultades técnicas hicieran imposible la conexión, en cuyo caso podrán ser obligadas, por el tiempo en que persista la imposibilidad técnica, a la implantación del servicio de vigilantes de seguridad, con personal perteneciente a empresas de seguridad.

Medidas de seguridad concretas

En los establecimientos u oficinas de las entidades de crédito o que actúen en nombre o representación de éstas, donde se custodien fondos o valores, deberán ser instalados, en la medida que resulte necesaria en cada caso teniendo en cuenta las circunstancias enumeradas en el artículo 112 del Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, y lo establecido en el Capítulo II de la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada:

- Equipos o sistemas de captación y registro, con capacidad para obtener las imágenes de los autores de delitos contra las personas y contra la propiedad, cometidos en los establecimientos y oficinas, que permitan la posterior identificación de aquellos, y que habrán de funcionar durante el horario de atención al público, sin que requiera la intervención inmediata de los empleados de la entidad.
- Dispositivos electrónicos, con capacidad para detectar el ataque a cualquier elemento de seguridad física donde se custodien efectivo o valores.

- Pulsadores u otros medios de accionamiento fácil de las señales de alarma.
- Carteles u otros sistemas de información de análoga eficacia, anunciadores de la existencia de medidas de seguridad con referencia expresa al sistema de apertura automática retardada y, en su caso, al sistema permanente de captación de imágenes.
- Las cajas fuertes deberán tener los niveles de resistencia establecidos y estarán protegidas con los dispositivos de bloqueo y apertura automática retardada. Cuando su peso sea inferior a 2.000 kilogramos, estarán, además, ancladas, de manera fija, en estructuras de hormigón armado, al suelo o al muro.

Los establecimientos u oficinas de las entidades de crédito o que actúen en nombre o representación de éstas, situados en localidades con **población superior a diez mil habitantes** deberán contar además, con una de las tres medidas de seguridad que se citan a continuación:

- El **recinto de caja** de, al menos, dos metros de altura y que deberá estar cerrado desde su interior durante las horas de atención al público, siempre que el personal se encuentre dentro del mismo, protegido con blindaje antibala del nivel que se determine y dispositivo capaz de impedir el ataque a las personas situadas en su interior, con el **nivel de blindaje** que se señala en el artículo 6 de la Orden INT/317/2011, de 1 de febrero. Se considerará recinto de caja el destinado a disponer de las cajas auxiliares en su interior.
- El **control individualizado de accesos** a la oficina o establecimiento, que permita la detección de masas metálicas, bloqueo y anclaje automático de puertas, y disponga de mando a distancia para el desbloqueo del sistema en caso de incendio o catástrofe, o puerta de emergencia complementaria, detectores de presencia o zócalos sensibles en vía de salida cuando se utilice el sistema de doble vía, con el **nivel de blindaje** que se determina en el apartado segundo del mencionado artículo 6.
- **Dispensadores de efectivo o recicladores** adecuados a lo dispuesto en el apartado tercero del artículo 122 del Reglamento de Seguridad Privada y en el artículo 13 de la Orden INT/317/2011, de 1 de febrero, cuando su instalación

sustituya a todas las cajas auxiliares. En caso de mantenerse alguna caja auxiliar, será preciso que ésta se encuentre dentro del recinto de caja.

En virtud del artículo 111 del Reglamento de Seguridad Privada, y al objeto de proteger el efectivo que manejen, las oficinas ubicadas en **poblaciones con menos de 10.000 habitantes deberán contar**con las medidas enumeradas en el primer apartado, y, además, si no disponen de alguna de las tres medidas de seguridad que se citan en el segundo apartado, con una caja auxiliar, que podrán ubicar en cualquier zona de la oficina bancaria, debiendo estar sujeta al suelo o pared, pudiendo hacerlo por procedimientos distintos a los contemplados en la Disposición Adicional Segunda de la Orden INT/317/2011, y reunir las características establecidas en el apartado segundo del artículo 122 del citado Reglamento.

En las localidades que cuenten con **una población entre 10.000 y 50.000 habitantes**, y en función de que superen o no la media nacional sobre robos con fuerza y robos con violencia o intimidación en entidades de crédito durante los dos últimos años, a contar desde la entrada en vigor de la Orden INT/317/2011 (18-08-2011), el Delegado o Subdelegado del Gobierno o, en su caso, la Autoridad autonómica competente, podrá dispensar el cumplimiento de las medidas de seguridad establecidas en el segundo apartado.

Cámaras acorazadas y cajas de alquiler

Las cámaras acorazadas de efectivo y de compartimentos de alquiler deberán tener las características y el nivel de resistencia establecidos en el artículos 8 y 10 de la Orden INT/317/2011, de 1 de febrero, y estar provistas de las siguientes medidas de seguridad:

- Dispositivo mecánico o electrónico que permita el bloqueo de su puerta desde la hora de cierre del establecimiento hasta la primera hora del día siguiente hábil.
- Sistemas de apertura automática retardada que deberá estar activada durante la jornada laboral, salvo las cámaras de compartimentos de alquiler que habrán de disponer de sistema electrónico de detección de ataques conectado las veinticuatro horas. En los supuestos en que las cámaras acorazadas, con la

finalidad de permitir el acceso a su interior en caso de emergencia, cuenten con trampones, éstos podrán estar libres de cualquier dispositivo de bloqueo o temporización, siempre que sus llaves sean depositadas para su custodia en otra sucursal próxima de la misma entidad o grupo.

- Detectores sísmicos, microfónicos u otros dispositivos que permitan detectar cualquier ataque a través de techos, paredes o suelos de las cámaras acorazadas o de las cajas de alquiler.
- Detectores volumétricos.
- Mirillas ojo de pez o dispositivos similares, o circuito cerrado de televisión en su interior, conectado con la detección volumétrica o provistos de videosensor, con proyección de imágenes en un monitor visible desde el exterior. Estas imágenes deberán ser transmitidas a la central de alarmas o, en caso contrario, la entidad habrá de disponer del servicio de custodia de llaves para la respuesta a las alarmas.

Cajas fuertes y cajeros automáticos

Las **cajas fuertes** deberán tener los niveles de resistencia establecidos en el artículo 9 de la Orden INT/317/2011, y estarán protegidas con los dispositivos de bloqueo y apertura automática retardada. Cuando su peso sea inferior a 2.000 kilogramos, estarán, además, ancladas, de manera fija, en estructuras de hormigón armado, al suelo o al muro.

Para el funcionamiento del establecimiento u oficina, las **cajas auxiliares**, además de cajón donde se deposita, en su caso, el efectivo necesario para realizar las operaciones, estarán provistas de elementos con posibilidad de depósito de efectivo en su interior, de forma que quede sometido necesariamente a apertura retardada para su extracción.

Los **cajeros automáticos** deberán estar protegidos con las siguientes medidas de seguridad:

- Cuando se instalen en el vestíbulo del establecimiento:

a. Puerta de acceso blindada con acristalamiento resistente al menos al impacto manual del nivel que se determine, y dispositivo interno de bloqueo.
b. Dispositivo de apertura automática retardada en la puerta de acceso al depósito de efectivo, que podrá ser desactivado, durante las operaciones de carga, por los vigilantes de seguridad encargados de dichas operaciones, previo aviso, en su caso, al responsable del control de los sistemas de seguridad.
c. Detector sísmico en la parte posterior.

- Cuando se instalen en fachada o dentro del perímetro interior de un inmueble, las medidas establecidas en los párrafos b) y c) anteriores.
- Cuando se instalen en el interior de edificios, locales o inmuebles, siempre que éstos se encuentren dotados de vigilancia permanente con armas, los cajeros automáticos quedan exceptuados del cumplimiento de las anteriores medidas de seguridad, y únicamente se exigirá que estén anclados al suelo o al muro, cuando su peso sea inferior a dos mil kilogramos.
- Si los cajeros automáticos se instalaran en espacios abiertos, y no formaran parte del perímetro de un edificio, deberán disponer de cabina anclada al suelo, y estar protegidos con las medidas mencionadas en el caso de que los cajeros se instalen en el vestíbulo del establecimiento.

Oficinas de cambio de divisas

Los establecimientos u oficinas pertenecientes a entidades de crédito u otras mercantiles, dedicadas exclusivamente al cambio de divisas, estacional o permanentemente, dispondrán como mínimo de las medidas de seguridad previstas para las Administraciones de Loterías y Apuestas Mutuas.

Los **bancos móviles** o módulos transportables, utilizados por las entidades de crédito como establecimientos u oficinas, deberán reunir, al menos, las siguientes medidas de seguridad:

- Protección de la zona destinada al recinto de caja y puertas de acceso con blindaje de cristal antibala de la categoría y nivel que se determinen, para evitar el ataque al personal que se encuentre en el interior de dicho recinto. El recinto de caja permanecerá cerrado desde su interior, durante las horas de atención al publico, siempre que el personal se encuentre dentro del mismo.
- Caja fuerte con dispositivo automático de retardo y bloqueo, que deberá estar fijada a la estructura del vehículo del módulo. La caja auxiliar estará provista de cajón de depósito y unida a otro de apertura retardada.
- Señal luminosa exterior y pulsadores de la misma en el interior.
- Carteles anunciadores de la existencia de medidas de seguridad.
- Servicio propio de vigilantes de seguridad, en el supuesto de que no se cuente con servicio de vigilancia de las Fuerzas y Cuerpos de Seguridad o con servicio de vigilantes de seguridad del inmueble o recinto en que se ubiquen.

La autorización para el funcionamiento de estos establecimientos corresponderá al Director General de la Policía o al Delegado del Gobierno de la provincia, según el ámbito territorial. Una copia de la autorización deberá estar depositada en la correspondiente unidad o módulo.

Joyerías, platerías, galerías de arte y tiendas de antigüedades

Medidas de seguridad concretas

En los establecimientos de joyería y platería, así como en aquellos otros en los que se fabriquen o exhiban objetos de tal industria deberán instalarse, por empresas especializadas y, en su caso, autorizadas, las siguientes medidas de seguridad:

1. Caja fuerte o cámara acorazada, para la custodia de efectivo y de objetos preciosos, dotada de sistema de apertura automática retardada, que deberá estar activado durante la jornada laboral, y dispositivo mecánico o electrónico que permita el bloqueo de la puerta, desde la hora de cierre hasta primera hora del día siguiente hábil. Cuando la caja fuerte tenga un peso inferior a 2.000 kg.,

deberá estar anclada, de manera fija, en una estructura de hormigón armado, al suelo o al muro.

2. Pulsadores antiatraco u otros medios de accionamiento del sistema de alarma, instalados en lugares estratégicos.
3. Rejas en huecos que den a patios y pasos interiores del inmueble, así como cierres metálicos en el exterior, sin perjuicio del cumplimiento de las normas de lucha contra incendios.
4. Puerta blindada, con resistencia al impacto manual del nivel que se determine, en todos los accesos al interior del establecimiento, provista de los cercos adecuados y cerraduras de seguridad.
5. Protección electrónica de escaparates, ventanas, puertas y cierres metálicos.
6. Dispositivos electrónicos con capacidad para la detección redundante de la intrusión en las dependencias del establecimiento en que haya efectivo u objetos preciosos.
7. Detectores sísmicos en paredes, techos y suelos de la cámara acorazada o del local en que esté situada la caja fuerte.
8. Conexión del sistema de seguridad con una central de alarmas.
9. Carteles, u otros sistemas de información de análoga eficacia, para su perfecta lectura desde el exterior del establecimiento, en los que se haga saber al público las medidas de seguridad que éste posea.

Los establecimientos de nueva apertura deberán instalar cristales blindados en escaparates en los que se expongan objetos preciosos, cuyo valor en conjunto sea superior a **90.151,82 euros**. Esta protección también será obligatoria para las ventanas o huecos que den al exterior.

Las galerías de arte, tiendas de antigüedades y establecimientos que se dediquen habitualmente a la exhibición o subasta de objetos de joyería o platería, así como de antigüedades u obras de arte, cuyas obras u objetos tengan un valor superior a **500.000 euros**, deberán adoptar las medidas de seguridad que se establecen en los párrafos b), c), d), e), f), h), e i) anteriormente reseñadas, y además, proteger con detectores sísmicos el techo y el suelo del establecimiento y las paredes medianeras con

otros locales o viviendas, así como con acristalamiento blindado del nivel que se fija en el apartado anterior los escaparates de los establecimientos de nueva apertura en que se exhiban objetos por la cuantía en el mismo determinada.

EXHIBICIONES O SUBASTAS OCASIONALES

Con independencia del cumplimiento de las normas aplicables, las personas o entidades que pretendan exhibir o subastar públicamente objetos de joyería o de arte, en locales o establecimientos no dedicados habitualmente a estas actividades deberán comunicarlos, con una antelación no inferior a quince días, al Delegado del Gobierno de la provincia donde vaya a efectuarse la exhibición o subasta.

Atendiendo a las circunstancias que concurran en cada caso y a los informes recabados, el Delegado del Gobierno podrá ordenar a los organizadores la adopción, con carácter previo a las exhibiciones o subastas, de las medidas de vigilancia y seguridad que considere adecuadas.

Gasolineras

Las estaciones de servicio y unidades de suministro de combustibles y carburantes **dispondrán de una caja fuerte**, que habrá de estar construida con material con grado de seguridad 4, debiendo contar, como mínimo, con la protección de un detector sísmico, un dispositivo de bloqueo y sistema de apertura retardada de, al menos, diez minutos. El sistema de bloqueo deberá estar activado desde la hora de cierre del establecimiento hasta la hora de apertura del día siguiente hábil. Cuando su peso sea inferior a 2.000 kilogramos, deberán estar ancladas, conforme a lo establecido en laDisposición Adicional Segunda de la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada.

Una de las llaves de la caja fuerte estará en poder del encargado del negocio u otro empleado y la otra en posesión del propietario o persona responsable de la recogida de los fondos, **sin que en ningún caso pueda coincidir la custodia de ambas llaves en la misma persona, ni en personas que trabajen juntas**.

A fin de permitir las devoluciones y cambios necesarios, cada empleado de las estaciones de servicio y unidades de suministro de combustibles y carburantes no podrá tener en su poder, cantidades de dinero superiores a **600 euros** en efectivo. En el caso de autoservicios, la caja registradora no podrá contener más de **1.200 euros** en efectivo. El dinero que exceda de estas cantidades deberá ser introducido en la caja fuerte.

Las estaciones y unidades de suministro podrán disponer, advirtiéndolo al público usuario mediante carteles situados en lugares visibles, que sólo se despachará combustible por cantidades determinadas de dinero, de forma que puedan ser abonadas por su importe exacto sin necesidad de efectuar cambios.

Oficinas de farmacia

Todas las oficinas de farmacia deberán contar con un dispositivo de tipo túnel, bandeja de vaivén o bandeja giratoria con seguro, que habrán de estar ubicados en un elemento separador que impida el ataque a las personas que se hallen en el interior. La utilización de esta medida será obligatoria únicamente cuando las farmacias presten servicio nocturno o de urgencia.

Los citados dispositivos podrán ser sustituidos por persianas metálicas, rejas homologadas, cristal blindado homologado, una pequeña ventana practicada en el elemento separador, o cualquier otro dispositivo con similares niveles de seguridad.

Lotería y apuestas mutuas

Las Administraciones de Lotería y los Despachos Integrales de Apuestas Mutuas Deportivo-Benéficas dispondrán de un recinto cerrado en el que existirá una caja fuerte, que deberá cumplir las caracterícas establecidas en el artículo 9 de la Orden INT/317/2011, de 1 de febrero, en la que se custodiarán los efectos y el dinero en metálico.

La parte del recinto destinada al público estará totalmente separada, por elementos o materiales de blindaje del nivel que se determine, de la zona reservada a los empleados que realicen transacciones con el público, la cual estará permanentemente

cerrada desde su interior y dotada de dispositivos que impidan el ataque a dichos empleados.

Las transacciones con el público se harán a través de ventanillas dotadas con un dispositivo tipo túnel, bandeja de vaivén o giratoria con seguro.

Locales de juegos de azar

Los **casinos** de juego dispondrán de las medidas de seguridad establecidas en el apartado anterior sobre Administraciones de Lotería y Apuestas Mutuas.

Las **salas de bingo** para más de 150 jugadores, y los salones de máquinas de juego para más de 75 máquinas de juego dispondrán de una caja fuerte con sistema o mecanismo que impida la extracción del dinero a través de la abertura destinada a su introducción en la caja, y dos cerraduras protegidas. La caja, que deberá tener las características enumeradas en el mencionado artículo 9 de la Orden INT/317/2011, estará empotrada en una estructura de hormigón armado, preferentemente en el suelo. Una de las llaves de la caja fuerte estará en poder del encargado del negocio u otro empleado y la otra en posesión del propietario o persona responsable de la recogida de los fondos, sin que en ningún caso pueda coincidir la custodia de ambas llaves en la misma persona, ni en personas que trabajen juntas.

7.4) Prevención en incendios provocados

Existen algunos indicadores de posibles fraudes en este tipo siniestros, entre otros:

El intermediario/asegurado tiene un historial de cambios frecuentes de compañía aseguradora: una adquisición repentina de cobertura para riesgos no asegurados anteriormente: una adquisición reciente de cobertura para interrupción de la actividad; aumentos inesperados de las cantidades asegurada anteriores reclamaciones dudosas: edificios y10 contenidos en venta: pérdida de un cliente importante.

Las empresas con una o varias de las características siguientes pueden ser vulnerables: alto nivel de endeudamiento; dependencia de las modas cuando un cambio

repentino da origen a productos anticuados: hipercapacidad o competencia comercial feroz en el sector industrial: rápida expansión de las ventas sin una gestión adecuada de los recursos financieros: fuerte dependencia de los bancos.

En su centro de trabajo

• Recuerde que generalmente por descuido se puede producir un incendio.

• Cumpla con las medidas de seguridad establecidas.

• Solicite que periódicamente revisen la instalación eléctrica.

• No sobrecargue los enchufes con demasiados aparatos; distribuya las cargas o solicite la instalación de circuitos adicionales.

• No fume en zonas restringidas, ni dentro de los elevadores.

• Apague totalmente los cerillos y las colillas de los cigarros; no los arroje encendidos al cesto de la basura.

• Evite la acumulación de basura.

• Conozca la ubicación de los extintores, equipo contra incendio y alarmas y aprenda a utilizarlos.

• Identifique claramente las rutas de evacuación, las salidas de emergencia y los puntos de revisión.

• No obstaculice las salidas de emergencia, ni los lugares donde se encuentra el equipo contra incendios.

• Encargue las revisiones y composturas eléctricas al técnico responsable; no las haga usted mismo.

• Sugiera que se realicen ejercicios y simulacros de evacuación y participe responsablemente en ellos.

• Solicite que se instalen detectores de humo.

• Pida información a la unidad de Protección Civil de su centro de trabajo sobre el plan de emergencia en caso de incendio.

• Si quiere colaborar en el combate de un incendio, intégrese con anticipación a la unidad de Protección Civil de su trabajo, en donde lo capacitarán.

• Antes de salir de su lugar de trabajo, cerciórese de que no haya colillas encendidas y de que cafeteras, parrillas, ventiladores y otros aparatos eléctricos estén desconectados.

Anexo

Cómo actuar ante una Llamada por Amenaza De Bomba

La Actuación del Operador

1. Mientras se responde y se habla con el comunicante (con calma y serenidad)
   - ✓ Anotar nombre del comunicante o nombre del que representa
   - ✓ Anotar si es hombre o mujer
   - ✓ Edad aproximada
   - ✓ Características de la voz (Calmada, enfadada, nasal, cansada, miedosa, grabada, disfrazada, etc ...)
   - ✓ Tono de voz (Lento, rápido, empleo de frases tipo y modismos, buena o mala pronunciación, seseo, ceceo, etc...)
   - ✓ Acento de la voz
   - ✓ Grado de colaboración (Educado, cortante…)
   - ✓ Ruidos de fondo (otras personas, tráfico, pájaros, música, máquinas etc.)
   - ✓ Anotar las palabras exactas que pronuncie
2. Preguntar ¿Cuándo explotará la bomba?
3. Preguntar ¿Dónde se encuentra la bomba?
4. Preguntar ¿Qué aspecto tiene?
5. Preguntar ¿Qué clase de bomba es?
6. Preguntar ¿Qué quiere que hagamos?
7. Preguntar ¿Puso usted la bomba?
8. Preguntar ¿Por qué puso la bomba?
9. Intente prolongar la llamada, esto nos puede dar más información
10. Debemos fijarnos en:
    - Si dice "yo" o "nosotros".
    - Si utiliza "evacue el personal" o "evacue su personal".
    - Si apunta con respecto a la colocación "he puesto" o "hemos puesto"; etc...

Bibliografía

http://www.redsafeworld.net/cultura-de-la-seguridad/

www.pwc.com/crimesurvey

https://www.agpd.es/portalwebAGPD/index-ides-idphp.php

http://www.mir.es/MIR/estrorganica/estructura/subsec/sgt1.html

Criminal Law Lawyer Source: Employee Theft

http://aecoc.es/aecoc/admin/web/general/Recomendaciones%20AECOC%20Perdida%20Desconocida.pdf

http://www.palermo.edu/economicas/contadores/presentaciones/Binder1.pdf

http://www.forodeseguridad.com/artic/segcorp/7208.htm

http://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/red_azul_presentacion.php

Belt Ibérica

Emergemap

http://derecho.isipedia.com/

Los robos de empleados en España ascienden a 454 millones de euros anuales

Protección contra el fraude, más vale prevenir que curar

Ministerio Interior

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD)

Ley de Seguridad Privada)

Documento para realizar Auditorías de Seguridad de Soto & Poveda Asociados

Autoridad Nacional para la protección de la protección de la información clasificada NS/03 - Seguridad física

CPD Seguridad Directores de Seguridad. Medios técnicos de Protección

Mapfre. Incendios provocados

La pérdida desconocida. Benjamín García (Juspedia)