

ARES

Revista
Protección
Integral

Edición 1 Nº 8 Septiembre 2008

Quito - Ecuador - Sur América

Protección Corporativa,
Clima Laboral Ético y
Desarrollo de la
Seguridad

Autoprotección
Repunte del Secuestro en
Ecuador y Venezuela

Seguridad Informática
Uso del Celular para
Lavado de Dinero

FUNDACIÓN

IPC

Integrated protection
concepts

Creando Cultura de Seguridad

Índice



Seguridad Corporativa
Clima laboral ético y Políticas de Prevención



Autoprotección
Repunte del Secuestro en Ecuador y Venezuela

Pág. 8



Seguridad Industrial
Seguridad en el Diseño de Plantas Industriales

Pág. 12



Seguridad Física
Importancia del Operador de Seguridad

Pág. 20



Seguridad Electrónica

Mecanismo de Protección de las Tarjetas Inteligentes

Pág. 25



Seguridad Informática

Uso del Celular para Lavado de Dinero

Pág. 29



Manejo de Crisis y Emergencias

Planes de Evacuación

Pág. 33



Seguridad Ciudadana

Cuatro pasos para salvar una vida

Pág. 36



Selección de Personal

Escolta: Presencia Capacidad, Entrenamiento

Pág. 39

DIRECTOR
Ing. Kevin Palacios, CPP, PSP, CPOI
e-mail: kpalacios@ipc.org.ec

EDITOR
Lic. María Fernanda Torres
e-mail: ftorres

COMITÉ EDITORIAL
Ing. Kevin Palacios, CPP, PSP, CPOI
Rubén Recalde, CPP, CPO
Lic. María Fernanda Torres
Francisco Llobregat

COORDINADORA COMERCIAL
Mónica Valencia

e-mail: mvalencia@ipc.org.ec

PRODUCTOS SECURITY

Gabriela Aguirre

e-mail: gaguirre

PRODUCTOS SAFETY

Edwin Carrillo

e-mail: ecarrillo@ipc.org.ec

**FUNDACIÓN IPC
INTEGRADOS DE PROTECCIÓN**

Av. Eloy Alfaro N 35 128 y Portugal
Quito – Ecuador

Tel: (593
Fax: (593 2) 227
info@ipc.org.ec

www.ipc.org.ec

TIRAJE: 6500 suscriptores
12 países

DISTRIBUCIÓN GRATUITA

Los contenidos de esta publicación pueden ser reproducidos por editor y haciendo referencia a la fuente Fundación IPC se reserva el derecho de aceptar o rechazar cualquier publicidad que se entregue para su publicación en la revista ARES.

Una organización del Grupo:



ADEMÁS

CURSOS Y EVENTOS

Pág. 42



SEGUR

2008

FERIA INTERNACIONAL DE SEGURIDAD

Adquiera su stand desde \$60 m²
Del 20 al 23 de noviembre del 2008



Centro de Exposiciones y Convenciones
MITAD DEL MUNDO

OFICINA QUITO

Paris N42-167 y Tomas de Berlanga Piso 2

Telefonos: 2446882 • 2448189 • 2449851

Fax: 2274174

E-mail: cemexpo@cemexpo.com.ec

RECINTO FERIAL

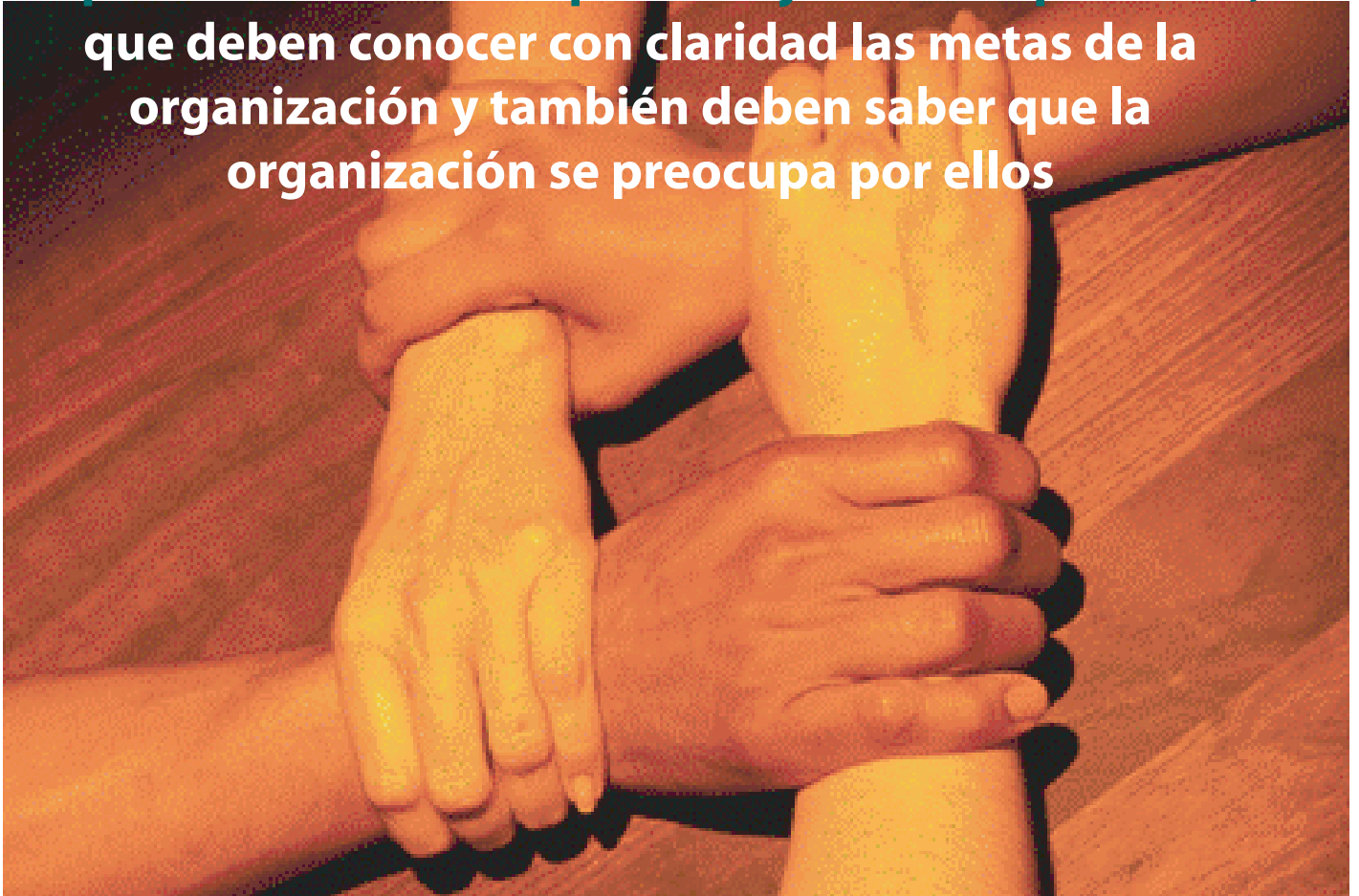
Av. Autopista Manuel Córdova Galarza Km.9
Telefonos: 1700-ferias / (593-2)2350053 / 043

Fax: (593-2) 2350028

E-mail: cemexpo@cemexpo.com.ec

Cuando una empresa u organización trabaja con ética laboral, mejora los niveles de servicios y ventas a sus clientes y los niveles de fidelidad de estos, por eso es importante reconocer que trabajamos con personas,

que deben conocer con claridad las metas de la organización y también deben saber que la organización se preocupa por ellos



Clima laboral ético y políticas de Prevención

En el mercado actual, altamente competitivo, atraer y retener talento humano se está convirtiendo en un verdadero reto. Por lo tanto, proporcionar horarios de trabajo más flexible que proporcionen un balance entre el trabajo y la vida personal no es únicamente importante para una satisfacción laboral sino también, es fundamental mantener al empleado valorado y así desarrollar cultura ética laboral, que en muchos lugares es imperativo. Así, los cargos de liderazgo, con el fin de fomentar normas éticas dentro de las organizaciones, primero, tienen que proporcionar un entorno que sea adecuado para el comportamiento ético.

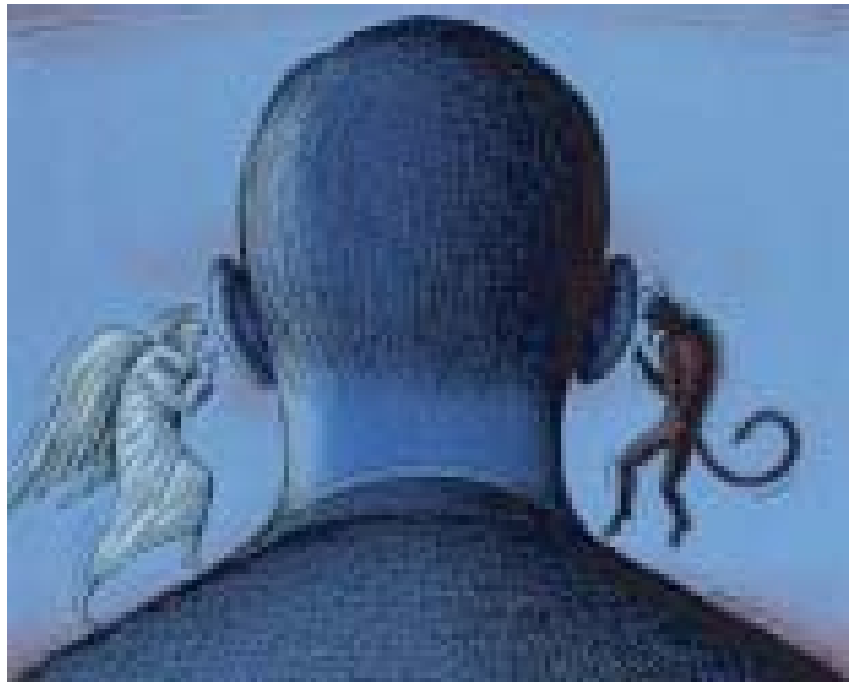
El clima laboral se echa a perder generalmente por pequeños actos torpes y mezquinos, que se van acumulando como la basura debajo de la alfombra, hasta que ya nadie puede obviarlos.

Lo primero que ocurre es la inconsistencia, o incoherencia (que a efectos organizacionales es lo mismo) Se dice algo y se hace otra cosa; se tiene un discurso sólidamente estructurado pero se le desprecia con los actos opuestos y evidentes. Las personas son menos tontas de lo que parecen, por lo que lo notan.



Es importante poner en consideración 3 aspectos de la ética antes de relacionarla con la prevención de riesgos laborales.

- **Primero, la ética parte de la vida y pretende fortalecerla.**
- **Segundo, la ética no tiene nada que ver con premios o castigos de la autoridad, sea ésta divina o humana.**
- **Tercero, la ética es propia de la humanidad y se manifiesta cuando tratamos y somos tratados como personas.**



Dependiendo de las estructuras de la personalidad presentes, esto puede generar desde un indiferente desprecio hasta frustración. Como sea, el "proyecto" y el "liderazgo" ya se han trizado.

Rápidamente vendrán las crisis de confianza, y las personas comenzarán a advertir los boquetes en el escenario. Y pronto se instalará la duda, lo que puede ser letal.

La pérdida de credibilidad generalizada frenará el involucramiento personal en el proyecto y se caerá con facilidad en el mero cumplimiento.

La pérdida de credibilidad provoca desgaste emocional, genera falta de energías, cansancio matutino, la clásica sensación de "estar fundido" que a veces mueve incluso a evitar la interacción con los demás. El rendimiento decrece, comienza una relación impersonal con el trabajo, hay menor concentración y memoria, y sobre todo falta de optimismo. Dos señales modernas del desvanecimiento de la ética laboral son el aumento en las llegadas tarde al trabajo y el abuso del permiso por enfermedad.

Así, el respeto a la dignidad personal es tan importante como el margen de ganancia. Y ello pasa fundamentalmente por la coherencia que es confianza motivadora, porque se trata de un elemento que está a la base de toda personalidad.

En cualquier ámbito de la vida, y también en las relaciones laborales, las acciones vienen motivadas por órdenes recibidas, por costumbres, deseos o decisiones racionales. Cada categoría motivacional tiene sus propias características, y todas ellas intervienen en

mayor o menor medida en nuestras acciones diarias laborales, y en concreto en las relacionadas con la seguridad en el trabajo. En la Prevención de riesgos laborales una vez implementadas las normas de trabajo seguro, evidentemente respaldadas por medios técnicos adecuados, y de profesionales, la ética laboral se fusiona en el trabajo y cada trabajador será responsable de su propia seguridad y de su equipo. Establecer y cumplir un código de ética es fundamental.

De este modo, "el empresario deberá asumir nuevas obligaciones éticas, y no como un deber,

sino como un factor competitivo, como son el desarrollo de competencias internas en la compañía, sanidad preventiva, trabajo temporal senior, responsabilidad social corporativa, conciliación con la vida familiar, para asegurar el bienestar de sus empleados, cuya máxima expresión será la satisfacción por el trabajo bien hecho, y el orgullo de pertenecer a la empresa".

Fuente:

http://www.deloitte.com/dtt/cda/doc/content/ec_en-us_ethics_workplace2007_080807.pdf

http://www.vertisub.com/articulos/OTROS/%C3%89tica_y_prevenci%C3%B3n_de_Riesgos_Laborales.pdf

<http://etica.duoc.cl/temas/4.pdf>

Aumento de fraudes lleva a empresas a ser más rigurosas al elegir ejecutivos de confianza

Hace dos meses, el ex jefe de tesorería de la compañía Bavaria, Carlos Germán Quintero, fue capturado en el aeropuerto El Dorado, en Bogotá, por el presunto desvío irregular de cerca de 1.400 millones de pesos.

La empresa cervecera, tras una investigación interna, detectó en sus cuentas movimientos irregulares de dineros y decidió por este hecho denunciar por hurto agravado a su ejecutivo ante la Fiscalía. Hoy el proceso sigue en investigación.

Este caso de fraude, que para muchos pasó inadvertido, es uno más de los que a diario se registran en el país pero de los que no existen estadísticas, pues la mayoría de empresas prefieren callarlos para proteger su imagen.

Según un estudio de la multinacional KPMG, que analiza riesgos en el interior de las compañías, el 85 por ciento de quienes cometen fraude en las empresas son hombres, un 70 por ciento se ubica en rango de edades de entre los 36 y 55 años, el 89 por ciento son empleados internos, el 68 por ciento actúa en forma independiente y un 60 por ciento son miembros de la alta dirección. "Los fraudes administrativos son más comunes de lo que la gente cree y es el reflejo de que la inseguridad también tiene en jaque a las compañías", dice Carlos Rincón, analista económico.

Para los expertos es claro que muchos de los fraudes que ocurren en las compañías obedecen al poco rigor en el proceso de selección laboral, a la debilidad en los controles internos, a la poca capacidad empresarial para evaluar riesgos y a la precaria forma que aplican para mitigarlos. "Las empresas tienen que entender que este es un problema al que hay que prestarle mucha atención porque vincula desde la ética hasta el equipo de trabajo -agrega Rincón-. Y por eso es necesario que siempre haya procedimientos de vigilancia y gestión de riesgo".

El informe de KPMG señala, por ejemplo, que en un 49 por ciento los fraudes ocurren por la poca vigilancia y en un 46% son detectados por denuncias anónimas o revisiones de la dirección. "Esto es una enfermedad silenciosa que no denuncian las empresas para no dañar su imagen o para no afectar sus procesos, pero que cada vez es más notoria", recalca un analista en seguridad de una multinacional.

La recomendación para las empresas es no entregarles a los empleados toda la información de los procesos ni los procedimientos de la organización y observar "con sospecha" cualquier actitud intempestiva o ciertas extravagancias. También medir valores intangibles como la ética del empleado y la trayectoria en escenarios difíciles y verificar las hojas de vida pues muchas personas suelen falsificar certificados y es claro que el que adultera una recomendación, una constancia o un diploma, no dudará en alterar un cheque, una factura o un contrato.

Lo cierto es que estos casos recientes de fraudes alertan a las empresas para poner más ojo avizor sobre sus manejos de recursos y sobre su estructura administrativa. Así que el mejor consejo es mirar con lupa a quién se contrata para evitar dolores de cabeza futuros. ISCLA - international Security Consultants (ISRAEL)

Fundación

Conceptos Integrados en Protección

-IPC-

Le invita a participar en la Conferencia

ACTUALIZACIÓN

LEGAL EN

SEGURIDAD

PRIVADA

Octubre 06 - 07

-QUITO-

Octubre 10 -11

-MANTA-

Octubre 15 - 16

-GUAYAQUIL-

Reglamento de la Ley de
Vigilancia y Seguridad
Privada y Reglamento de
la Ley de Manejo de
Armas. Cambios en la
Constitución

No permita que le sancionen!!!

Informes y Suscripciones

Fundación -IPC- Av. Eloy Alfaro N 35-144 y Portugal

Telf. (593 2) 2923 600 | 601 Cel. 098 104 457

E-mail. info@ipc.org.ec

FUNDACIÓN

IPC

Integrated protection
concepts

Creando Cultura de Seguridad

Repunte del Secuestro en Ecuador y Venezuela

La organización No gubernamental holandesa IKV Pax Christi alertó el 14 de Agosto, en un informe, sobre un repunte de los casos de secuestros en Ecuador y Venezuela.

En el Informe presentado, la Organización pacifista, que opera en Colombia y en otros países, establece que el incremento de plagio en ambos países es atribuida a la delincuencia común y a la falta de políticas estatales para combatirla.

El informe, resultado de una investigación sobre la exportación de la práctica del secuestro a los países vecinos desde Colombia, establece que los casos de secuestros en este país responden a razones políticas y económicas y que la retención suele extenderse por años, mientras que en Ecuador y Venezuela, los secuestros duran

horas o días y su objetivo es netamente económico.

La modalidad más común de secuestros en estos países se define como secuestro Express en la que los plagiarios demandan una suma de dinero relativamente pequeña a cambio de la libertad de la persona que queda libre en pocas horas. La modalidad también incluye el llevar a la víctima a sacar dinero de sus cuentas en cajeros automáticos.

De acuerdo a la legislación ecuatoriana el delito comúnmente conocido como secuestro está tipificado en el

código penal como Plagio, y el secuestro Express es legalmente catalogado como robo agravado.

En Ecuador, las estadísticas manejadas por las instituciones involucradas, Unidad Antisecuestros de la Policía (Unase), la Policía Judicial y la Escuela Superior Politécnica del Litoral (Espol) reflejan esa confusión, pues la Unidad Antisecuestros -UNASE- reportó 247 secuestros de carácter extorsivo desde el año 2000 hasta el 2007, la policía judicial registró desde el 2004 hasta octubre de 2007 un total de 1.270 casos de secuestros y la Espol citó que en 2005 y 2006

1.270 casos de secuestros y la Espol citó que en 2005 y 2006 tuvieron lugar, solo en Guayaquil, 1.048 y 1.000 secuestros, respectivamente, destacó el informe.

En julio del 2008, la Policía Judicial recibió un total de 36 denuncias de plagio o secuestro, correspondientes a 6 denuncias en la Provincia de Pichincha, 5 en Guayas, mientras que secuestros Express, a nivel nacional es de 6, cinco (5) denuncias en la Provincias del Guayas y 1 en Manabí. El total de estos delitos evidencian, sin que se logre establecer si es una disminución de denuncias o del hecho, pues en el mes de junio, se denunciaron 44 casos de plagio o secuestro y 10 de secuestro Express.

Por otro lado, los delitos denunciados en las oficinas del Ministerio Público, en la ciudad de Guayaquil, entre el 16 de agosto y el 22 de agosto de 2008, maneja las siguientes cifras: 11 denuncias de plagio y secuestro, y 5 denuncias de secuestro Express. Cifras



que comparadas con la semana del 9 al 15 de agosto de 2008, muestran una disminución de casos de secuestro (16) mientras que no se ha presentado variación de denuncias de secuestro Express (5)

La aprobación de la Ley Reformativa al Código Penal, en el 2005, establece una reclusión mayor especial de 16 a 25 años para quienes en el cometimiento del delito -"retención o apoderamiento de las personas, mediante amenazas, violencia, o cualquier otro medio ilegítimo, dentro de un vehículo motorizado, y castigar con mayor severidad en caso de que los delincuentes utilicen el automotor para cometer otros crímenes"- hayan causado la muerte o la incapacidad permanente de la o las víctimas.

En el caso venezolano, La Asamblea Nacional venezolana aprobó una ley que incrementó hasta a 30 años las penas de prisión para secuestradores

Autoprotección

sus familiares, como una medida para contrarrestar ese flagelo.

Según el Cuerpo de Investigaciones Científicas Penales y Criminalísticas, el número de secuestros en Venezuela pasó de 44 en 1999 a 382 en 2007, lo que equivaldría un 48,6 por ciento más que el 2006 cuando se registraron 257. Según esta información, el estado Zulia, fronterizo con Colombia, registró el mayor índice de secuestros al ubicarse en 73 casos, en su mayoría de productores agropecuarios, de los cuales, cinco aún permanecen secuestradas. Distrito Capital segunda en la lista, registró 41 casos, con dos personas aún en cautiverio. El modus



operandi más común fue el secuestro Express y el perfil predominante ha sido el de la figura de comerciante. El estado llanero de Barinas, estuvo cerca de Distrito Capital con 36 casos de secuestros y Táchira, también fronteriza con el país colombiano, tuvo 35 casos.

RECOMENDACIONES PARA PREVENIR UN SECUESTRO EXPRESS (ROBO AGRAVADO)

- 1.- Estar atentos en la calle y al salir o entrar a nuestra residencia u oficina. Estar pendientes si nos siguen.
- 2.- Si es notificado por otro conductor que observa problemas en su vehículo, no se detenga sino en un sitio seguro.
- 3.- No recoja a desconocidos, no importa el sexo o la apariencia.
- 4.- Si siente que lo están siguiendo, permita que el carro que lo sigue lo pase y deténgase en un lugar público para solicitar ayuda.
- 5.- Si un motorizado lo amenaza gire bruscamente y luego retírese del lugar a fin de evitarlo.
- 6.- Cuando camine por la calle aléjese de los bordes de las aceras.
- 7.- Sea discreto, evite hacer comentarios sobre el dinero que recibe.
- 8.- Evite hacer transacciones en cajeros ubicados en lugares de poca seguridad.
- 9.- Evite tener las ventanas abiertas de su vehículo, sobre todo en semáforos o en tránsito lento.
- 10.- Evite dejar el vehículo estacionado en la calle.
- 11.- En la calle, evite comprar artículos a vendedores ambulantes.
- 12.- No utilice prendas llamativas cuando salga a la calle.



13.- Cuando entre a su residencia, esté atento a las personas que se encuentran en los alrededores. Es prudente pasar de largo para verificar mejor la zona y luego proceder a entrar, sobre todo en horas nocturnas.

14.- No suministre información sobre sus bienes y su poder adquisitivo.

15.- Hágle caso a su intuición.

"...Nunca cambie un lugar abierto por un lugar cerrado..."

RECOMENDACIONES PARA MANEJAR UNA SITUACIÓN DE SECUESTRO EXPRESS (ROBO AGRAVADO)

- **No sea víctima, en la calle no se comporte como una víctima. Si cayó en manos de delincuentes, y es una víctima, trate de controlar su emoción**
- **No sea usted factor que informa, no diga: "mi papá tiene dinero, mi marido resuelve esto, en la casa tengo dólares..."**
- **No diga espontáneamente en donde vive. Recuerde que el punto de inseguridad en donde estamos parados es irreversible, o nos adaptamos o sencillamente perecemos.**
- **Minimice su nivel y situación social. No mencione que conoce a personas o sectores influyentes. Usted es una simple persona que está dispuesto a entregar lo que tiene, pero no lo que no tiene**
- **Negocie con elementos ciertos, no con falsedades o promesas... Si por ejemplo tiene dinero en la casa, no lo informe.**
- **Recuerde que el tiempo está a favor suyo. Los delincuentes necesitan negociaciones rápidas y efectivas.**
- **Recuerde que en la negociación se plantea un juego de poder. Las horas que dura un robo agravado son de tensión, miedo, nervios y angustia.**

EJERCITE LA "PRECAUCIÓN"

1. Disminuya la excesiva confianza en lugares o gentes desconocidas.
2. No dé información sobre sus viajes y desplazamientos. Evite dar datos exactos o modifíquelos a última hora.
3. Mantenga una buena y cordial relación con sus vecinos, ya que podrán ayudarlo al presentarse una emergencia.
4. Evite multitudes de cualquier tipo. Es generalmente, el caldo de cultivo para operar el criminal en "arrebataadores" y otros delitos afines.
5. Memorice por favor, los números telefónicos de Emergencia que se utilizan comúnmente y que pueda necesitar ante un hecho como el descrito.
6. Si porta un arma de fuego, debe estar preparado(a) psicológicamente y conocer " bien su uso", así como la legislación básica sobre "Defensa

Propia".

7. Las armas de fuego no son para exhibirlas, amenazar o "jugar" con ellas.
8. Trate a todas las armas de fuego como si estuviesen cargadas. Jamás apunte a alguien jugando, solo a quien esta dispuesto a dispararle. NUNCA deje (armas) al alcance de los niños.
9. Al llamar durante un situación de emergencia interna o externa, recuerde informar PRIMERO LA UBICACIÓN EXACTA de usted, luego los hechos y detalles posteriores.
10. No desestime a las MUJERES en cuanto a su participación activa en hechos delictivos: un notable porcentaje de los delitos contra la propiedad y las personas (robos, hurtos, lesiones y homicidios, etc.) son cometidos o ejecutados por ó con la participación cómplice y activa de "ellas"

Fuente:

<http://www.ecuadorinmediato.com/noticias/23669>
<http://www.eluniverso.com/2008/08/16/0001/10/C5000DFDC37340C18D247B5D93F8E97B.html>
http://www.icm.espol.edu.ec/delitos/ultima_semana.htm
 Estadísticas Policía Judicial -junio y julio 2008-
<http://www.inforc.ec/inforc/secuestroexpress.htm>
<http://www.elsequestro.com/consejos.php>

Estudios de

La Seguridad en el diseño y el proceso depende principalmente del empleo de los diversos códigos de diseño, que requieren experiencia y conocimiento de expertos y de especialistas.

de riesgo y Operatividad

ño de las plantas de
almente del modo de
códigos de práctica o
se basan en la vasta
ntos de profesionales
alistas en la Industria

Todo proyecto nuevo incluye algún elemento de cambio pero en la industria de procesos el grado de cambio de una generación de plantas a otra es, a menudo, considerable. Es importante reconocer que la parte principal de la experiencia establecida, que se manifiesta en los códigos, está limitada por el grado de los conocimientos existentes y solo puede ser relevante en la medida en que sea posible aplicársela a productos nuevos, plantas nuevas, y métodos nuevos de operación involucrados en el nuevo diseño. Se ha vuelto cada vez más claro, en años recientes, que aunque los códigos de práctica son extremadamente valiosos, es particularmente

importante complementarlos con una anticipación imaginativa de los riesgos, sobre todo cuando los proyectos involucran una tecnología nueva.

Invariablymente después de un accidente y a veces, cuando se encuentran dificultades operacionales importantes, existe una forma de investigación para establecer la causa o las causas. A menudo, una vez que estas se han encontrado, la falla en el diseño o en los métodos de operación parece obvia. Esto sucede a pesar del cuidado que se tenga, tanto en el diseño de la planta como en la comprobación del mismo. En parte aprendemos gracias a la experiencia pero,

mientras esto es valioso, puede ser costoso en términos del sufrimiento humano y de las pérdidas financieras.

Por lo tanto, necesitamos alguna forma de "experiencia sintética" que haga casi tan fácil descubrir los problemas en perspectiva como en retrospectiva. Los estudios de riesgos y operabilidad, HazOp (Hazard and Operability) son el método de proporcionar la forma de esa experiencia sintética. Funcionan utilizando la imaginación de los componentes del grupo para que visualicen las maneras en que una planta puede funcionar mal o puede ser mal operada. Sin embargo, la sola imaginación no es suficiente. Los ingenieros utilizan mucha imaginación al diseñar una planta, por lo tanto la imaginación de los integrantes del grupo de análisis debe guiarse y estimularse de una manera sistemática pero creativa para que abarque todas las partes de la planta y todos los casos de mal funcionamiento y mala operación imaginables. Esto se logra en lo que se llama el "análisis".



decide si estas desviaciones pueden dar origen a riesgos.

El interrogatorio se enfoca por turnos en cada parte del diseño. Cada parte se somete a un número de preguntas que se formulan alrededor de un número de palabras guías que se originan en técnicas de estudios de métodos. Las palabras guías se utilizan para asegurarse que las preguntas, que se plantean para examinar la integridad de cada parte del diseño, exploren todas las formas imaginables en

que ese diseño se podría desviar de su propósito.

Eso por lo general produce una cantidad de desviaciones teóricas y cada desviación se tiene en cuenta para decidir de qué manera se podría presentar y cuáles serían las consecuencias.

Algunas de las causas pueden ser irreales, de tal manera que las consecuencias que de ahí provengan se rechazan por no tener ningún significado.

Esencialmente el proceso de análisis interpreta la descripción completa del proceso, cuestiona sistemáticamente cada parte de él, para descubrir cómo es que las desviaciones del intento del diseño se pueden presentar, y

Algunas de las consecuencias con causas imaginables y que sean potencialmente correctivas. Después de haber analizado una parte del diseño y haber anotado cualquier riesgo potencial asociado con él, se continúa con el estudio para enfocarlo en las siguientes partes del diseño. El análisis se repite hasta que se haya estudiado toda la planta.

El objetivo del análisis es identificar todas las posibles desviaciones de la forma como se espera que el diseño funcione,



y todos los riesgos asociados con esas desviaciones. Además, algunos de los riesgos se pueden prevenir. Las decisiones se pueden tomar en el acto y el diseño se puede modificar inmediatamente, si la solución es obvia y no existe la posibilidad de que cause efectos adversos en las otras partes del diseño. Esto no siempre es posible, pues puede que sea necesario obtener más información. De esta manera, el resultado de los análisis consiste

Una lista de chequeo de palabras guías es utilizada luego en forma sistemática, para identificar riesgos potenciales y problemas de operabilidad que pueden derivarse de las desviaciones de esa intención del diseño.

Las causas posibles de tales desviaciones se registran junto con las consecuencias, las protecciones existentes en el diseño y las recomendaciones del equipo de estudio para limitar la severidad o reducir la posibilidad de que se presenten los peligros que originan riesgos.

Limitaciones

La metodología de HazOp es diseñada principalmente para revisar la información mostrada en los Diagramas de Tubería e Instrumentos (P&IDs) y los procedimientos de operación asociados. Información no mostrada en los P&IDs (por ej. Detalles de distribución del equipo) y modos de operación no cubierto por los procedimientos disponibles para el análisis, no será cubierta totalmente y se necesitarán **revisiones separadas para su consideración.**

normalmente de una mezcla de decisiones y de preguntas que deben ser contestadas.

ESTUDIOS DE RIESGO Y OPERABILIDAD HazOp

Un estudio HazOp es una técnica sistemática formal para identificar riesgos potenciales y problemas de operabilidad, inherentes en diseños de plantas de proceso. No es una técnica para resolver o cuantificar estos problemas.

Aplicación

La técnica Hazop puede ser aplicada a procesos tanto continuos como discontinuos, durante la etapa del diseño de plantas nuevas, o modificaciones a plantas existentes, y a plantas en operación, en la condición de "como fueron construidas".

La técnica ha tenido desarrollos posteriores a su creación para la identificación de riesgos en actividades de operación, que involucran equipos, procedimientos y personal.

También se ha desarrollado un método en la metodología estándar de Hazop para incorporar análisis de riesgos introducidos por error humano. Si se aplica de una manera consistente y sistemática, este enfoque ayuda a identificar situaciones, equipo y factores relacionados que pueden crear peligros a los procesos, causados por factores humanos.

El sistema o procedimiento que va a ser estudiado se divide en elementos pequeños (secciones o nodos) y la intención del diseño de cada uno de estos elementos se explica al equipo de análisis.



Los estudios HazOp consideran usualmente riesgos que se originan de una o al menos dos fallas creíbles y por lo tanto no cubrirán todos los eventos catastróficos o de múltiples fallas. Estos eventos de accidentes mayores son mejor identificados por un enfoque de arriba-abajo tal como Hazid o un Análisis de Árbol de Fallas.

La efectividad del estudio para identificar y evaluar los riesgos creíbles descansa en el conocimiento, experiencia y motivación de los miembros del equipo de análisis como también de la competencia del jefe líder del estudio.

APLICACIÓN A INSTALACIONES NUEVAS

La técnica se aplica normalmente cuando el diseño está esencialmente completo (omisión de los P&IDs) Sin embargo puede aplicarse en etapas preliminares del diseño, así que la mayoría de los problemas puedan manejarse durante la etapa del diseño detallado, y por lo tanto se pueda reducir el número de acciones recomendadas por el HazOp principal del diseño completo, o posibilitar cambios subsiguientes que va a ser cubierto por un riguroso procedimiento de revisión de cambios en el diseño.

Todos los cambios, incluso

aquellos que resulten de recomendaciones del HazOp deberán ser revisados y, donde sea apropiado, sujeto a un seguimiento del estudio HazOp.

APLICACIÓN A INSTALACIONES EXISTENTES

La técnica también puede ser aplicada a los P&IDs o procedimientos operativos de plantas existentes para identificar riesgos potenciales o problemas de operabilidad que no hayan sido descubiertos por la experiencia de la operación, o para revisar operaciones no estándares o procedimientos no cubiertos previamente.

Las modificaciones que involucren cambios significativos a los P&IDs, cambios a cómo opera el proceso o cambios a los sistemas de seguridad asociados, también deberán estar sujetos a estudios HazOp.

El alcance deberá indicar claramente si el estudio se va a limitar a las modificaciones solamente o se aplica a la planta entera. Todas las interfaces (proceso/servicio) entre la planta existente y las modificaciones se deberán identificar y analizar. Atención especial merecen las interconexiones (tie-ins) a la planta existente.

Alcance

El alcance del estudio deberá ser formalmente acordado entre el cliente/proyecto y el líder del estudio HazOp antes de que comience el estudio. En particular debe hacerse énfasis en que el estudio HazOp está especialmente interesado en la identificación de riesgos y los problemas de operabilidad, no en resolverlos ni en cuantificarlos.

HazOp conducido por el Contratista

En la mayoría de los proyectos grandes, la responsabilidad por la conducción del estudio HazOp es del Contratista del Diseño de Ingeniería, como parte de la revisión de éste.



OBJETIVOS DEL HazOp

El objetivo de un estudio Hazop es verificar el diseño completo del proceso para buscar desviaciones de la operación e interacciones del proceso, que pudieran dar lugar a situaciones peligrosas o problemas de operabilidad. Esto podría incluir:

1. **Peligros a la seguridad y la salud de los trabajadores.**
2. **Daños al equipo o a la propiedad.**
3. **Problemas de la operación o del mantenimiento.**
4. **No disponibilidad de la planta.**
5. **Calidad del producto.**
6. **Emisiones ambientales.**
7. **Peligros durante la construcción o la puesta en marcha.**

COMPOSICIÓN DEL EQUIPO

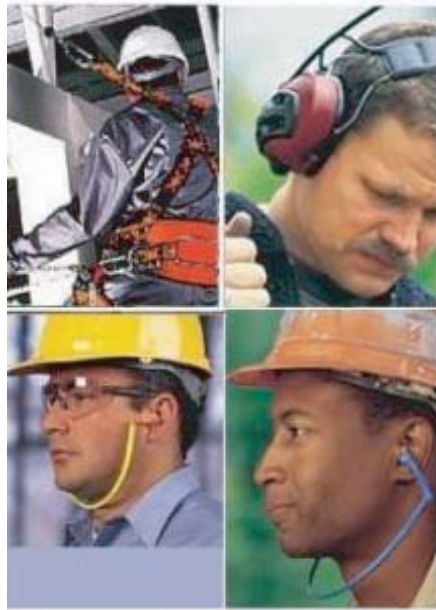
El equipo del estudio deberá incluir las varias disciplinas apropiadas para el sistema o procedimiento bajo estudio. Típicamente para estudios de proyectos complejos se requerirán ingeniería de proceso, ingeniería mecánica y expertos en arranque de plantas u operación de las mismas. Otros especialistas, como ingenieros de control, pueden ser requeridos por tiempo parcial o a través de todo el estudio, dependiendo del sistema que se esté revisando.

Un secretario permite que los miembros del equipo se puedan concentrar en los detalles del estudio sin la tarea de tener que preocuparse de llevar registros del trabajo. El secretario también se ocupa de otros aspectos administrativos y no participa en la discusión, salvo cuando se requieren aclaraciones relacionadas con los registros que debe llenar sobre las discusiones o las decisiones que tome el equipo.

Todo este equipo será dirigido por un líder, independiente del diseño del sistema, con suficiente experiencia en la actividad. No requiere conocer el sistema que se va a estudiar, pero líderes con experiencia en ingeniería de procesos u operaciones y con un nivel básico de conocimientos del sistema bajo estudio son más fácilmente aceptados por el resto del equipo.

El Líder también debe asegurar que se preparen registros claros y

precisos y reportes, para tomar responsabilidad formal por las recomendaciones que él acuerde con su equipo.



EL PROCEDIMIENTO HazOp

Un estudio de Hazop sigue una lista estructurada de pasos para asegurar un análisis completo. A continuación se describe cada uno de los pasos mayores en el proceso de revisión:

1. Seleccionar un nodo y explicar la intención del diseño

El Estudio se conduce dividiendo el proceso, representado en los Diagramas de Tubería e Instrumentos (P&IDs) en nodos o partes pequeñas del diseño que deben contener al menos un vasija, una bomba o intercambiadores y la tuberías de conexión. Cada nodo es analizado a su vez, hasta cuando todos los

planos hayan sido estudiados. El método preferido es comenzar desde el principio del proceso y seguir el flujo hasta terminar, dejando los servicios industriales para el final. En algunos casos esto no es posible.

Al principio del estudio, un representante del equipo, de operaciones, o ingenieros de proceso será solicitado para que dé una explicación del proceso.

Para asegurar que todos los miembros del equipo entiendan la porción del proceso bajo revisión, se suministrará una breve descripción de la intención del diseño de la sección. Esta descripción incluye información de los parámetros claves, tales como flujo, presiones, temperaturas, composición, niveles, etc.

2. Aplicar una palabra guía y desarrollar una desviación

El objetivo de Hazop es identificar problemas. Una premisa de la técnica es que solo puede existir un problema si el proceso se desvía del diseño. Las palabras guías son, por lo tanto, combinadas con los parámetros claves para desarrollar desviaciones. La combinación de la palabra guía NO con el parámetro "FLUJO" crea la desviación "NO FLUJO". En forma similar, las otras palabras guías serán combinadas con los otros parámetros para desarrollar desviaciones significativas. Puesto que se pueden concebir un gran número de desviaciones, solo aquellas que son significativas se aplicarán. Una desviación significativa se puede definir como aquella que tienen causas reales, y una consecuencia que puede crear un riesgo.

3. Identificar las causas de la desviación

Las causas de la desviación deben ser desarrolladas ahora a través de una tormenta de ideas. El líder debe iniciar la discusión y alentar

la creatividad del grupo para asegurar que todos los escenarios posibles sean considerados. Debe tenerse en mente la siguiente regla: la causa de la desviación deberá estar en la sección bajo análisis. Las consecuencias deben buscarse donde se produzcan. "La causa en el nodo, las consecuencias en cualquier parte". Todas las causas reales de la desviación se registran para su discusión.

4. Evaluar las consecuencias

Ahora las consecuencia de cada una de las causas deben ser examinadas y registradas. El equipo debe trabajar unido para identificar todas las consecuencias directas e indirectas. Estas deben ser discutidas hasta agotarlas sin tener en cuenta las protecciones de diseño y administrativas que ya están en aplicación para prevenir o mitigar el evento. Los miembros del equipo, utilizando sus vastos conocimientos y variadas experiencias, determinan la cadena de eventos que ocurrirán en el nodo como resultado de una causa dada. La base de los conocimientos del equipo tendrá un efecto significativo en su habilidad para predecir las consecuencias de un evento.

5. Identificar protecciones

Una vez que el equipo haya discutido lo que podría suceder, deberá discutir las razones de diseño o de tipo administrativo para que el evento no ocurra. Estas protecciones pueden reducir la probabilidad del evento o mitigar sus efectos, siendo deseable lo primero. Las protecciones incluyen entre otras: sistemas de enclavamiento y apagada de emergencia, que actuarán en el evento de la desviación o sus consecuencias, sistemas de alivio de presión o descarga a la tea, sistemas de transferencia de materiales en emergencia,

sistemas de detección de escapes, sistemas de contraincendios fijos/automáticos, etc. Este paso es importante para ayudar al equipo a decidir si se requiere una recomendación para protecciones adicionales.

6. Decidir si se requiere una recomendación y acordar acción apropiada

Se justifica una recomendación si la probabilidad y/o las consecuencias de un evento son muy severas para aceptarlas sin acciones correctivas. Si los miembros del equipo no se sienten bien con el nivel actual de protección contemplada en el diseño, entonces se debe generar una recomendación para tomar acción posterior. El grado de solución de problemas que tiene lugar durante el estudio variará. Esto puede oscilar desde un estudio en el cual no se exploran soluciones, los resultados simplemente se registran y se programan para estudio posterior, hasta uno en el cual un equipo identifica una solución detallada antes de proceder con los siguientes aspectos.

MODO DE TRABAJO

Se suministrará, como documento de referencia para el HazOp, los planos de tubería e instrumentos actualizados (P&IDs), los diagramas de flujo de la operación, los procedimientos de operación y mantenimiento de la planta, las hojas de especificaciones de instrumentos, válvulas de control y equipos principales (bombas, compresores, tanques, intercambiadores de calor, hornos, calderas, reactores, torres, etc.)

El grupo que practicará el análisis HazOp deberá conformarlo la empresa, de entre su personal técnico de ingeniería, mantenimiento, operaciones y seguridad industrial.

El secretario de las sesiones de HazOp deberá ser apartado de entre los funcionarios que aporte para la elaboración del estudio HazOp.

*Luis Carlos Osorio Rivas
Consultor Consejo Colombiano de Seguridad
Mayo de 2007
Bogotá Colombia*



Un Regalo de Vida
**Herramienta de
Rescate**
RESQME



2 EN 1

**CORTA-CINTURONES
ROMPE - CRISTALES**

20,00 USD

Salva Vidas en caso de choque o volcadura

INFORMES Y VENTAS

<http://www.ipc.org.ec/cursos/conduccion.htm>

Info@ipc.org.ec

**Tef: (+593 2) 2923 600 | 601 ext. 124
Quito - Ecuador**

IMPORTANCIA DE LA PRESENCIA DEL OFICIAL DE PROTECCIÓN

El Oficial de Protección, es un elemento crucial dentro del plan de protección integral.

Las funciones del Oficial deben relacionarse con todos los otros elementos del plan; pero muchas organizaciones enfocan erróneamente su problema, y asumen que sus empresas pueden ser protegidas adecuadamente mediante el uso de un solo guardia, a menudo descubren que esto por sí solo no puede resolver sus problemas.

Es cierto que los servicios de un oficial de Protección son costosos. En EE.UU. en el 2000, la media de ingresos anuales totales para los guardias de seguridad fue de \$ 17,570. El cincuenta por ciento ganaba entre \$ 14,930 y \$ 21,950, 10

por ciento ganaba menos de \$ 12,860 y el 10 por ciento obtuvo más de \$ 28,660. Media anual de ingresos de los oficiales de seguridad en los hospitales fueron de \$ 22260; los que están en las escuelas primarias y secundarias recibieron \$ 22,240 dólares, mientras que los oficiales de seguridad empleados en diversos servicios a las empresas tenían una media de ingresos anuales de \$ 16,830.

Los costos de protección también se incrementan regularmente en proporción directa al tiempo de trabajo ejecutado. Incluso con el gasto adicional, los oficiales de

seguridad son necesarios y sus costos están justificados en muchos aspectos dentro del Programa de Protección. Sin embargo, el costo dictado para el puesto de oficial de Protección debe ser periódicamente evaluado, así como otras técnicas de Protección – tales como sistemas hardware y electrónicos-.

En Ecuador, el Mandato 8, de la Asamblea Constituyente, establece los límites a los servicios complementarios y las disposiciones relacionadas a las empresas de vigilancia y seguridad privada que ahora serán vigiladas por sus clientes en el pago de remuneraciones establecidas en el Código de Trabajo y demás leyes laborales. El nuevo reglamento a la ley de Vigilancia y Seguridad Privada sugiere cambios en la estabilidad laboral de los custodios, mejoras de sus salarios, contratación de seguros de vida y otro tipo de atenciones.

RELACIONES PÚBLICAS

El oficial de Protección tiene un rol definido de Relaciones Públicas al ejecutar sus funciones de protección, pues es el primer (y final) contacto que tiene el visitante, cliente, vendedor o



empleado con la organización. Y la manera en la que él se desenvuelva con la gente marcará de manera positiva o negativa su primera impresión. Por tanto es importante la cortesía y la eficiencia en las labores del Oficial de Protección para mantener buenas relaciones entre la Organización y otras compañías.

Establecer relaciones sociales y profesionales apropiadas con los

empleados no siempre es fácil principalmente porque algunas personas adquieren posiciones antagónicas frente a posiciones de autoridad, sin embargo, oficiales bien entrenados que son corteses, actúan con moderación, y utilizan la técnica y el sentido común puede superar esa resistencia.



NÚMERO DE OFICIALES REQUERIDOS

El número de Oficiales requeridos dentro de una instalación determinada debe considerar algunos factores:

1. La complejidad física de una instalación
2. El número de empleados
3. El carácter de la labor realizada
4. El número de entradas, y las horas que están abiertas
5. El número de patrullas necesarias para proteger las instalaciones, y
6. El número de escoltas y tareas especiales que deben realizarse



PATRULLAJE

Los Oficiales de Protección observan una variedad infinita de gente y lugares y reportan una cantidad de información dirigida evidentemente a las autoridades. Esta información, cuando es debidamente recolectada y analizada proporciona un invaluable apoyo a la operación del Programa de Protección Integral de la Empresa. Los daños son reportados y las deficiencias en el programa de protección son destacadas para que puedan realizarse cambios en los procedimientos, personas y tecnología antes de que se generen pérdidas.

Los patrullajes se dividen en dos categorías: patrullaje a pie y vehicular, sin embargo, en ambas

CONTROL

La función fundamental del Oficial de Protección es el Control de Acceso, permitiendo el ingreso a las instalaciones a las personas autorizadas y manteniendo afuera a las no autorizadas. Las instrucciones básicas del Oficial de Protección, en materia de empleados y visitantes, son las siguientes:

1. Asegurarse que todos los empleados y visitantes lleven insignias visibles en todo momento dentro de la Instalación.
 2. Identificar a todos los visitantes con pases especiales.
 3. Identificar y denunciar a cualquier persona en la instalación sin la debida identificación.
 4. Informar de las personas que pretenden introducir bebidas alcohólicas u otro tipo de contrabando en la instalación, o que parecen estar bajo la influencia del alcohol o sustancias controladas.
 5. Identificar e interrogar a las personas que circulan por la propiedad para asegurarse de que tiene una propiedad pase o eliminación se autorice otra cosa para eliminar la propiedad.
- Un oficial de Protección debe verificar todos los vehículos, trenes, aviones y embarcaciones que entran y salen de la instalación. Un oficial debe acercarse lo suficiente al vehículo para inspeccionar a fondo y evitar que material o personas no autorizadas pasen por el punto de acceso.

categorías, el Oficial debe patrullar un área asignada de manera aleatoria en orden y tiempo.

Es función del Oficial, conocer el área que patrulla, ser consciente de atajos, callejones sin salida, obras en construcción y cualquier otro factor que pueda afectar la respuesta. El conocimiento de las actividades legítimas y los peligros en la zona son también un requisito. Recuerde que la observación es la primera labor del Oficial, por lo que debe ser cuidadoso en todos los aspectos del medio. Cuando algo no común ocurre, el Oficial debe evaluar la situación y tomar acciones idóneas de acuerdo a su entrenamiento. Particular cuidado debe tomarse cuando se monitoree a individuos.



Entre los elementos más comunes que un Oficial de Protección debe verificar en un patrullaje son:

- Puertas, ventanas u otras áreas abiertas no seguras
- Personas con actitudes sospechosas o vehículos o circunstancias similares
- Actividades inusuales o desordenadas –cualquier individuo influenciado por el alcohol u otra sustancia, grupos inusuales de personas, personas desordenadas o querellas.
- Condiciones peligrosas-como fugas de agua u otro líquido, riesgos de incendios y mal funcionamiento de los equipos



ESCOLTA

Visitantes y clientes no deben ser escoltados por el Personal de seguridad mientras estén en las instalaciones de la compañía puesto que esta función obliga a los oficiales a mantenerse fuera de sus tareas de protección y la debilita.

En las únicas ocasiones que a los Oficiales se les requiere como escoltas, es para proteger a personas con grandes cantidades de dinero, propiedad clasificada de una compañía o Gobiernos o cuando se requiera la protección para un empleado.

ASIGNACIONES ESPECIALES

Las tareas de inspección y auditorías pueden desarrollarse en conjunto con otras asignaciones, en el patrullaje. Cuando se habla de inspección, nos referimos

a inspecciones de peligro de incendios, puertas no aseguradas, entre otros. Algunas Organizaciones también añaden entre las funciones del Oficial inspecciones de Seguridad (Safety)

En muchas instalaciones, las fuerzas de protección está en servicio las veinticuatro horas del día y los oficiales pueden ser el único personal disponible para asignaciones especiales. Tales asignaciones incluyen mensajería, coordinación de comunicaciones o conductores, o realizar otras funciones no relacionadas a sus labores de protección. Sin embargo, debemos hacer énfasis en que la desviación de tareas para realizar diversos servicios ajenos a sus labores, erosiona el programa de protección en las instalaciones.

Fuente:

Protection of Assets Manual, ASIS Internacional, Chapter 9, pag. 9-2 a 9-7



FUNDACIÓN CONCEPTOS INTEGRADOS DE PROTECCIÓN -IPC-

Con el respaldo internacional de International Foundation for Protection Officers -IFPO-, Ministerio de Educación, Comité Interinstitucional de Seguridad e higiene en el trabajo -CISHIT y Consejo Nacional de Capacitación y Formación Profesional -CNCF-

**LE INVITA A OBTENER
LA**

**Certificación en Supervisión y
Gerencia de Protección -CSSM-**

**INICIO
27 DE OCTUBRE**

**LUGAR
Quito
Guayaquil
Manta**

**Su Certificación Internacional le
otorga reconocimiento a nivel
mundial**

Problemas de Protección de las Tarjetas Inteligentes

Básicamente una Tarjeta Inteligente es una tarjeta plástica del tamaño de una tarjeta de crédito convencional, que contiene un pequeño microprocesador, que es capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a través de mecanismos avanzados de seguridad.

Las dos aplicaciones fundamentales de las tarjetas inteligentes son:

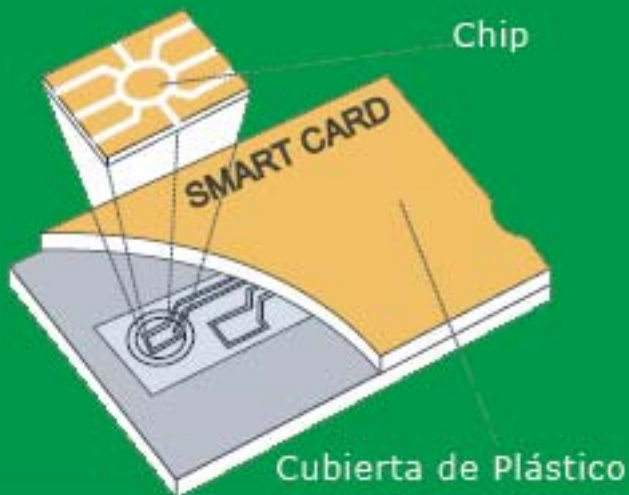
- Identificación del titular de la misma.
- Pago electrónico de bienes o servicios mediante dinero virtual.
- Almacenamiento seguro de información asociada al titular.

Las aplicaciones de las tarjetas inteligentes incluyen su uso como tarjeta de crédito, SIM para telefonía móvil, tarjetas de autorización para televisión por pago, identificación de alta seguridad, tarjetas de control de acceso y como tarjetas de pago del transporte público.



40% de los ingresos de mafias proceden de violaciones de la seguridad electrónica de las tarjetas inteligentes

CAPACIDADES



Una Tarjeta inteligente es un mecanismo muy seguro para el almacenamiento de información financiera o transaccional, la tarjeta inteligente es un lugar seguro para almacenar información como claves privadas, número de cuenta, contraseña o información personal muy valiosa, esta capacidad se debe:

1. Encriptación.
2. Clave segura (PIN).
3. Clave secundaria de seguridad.
5. Firmas digitales.
6. Alta seguridad en el acceso físico a: recintos, laboratorios, controles, salas informáticas.
7. A través de sistemas biométricos, huella dactilar y retina.

- **Capacidad de Almacenaje:** Es capaz de almacenar cualquier tipo de información, además es autónoma en la toma de decisiones al momento de realizar transacciones.

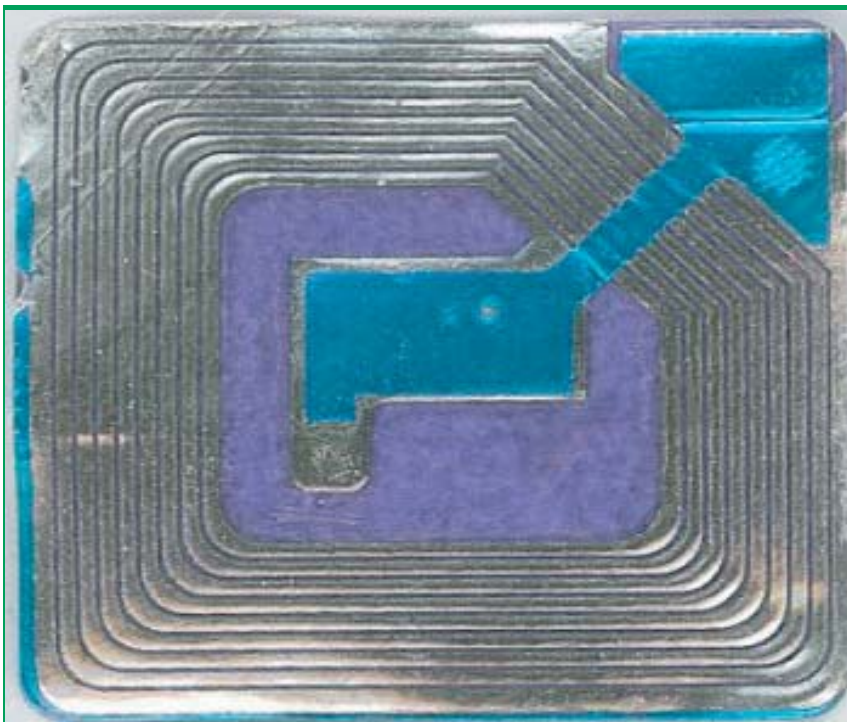
- **Utiliza clave de acceso o PIN:** Para poder utilizarse es necesario digitar un número de identificación personal, es posible además incorporar tecnología más avanzada como identificación por técnica biométrica, huella digital o lectura de retina.

- **Actualización de cupos:** Después de agotado el cupo total de la tarjeta inteligente es posible volver a cargar un nuevo cupo.

CARACTERÍSTICAS



ZONAS



1. **Zona Abierta:** Contiene información que no es confidencial. (el nombre del portador y su dirección).

2. **Zona de Trabajo:** Contiene información confidencial. (Aplicaciones bancarias: cupo de crédito disponible, el número de transacciones permitidas en un periodo de tiempo).

3. **Zonas Secretas:** La información es totalmente confidencial. El contenido de estas zonas no es totalmente disponible para el portador de la tarjeta, ni tiene por que conocerla la entidad que la emite ni quien la fabrica.

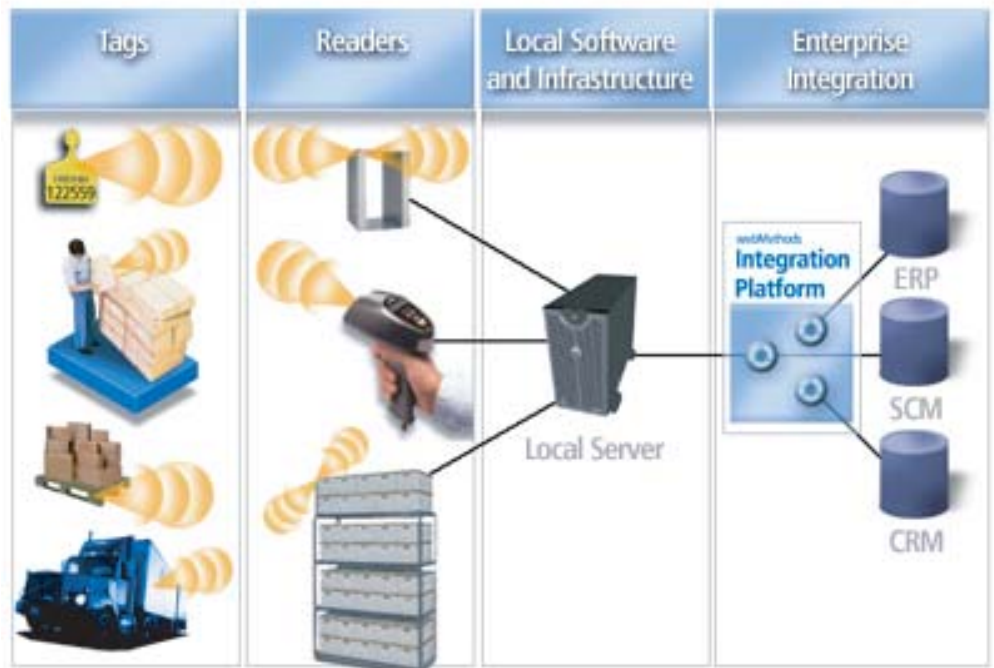
Es poco probable que estas zonas vean afectadas su seguridad, sin embargo, existe un riesgo latente. Se sabe que los sistemas de cifrado son muy seguros pero su implementación deja mucho que desear.

Por un lado, la criptografía ha avanzado notablemente; por otro, la seguridad de la información tiene muchos fallos.


Así, entre los dispositivos que dan problemas son las denominadas etiquetas inteligentes o RFID (radio frequency identification) que se encuentran en muchos productos comerciales, y es elemento fundamental de carnets electrónicos, tarjetas sanitarias, de crédito, de móvil y de transporte.

¿PERO CÓMO FUNCIONA LA RFID?

Las RFID se usan para controlar la posición de cualquier producto durante la cadena que va del fabricante al consumidor. Por ejemplo, pueden ser útiles para identificar fácilmente un "stock" de productos caducados o para evitar perder paquetes o cartas. Sin embargo, no pierden su función tras llegar a manos del comprador. Para captar la presencia de una tarjeta RFID en un radio de unos metros, solo hace falta una sencilla antena. Sin embargo, especialistas criptógrafos, alertan de los problemas de aplicaciones como esta.



El principal problema de interceptación es que el dueño no se entera de ella. Y, sobre todo, sin que pueda elegir ocultar la información. Las etiquetas inteligentes son muy pequeñas y delgadas, así que es difícil introducir en ellas un programa complejo de encriptación de datos que impida el acceso a las personas no autorizadas.



El otro dispositivo que presenta problemas de seguridad, según los investigadores, es la smartcard, la pequeña placa insertada en carnets y tarjetas de todo tipo, como DNI y pasaportes digitales. En los últimos 10 años la industria de las tarjetas inteligentes lucha contra una gran comunidad de falsificadores, se calcula que hay unos 750.000 individuos en todo el mundo que consiguen utilizar ilegalmente tarjetas de TV de pago. Asimismo, en el mercado negro de algunos países se puede comprar fácilmente un kit de clonación de tarjetas de móvil. Se trata de negocios importantes: las violaciones de la seguridad de la información ya representan el 40% de los ingresos de las mafias de todo el mundo, según un estudio del Departamento de Defensa de EEUU.

Las violaciones son graves, si afectan a información sensible, como documentos electrónicos; pero las tarjetas inteligentes son una mejora respecto a las bandas magnéticas porque reconocen que la máquina que las lee es falsa.

Por tanto, no debemos olvidar que algunas tarjetas son más susceptibles a los ataques que otras. Hay una serie de medidas de seguridad perfectamente conocidas que pueden añadirse a los microprocesadores de las tarjetas "chip" o a las aplicaciones, pero no siempre son utilizadas o activadas. Los "chips" que han sido utilizados tradicionalmente en las tarjetas inteligentes fueron diseñados en su origen como microcontroladores incrustados y además son utilizados en una amplia variedad de aplicaciones donde la seguridad no es un problema.



De hecho, la seguridad puede ser innecesaria en estas otras aplicaciones, porque fueron diseñadas para entornos de alta fiabilidad. Esto quiere decir que si algo va mal, el "chip" tratará de solventar el problema y continuará "haciendo lo que ha sido diseñado para hacer". Pero en una tarjeta inteligente, ese problema puede ser un signo de que un "hacker" está intentando obtener información confidencial de la tarjeta. Lo que



necesitamos de ese "chip" es que "falle" limpiamente con un "reset" o un bloqueo total, dependiendo del tipo y la gravedad del ataque.*

*"Este contenido se incluye con permiso del Criptonomicón. Copyright © 1997-2000 Gonzalo Álvarez, CSIC. Todos los derechos reservados."

Fuente:

Seguridad en Tarjetas con Microprocesador: Procedimientos de Evaluación y Consecución de Estándares, Ginel Francisco, 2000
http://www.elperiodico.com/default.asp?idpublicacio_PK=46&idioma=CAS&idnoticia_PK=412197&idseccio_PK=1021&h=
<http://www.monografias.com/trabajos10/tarin/tarin.shtml>

Uso de celulares para el lavado de dinero

En Ecuador, el Registro Oficial Nro. 127, del día martes 18 de Octubre del 2005, se publicó la Ley para reprimir el lavado de activos; ésta tiene veinticinco artículos, cuatro disposiciones generales, cuatro transitorias y dos reformatorias y derogatorias a otros cuerpos legales.

El lavado de dinero teóricamente tiene por finalidad ocultar su origen ilícito, introduciéndolo en los procesos productivos lícitos o mezclándolo en la circulación regular de capitales

El lavado de activos sin duda alguna tendrá su origen en el dinero, bienes, efectos o ganancias que provienen de los delitos de tráfico ilícito de drogas, delitos contra la administración pública, secuestro, proxenetismo, tráfico de menores, defraudación tributaria, delitos aduaneros u otros que generan ganancias ilegales.

El delito lo cometen los usuarios de los servicios bancarios, que por este medio, invierten en acciones de compañías, en adquisiciones de propiedades, automóviles, yates, aviones, colecciones de arte plástico y escultórico, o giren el dinero depositado en las cuentas hacia otras personas, etc.

Frente al cerco legal que las autoridades han formulado para controlar este delito, las organizaciones delictivas han encontrado otros mecanismos que les permita lavar dinero, así el uso de sistemas electrónicos y otras tecnologías han sido empleadas por el anonimato que ofrecen y la escasa regulación. Entre la amplia gama de opciones que tienen los delincuentes para limpiar el "dinero sucio" destacan las tarjetas de pre-pago, los mundos virtuales y teléfonos celulares.

Las transacciones mediante las tecnologías emergentes para cometer delitos son "realmente aterradoras", puesto que en los últimos años se ha generado una explosión de tecnología avanzada, se ha mejorado el servicio, así como se ha incrementado los sitios en Internet para realizar pagos electrónicos, por lo que este espacio es aprovechado por los



La modalidad individual se presenta en forma prepaga o con pago posterior. En el sistema de pago posterior, el operador telefónico autoriza al dueño del teléfono a cargar pagos en su cuenta telefónica. En el sistema prepago, el operador telefónico autoriza al dueño del teléfono a depositar fondos en una "cuenta" (ésta no es una cuenta bancaria) que tiene el operador a estos fines. En la opción individual, las compañías telefónicas que prestan el servicio posiblemente no sean supervisadas por los reguladores antilavado de dinero (ALD) del país.

"lavadores de dinero", en especial porque de esa misma forma se observa un crecimiento del número de entidades que no están bien reglamentadas.

Conocemos que los riesgos para el lavado de dinero con estos sistemas consisten en que hay "más capas entre las instituciones y el cliente"; son más fáciles "que nunca" las transacciones a través de las fronteras; hay una limitada información y al existir múltiples negocios involucrados es un reto para la supervisión de las actividades financieras.

Sin embargo, un riesgo superior generan los pagos a través de los teléfonos celulares, principalmente porque con este sistema se transfieren cantidades de dinero pequeñas de manera anónima, sin regulación y con mayor frecuencia. Este sistema, se vuelve cada vez más popular, principalmente porque al utilizar los celulares el usuario puede borrar la transacción y al no existir un registro del sitio de la transferencia es más difícil detectarla.

¿CÓMO FUNCIONA ESTE SISTEMA DE LAVADO?

El lavador de dinero puede abusar del sistema móvil de pago de esta forma: compra una tarjeta prepaga y la carga con dinero mal habido. Luego se registra en línea con un proveedor de pago móvil, utilizando una cuenta de correo electrónico anónima y gratuita, el número de teléfono móvil prepago y el dinero en una tarjeta de valor acumulado. Por supuesto, dan un número de identificación falso y un domicilio falso.

Al usar el teléfono móvil, el lavador luego se conecta en el sitio de Internet del proveedor de servicios de pago e ingresa el número de teléfono celular al cual desea transferir los fondos de la tarjeta prepagada. La compañía telefónica envía un mensaje al número de teléfono del receptor en el cual le pregunta adónde desea enviar el dinero.

Si tiene cuentas en el banco, el receptor puede solicitar que la transferencia sea hecha a su tarjeta de valor acumulado. Eso ahora le permitiría extraer los fondos en cualquier cajero automático, en cualquier lugar. La transacción no dejaría muchos rastros que pudieran ser auditados: dos números de teléfonos celulares, el monto de la transacción, unas breves instrucciones sobre la transmisión de los fondos y la recepción del dinero.

Esto crea una situación en la que existen mínimos rastros y donde hay anonimato, combinado con que funciona de manera similar a una tarjeta de débito o crédito o a un servicio de remesa. Y todo ello está virtualmente sin regular.



MITIGANDO EL RIESGO

Montos. Es más probable que exista lavado de dinero y fraude cuando los montos de las transacciones y de carga de la tarjeta son altos. Cuando los teléfonos celulares son solo dispositivos de acceso a cuentas bancarias o de tarjetas de crédito subyacentes, esas restricciones pueden no ser necesarias. Si los pagos móviles no están vinculadas con cuentas bancarias subyacentes, el proveedor telefónico a menudo fija un monto máximo por transacción diaria - tal vez unos pocos cientos de dólares o euros - lo que limita la vulnerabilidad al lavado de dinero.

Identificación. Si el servicio de



teléfono celular y los fondos utilizados para facilitar el pago móvil son prepagos, el proveedor del servicio puede no estar motivado para identificar totalmente a los clientes, porque él no tiene riesgo de crédito y no se ve obligado a cumplir obligaciones legales. Aún así, sería prudente identificar al cliente y verificar la información brindada en el proceso de inscripción. De lo contrario, el proveedor telefónico no tiene forma de saber si la información recibida es real o si fue robada a otra persona.

Método de fondeo. Los pagos móviles realizados de una cuenta prepagada pueden recibir los fondos de una cuenta bancaria o de una tarjeta de débito/crédito prepagada. Las fuentes de pago que verificaron en forma independiente la identidad del propietario del teléfono y que mantienen un registro de los fondos transferidos a la cuenta móvil presentan un riesgo bajo.

El uso de dinero en efectivo para fondear una cuenta de pago móvil, además de otros factores de riesgo, puede presentar algún peligro limitado de lavado de dinero y financiamiento del terrorismo. La restricción sobre las opciones de fondeo puede mitigar el riesgo.

Uso de límites. Generalmente, los pagos de transacciones en puntos de venta (point of sale, o POS) pueden ser aceptados solamente por los comerciantes participantes o por otros suscriptores del servicio. Los suscriptores también pueden extraer dinero a través de sus cuentas de pago móvil directamente de sus cuentas bancarias o como efectivo de los cajeros automáticos con una tarjeta prepagada. El monto máximo de la transacción y la escasa funcionalidad transfronteriza pueden ayudar a reducir el riesgo.

DETECTANDO AL LAVADOR DE TELÉFONO CELULAR

Las compañías telefónicas pueden no estar obligadas legalmente a hacerlo, pero sus políticas y procedimientos internos o sus acuerdos con bancos pueden obligar a reportar operaciones sospechosas. A fin de hacer esto, no sólo deben identificar al cliente, sino que también deben conservar registros de cada transacción (incluidos los micro pagos) a fin de identificar

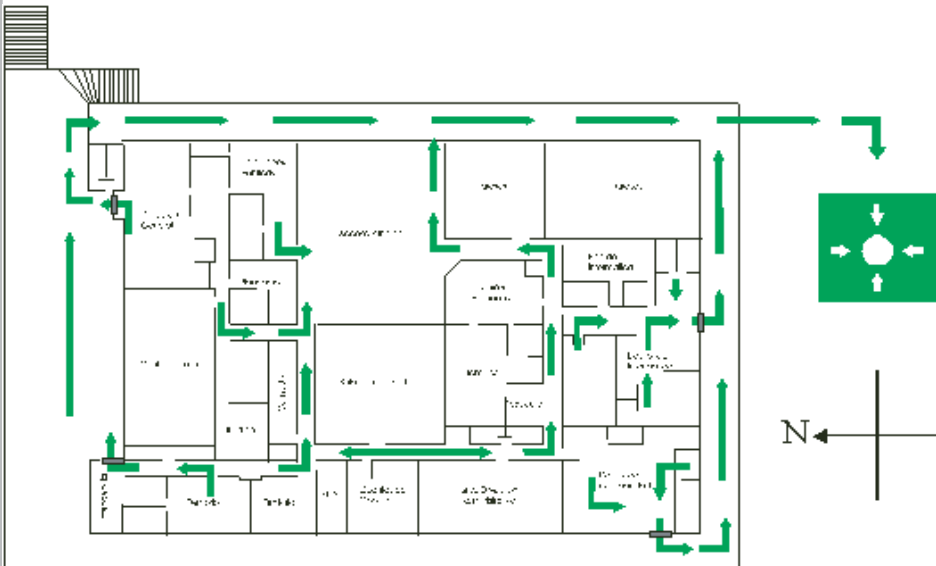


patrones de transacciones y monitorear las transacciones sospechosas.

El riesgo es la probabilidad de que una amenaza determinada ataque a una vulnerabilidad determinada y cause un daño específico. La probabilidad de que los teléfonos móviles sean usados para cometer lavado de dinero no es tan grande si se toman las medidas precautorias adecuadas. Pero si una compañía telefónica aparece en el titular de un diario vinculada a un caso de lavado de dinero o financiamiento del terrorismo, el impacto puede ser tremendo y su reputación se puede ver dañada para siempre. Sólo con una administración de riesgo adecuada las compañías pueden aislar los riesgos e identificar las posibles opciones para mitigarlo y mantenerse alejadas de los problemas.

Fuente:

- *Lavando a través del teléfono celular: ¿Realidad o ficción?*, Rietbroek Saskia, julio 2008
- <http://www.diariocorreio.com.br/archivo/2006/03/27/lavado-de-ativos>
- <http://archivo.eluniverso.com/2006/09/03/0001/10/855236CAE55846A6912F47DF42D2C6ED.aspx>
- http://www.soitu.es/soitu/2008/03/19/info/1205882676_321012.html
- <http://elmetaverso.com/2008/03/18/mundos-virtuales-usados-para-lavado-de-dinero/>



Plan de Evacuación

Hoy en día, los planes de evacuación son cada vez más requeridos en caso de auditorías de seguridad de un edificio, negocio o empresa. Ante casos críticos, la elaboración anticipada de un plan de evacuación puede suponer la diferencia entre lamentar víctimas o, simplemente, afrontar pérdidas materiales.

Algo que parece muy simple y es tan complejo como un plan de evacuación o un plan de emergencia es una labor fundamental de la prevención. No debemos olvidar que el plan de emergencia debe definir la secuencia de acciones a desarrollar para el control inicial de las emergencias que puedan producirse. Se enunciarán los factores de riesgo más importantes que definen la situación de emergencia y que pueden precisar diferentes acciones

para su control. Como mínimo se tendrá en cuenta la gravedad de dicha situación y la disponibilidad de medios humanos.

El plan de evacuación hace parte de los planes de contingencia o respuesta y es, a su vez, una de las formas de intervenir los factores de riesgo.

La ocurrencia de un evento entra en operación con el plan de evacuación, que consiste en el conjunto de actividades y procedimientos tendientes a

conservar la vida y la integridad física de las personas, en el caso de verse amenazadas, mediante el desplazamiento a través y hasta lugares de menor riesgo.

Los simulacros de evacuación permiten poner en práctica un plan y una organización previstos por la comunidad o el personal empresarial o industrial, para evaluar su desarrollo y realizar los ajustes necesarios. Los simulacros deben efectuarse inicialmente por grupos, para luego involucrar a todos los miembros de la institución, industria o empresa. Es de vital importancia realizar simulacros de evacuación y revisar los botiquines y los equipos de detección, control y extinción de incendios, etc. periódicamente.

En función de su gravedad, las situaciones de emergencias se clasificarán, según las dificultades existentes para su control y sus posibles consecuencias, en:

- Conato de emergencia,
- Emergencia parcial, y
- Emergencia general

En función de las disponibilidades de medios humanos, los planes de actuación en emergencia podrán clasificarse en:

- Diurno,
- Nocturno,
- Festivo, y
- Vacacional

Las distintas emergencias requerirán la intervención de personas y medios para garantizar en todo momento la alerta, alarma, intervención y apoyo. En este sentido los equipos de emergencia constituyen el conjunto de personas especialmente entrenadas y organizadas para la prevención y actuación en accidentes dentro del ámbito del establecimiento.

Los esquemas se referirán de forma simple a las operaciones a realizar en las acciones de alerta, alarma, intervención y apoyo entre las Jefaturas y los Equipos de Emergencia.

Los sistemas de control e identificación permitirán conocer en todo momento quién se encuentra en cada zona, así como cuántos de los afectados ya están fuera de peligro o en los puntos de reunión planificados, esta información puede ser requerida por los agentes de la autoridad o los bomberos para proceder con un protocolo de emergencia u otro.

Todo el personal de las instalaciones debe conocer las rutas de evacuación, las mismas que se plasmarán en gráficos o esquemas, ubicadas en lugares estratégicos a la vista del personal; además, debe existir señalización de rutas y del punto de encuentro, con el fin de que los visitantes ocasionales las reconozcan.



PROCEDIMIENTO DURANTE UNA EVACUACIÓN

- No correr ni utilizar ascensores
- No devolverse por ningún motivo
- Dar predilección a discapacitados y personas con mayor exposición al riesgo
- Si hay humo, desplazarse agachados
- Al salir de recintos cerrados, cerrar las puertas sin seguro
- Verificar la lista de personal y personas de la institución en el punto de encuentro.



Es importante tener siempre en cuenta que el plan de evacuación depende el tipo de evento que pueda presentarse. Es así como en caso de una tormenta eléctrica, los estudiantes no deberán estar a campo abierto ni cerca de árboles ni de rejas metálicas, sino protegidos dentro de un salón. En caso de un sismo, primero deben protegerse en un sitio que consideren seguro y, una vez pasado el sismo, proceden a la evacuación. Si se trata de una granizada fuerte, no deben pasar por debajo de domos ni estar cerca de vidrios ni de marquesinas o techos endebles que puedan ser averiados por el granizo y causar daño a los estudiantes; en este caso deben protegerse debajo de un techo de plancha de concreto.

EL PLAN DE EVACUACIÓN DEBE:

- Asignar responsabilidades a individuos u organizaciones para llevar a cabo acciones específicas en un tiempo y lugar determinado durante un evento adverso.
- Establecer líneas de autoridad, de relaciones y coordinación
- Identificar personal, equipamiento, instalaciones, insumos, etc., para las operaciones de respuesta.
- Identificar los pasos de mitigación a tener en cuenta durante las actividades de respuesta y



ACTIVIDADES PREVIAS AL SIMULACRO DE EVACUACIÓN

Una vez conformado los Comités Internos de Protección , estos deben realizar las siguientes tareas:

- Establecer el punto de reunión en el exterior del edificio.
- Difundir el plan de emergencia a los brigadistas.
- Implementar y probar el sistema de alarma interna.
- Entregar silbatos a los jefes de piso y brigadistas.
- Entregar equipo a brigadistas (gafetes, brazaletes, chalecos, etc.)



- Designar funciones a:
 - Guías y retaguardias.
 - Brigadistas de control de tránsito vehicular.
 - Brigadistas de control de accesos y resguardo del edificio.
 - Observadores.
 - Brigadistas que realizarán censo del personal.
 - Personal que tome el tiempo oficial de evacuación.

Fuente:

<http://www.desastres.org/articulos.php?id=03032008-01>

<http://sire.gov.co>





4 PASOS

FUNDAMENTALES

PARA SALVAR

UNA VIDA

Primera Parte

Por Raúl Subía, CPO

Cuando una persona deja de respirar, sus órganos no reciben oxígeno. La falta de oxígeno puede provocar serias lesiones neurológicas y hasta desembocar en la muerte de la persona.

Ante una situación de estas características es

importante actuar con rapidez. La técnica de resucitación cardiopulmonar (RCP) tiene como objetivo mantener el cerebro con vida y el corazón con actividad cardíaca. Es importante aprender a realizar esta maniobra y ejercitarla para no olvidar ninguno de sus pasos. Su correcta aplicación ha salvado innumerables vidas.

En esta edición le presentamos dos (2) de los cuatro pasos que debe realizar par salvar la vida de una persona:

1. Despejar la entrada de aire; restaurar la respiración y los latidos del corazón (según sea necesario)

2. Detener la hemorragia.

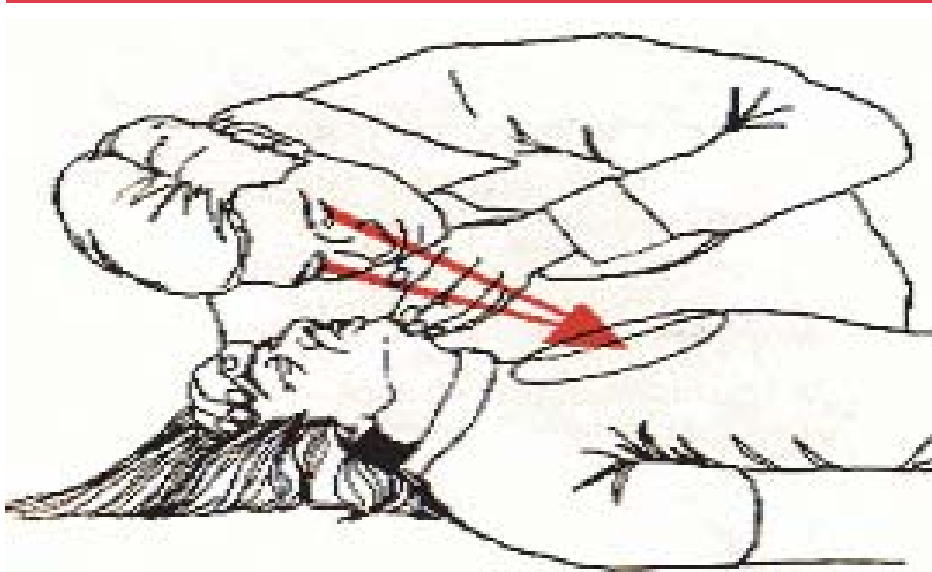
3. Administrar tratamiento para postergaciones nerviosas (shock)

4. Aplicar correctamente apósitos y vendajes.

PRIMER PASO "Despejar la Entrada de Aire"

- Virar la cabeza del herido hacia un lado, pasar rápidamente los dedos, por atrás de los dientes inferiores a fin de eliminar mucosidades u objetos extraños.
- Retirar del herido, toda prótesis como dentadura postiza, parcial o total.
- Chequear la posición de la lengua.
- La maniobra antes indicada no debe demorar más de 4 ó 5 segundos.
- En ausencia de signos vitales, coloque su mano o su oreja cerca a la boca o nariz del herido.
- El dar respiración artificial a un herido no le afecta en nada.

- Déle respiración de 10- 20 veces/min.
- Existen dos métodos básicos: método de boca a boca ó de boca a nariz.
- Mire la elevación del pecho.



Respiración

A medida que una persona envejece la frecuencia respiratoria tiende a disminuir por la edad. Las cifras normales son:

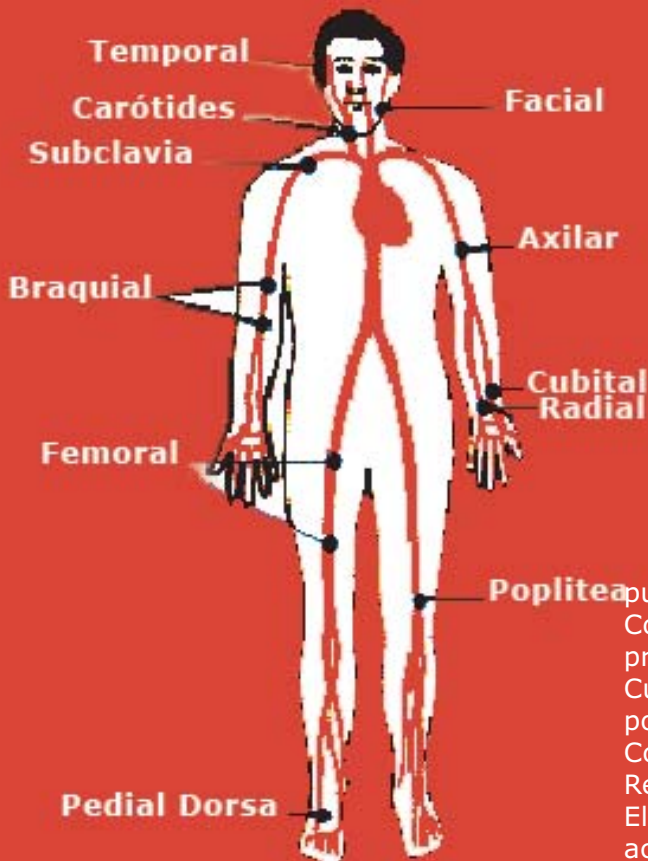
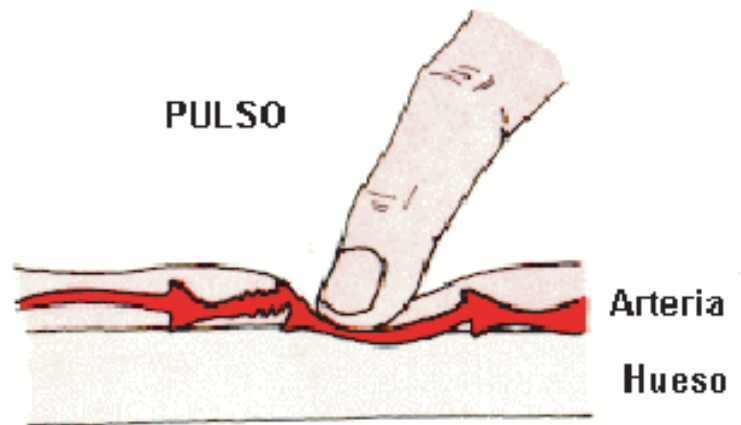
- Niños lactantes 40 a 60 respiraciones por minuto
- Niños hasta ocho años 20 a 40 respiraciones por minuto
- Adultos 16 a 20 respiraciones por minuto
- Ancianos menos de 16 respiraciones por minuto

PULSO

El pulso normal varía de acuerdo a diferentes factores; siendo el más importante la edad.

- Niños lactantes 90 a 190 pulsaciones por minuto
- Niños 85 a 140 pulsaciones por minuto
- Adultos 60 a 80 pulsaciones por minuto
- Ancianos 60 o menos pulsaciones por minuto

El pulso se puede tomar en cualquier arteria superficial que se pueda apretarse contra un hueso.



SITIOS DONDE SE TOMAR EL PULSO

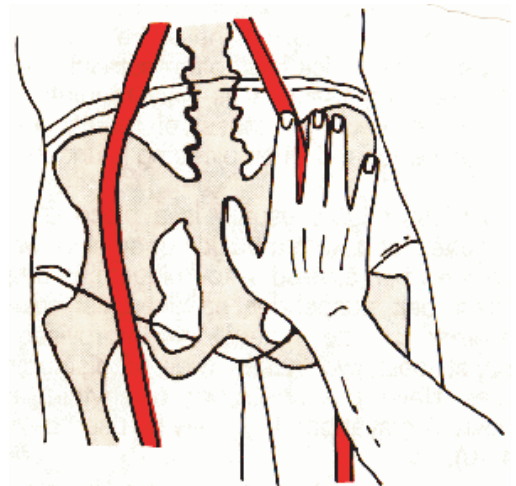
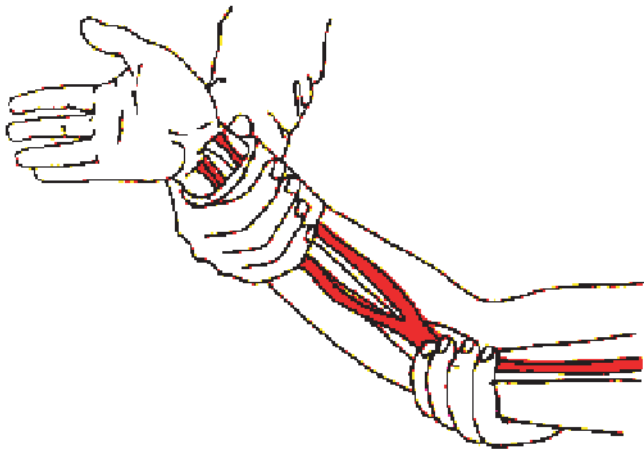
- En la sien (temporal)
 - En el cuello (carótida)
 - Parte interna del brazo (humeral)
 - En la muñeca (radial)
 - Parte interna del pliegue del codo (cubital)
 - Palpe la arteria con sus dedos índice, medio y anular. no palpe con su dedo pulgar. El pulso de este dedo es más perceptible y confunde el suyo. Palpe la arteria radial, que está localizada en la muñeca, inmediatamente arriba en la base del dedo pulgar.
- Coloque sus dedos (índice, medio y anular) haciendo ligera presión sobre la arteria.
 Cunte el pulso en un minuto. no ejerza presión excesiva, porque no se percibe adecuadamente
 Controle el pulso en un minuto en un reloj de segundero.
 Registre las cifras para verificar los cambios.
 El pulso radial es de mayor acceso, pero a veces en caso de accidente se hace imperceptible

SEGUNDO PASO: Detener la Hemorragia

- Determine si existe más de una herida.
- Cualquier objeto que atraviese el cuerpo, producirá una abertura mayor en la salida.
- Corte la ropa que sea posible y/o quítela de la herida.
- No toque las heridas ni trate de limpiarlas.
- Cubra la herida con apósitos y aplique presión sobre ella.
- Debe apretarse fuerte por un tiempo de 5 ó 10 minutos
- El objeto es formar un coágulo capaz de detener la hemorragia.
- Si carece de apósitos, use la tela más limpia disponible.
- En emergencias, la rapidez es más importante que la limpieza.
- Una hemorragia puede reducirse, elevando sobre el nivel del corazón los miembros afectados, siempre que no esté fracturado.

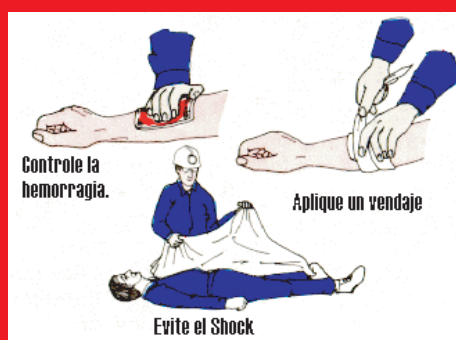
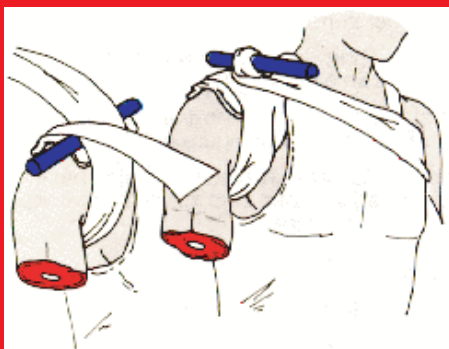
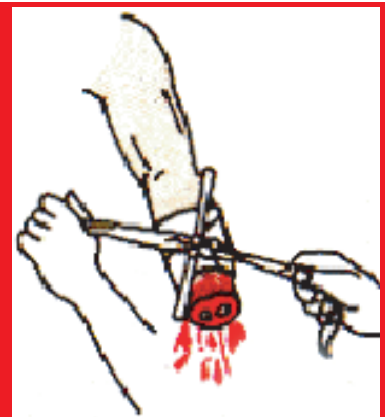


Arterial	Venosa	Capilar
Salida intermitente. Sangre rojo Brillante.	Salida Continua. Sangre rojo Oscuro.	Salida de sangre en poca cantidad.



USO DEL TORNIQUETE

- Un torniquete solo debe ser usado como último recurso.
- Se lo usa cuando un apósito con presión no es suficiente para detener hemorragia.
- Se lo usa cuando un miembro queda amputado, aplastado o destrozado.
- Debe ser colocado entre la herida y el tronco.
- Nunca lo coloque sobre la herida.
- Nunca aplique sobre una fractura.
- Cualquier material flexible es bueno para usarlo como torniquete



Perfil del Escolta: Presencia, Capacidad, Entrenamiento

No debemos olvidar que son funciones de los escoltas, con carácter exclusivo y excluyente, el acompañamiento, defensa y protección de personas determinadas, impidiendo que sean objeto de agresiones o actos delictivos.



Es misión fundamental de un escolta, realizar actividades de reconocimiento en avanzada a los movimientos del ejecutivo y Protector, así como, estar en condiciones de brindar apoyo y reacción inmediata al vehículo del Protegido, con el objetivo de mantener la integridad física de la persona que protegen.

- Dentro de las condiciones para cumplir las funciones de escolta se encuentra:
- Haber calificado en las pruebas de conducción,
- Comunicaciones,
- Defensa personal y
- Manejo de armas

FORMACIÓN DE LOS ESCOLTAS

La formación de los escoltas corre a cargo de las empresas de seguridad, así como también de centros privados, en ambos casos los requisitos son los mismos:

Área Jurídica Área Técnico-Profesional

Al igual que las empresas de seguridad, los centros de capacitación que se dediquen a la enseñanza y formación de Oficiales de Protección, Protectores y Escoltas deben estar



debidamente registrados.

El Artículo 8, de la Ley de Vigilancia y Seguridad Privada del Ecuador establece que el pènsium de estudios y carga horaria para el personal operativo, ... tendrán una duración mínima de 120 horas, distribuido en un tiempo no menor a dos meses. Incluirá temas de vigilancia, seguridad, relaciones humanas, defensa personal, primeros auxilios, manejo de armas, tiro; Ley y Reglamento de Fabricación, Importación, Comercialización y Tenencia de Armas, Municiones, Explosivos y Accesorios; Ley y Reglamento de Vigilancia y Seguridad Privada, leyes laborales, procedimientos de seguridad privada, entre los principales temas. En general, se deberá brindar capacitación de conformidad con las necesidades de la empresa y al tipo de servicio que presten sus clientes.

RESPONSABILIDADES DE LOS ESCOLTAS

1. Portar sus armas solamente cuando se encuentren en el ejercicio de sus funciones, debiendo depositarlas, a la finalización de cada servicio, en el rastrillo de la empresa. Portarán armas con discreción y sin ostentación de ellas, pudiendo usarlas solamente en caso de verse atentada la vida, integridad física o libertad, y atendiendo a criterios Uso de la Fuerza.

2. Portar siempre los documentos en regla (Licencia de conducción, tarjeta de la empresa, cédula, libreta militar)

3. Recibir y entregar la moto físicamente con los estados del mismo, asegurarse que este en perfecto estado de funcionamiento.

Cumplir los procedimientos seguros para el manejo de armas.

4. Estar en contacto con el centro de operaciones, antes y después de cada movimiento, durante desplazamientos o en operativos, reportarse en los puntos de control establecidos.

Utilizar todos los medios y equipos asignados al puesto, esto incluye manos libres, EPP, armamento, comunicaciones.

5. Conocer los planes de emergencia de las diferentes instalaciones a las cuales el ejecutivo asiste. Estar siempre en el área asignada, bajo ninguna circunstancia abandonar o perder de vista al vehículo donde está el protegido.

6. Realizar reportes diarios de actividades, reporte de rutas, situación de seguridad en la ciudad, e informar oportunamente cualquier indicio o amenaza que pueda afectar a las operaciones. Realizar un reconocimiento de las rutas principales del próximo movimiento con el ejecutivo. Tener totalmente identificados los lugares de alto riesgo y pedir información de los últimos incidentes de la ciudad y en los valles.

7. Mantener una velocidad segura, que le permita maniobrar, evadir o frenar, sin que esta acción

termine en accidente. Recordar los fundamentos de una conducción segura en moto.

8. Observar cómo está organizada la seguridad física y protección de la misma; si observa algún tipo de vulnerabilidad comunique inmediatamente al ERC, determinar y establecer salidas en caso de emergencia.

9. Verificar que el área asignada para periodos de stand by o espera en las residencias u otras, se encuentre limpia, ordenada y organizada de forma profesional.
Cumplir con las normas, políticas y procedimientos establecidos por la empresa de Seguridad Privada.

10. Por su parte las empresas de seguridad serán responsables de la conservación, mantenimiento y buen funcionamiento de las armas y los escoltas del cuidado y uso correcto de las que tuviera asignadas durante la prestación del servicio.

En resumen, el escolta debe cumplir con tres requisitos fundamentales:

PREVENIR

Evitar situaciones que lleguen a ser peligrosas:

Evitar lugares peligrosos

Lugares aislados

Muchedumbres

Lugares desconocidos

PROTEGER

El escolta debe estar dispuesto a efectuar la protección de su protegido con su propio cuerpo. En este caso el escolta debe poseer un alto grado de capacitación en Protección y grandes habilidades y destrezas en el manejo de motocicletas, además de liderazgo, trabajo en Equipo,



PLANIFICAR

La protección debe estar planificada desde el principio para saber si se quiere una protección a lo largo de toda la jornada o únicamente durante un período determinado.



CURSOS Y EVENTOS

CURSO	FECHA	LUGAR
Oficial Básico de Protección –BPSO-	Inicia Septiembre 19	Quito
Review para la Certificación –CPO- Oficial Certificado de Protección	Inicia Septiembre 27	Quito
Actualización legal en Seguridad Privada	Octubre 06 y 07	Quito
Review para la Certificación –CPO- Oficial Certificado de Protección	Inicia Octubre 02	Guayaquil Manta
Actualización legal en Seguridad Privada	Octubre 10 y 11	Manta
Actualización legal en Seguridad Privada	Octubre 15 y 16	Guayaquil
Inicio del Curso a Distancia para la obtención de la Certificación en Supervisión y Gerencia de Protección –CSSM-	Inicio Octubre 27	Quito Guayaquil Manta
Diplomado en Alta Dirección de Seguridad Corporativa 2008	Septiembre 22 al 26	Departamento de Estudios de Postgrado y Educación Continua de la Universidad de Belgrano. Lavalle 485, Buenos Aires, Argentina

FELICITAMOS A LA NUEVA PROMOCIÓN DE PROFESIONALES EN PROTECCIÓN INTEGRAL

Visite nuestra página Web y lea la lista Oficial de Profesionales Certificados CPO Y BPSO

www.ipc.org.ec/certificados/CPO

GRUPO DE PROFESIONALES CERTIFICADOS POR LA FUNDACIÓN IPC



GRUPO PROSEC INTERNACIONAL



INTERCOM

ANDESPETRO



BANCO CENTRAL

Y LA SEGUNDA EN OBTENER LA CERTIFICACIÓN INTERNACIONAL -BPSO- BASIC PROTECTION OFFICER



HOTEL QUITO



FUNDACIÓN IGLESIA DE LA COMPAÑÍA



POLICÍA METROPOLITAN DEL ILUSTRE MUNICIPIO DE QUITO



PROSEC
INTERNATIONAL

Hacemos del Mundo un lugar más Seguro

**ASESORÍA
Y CONSULTORIA
INTEGRALES EN
PROTECCIÓN Y
SEGURIDAD**

Análisis de riesgo Asesoramiento en Seguridad Auditorías

¡NO SE LANCE AL VACÍO!

**Especialistas del área le ayudarán
a orientar su negocio para que
sea más productivo**

CONTÁCTENOS

Av. Eloy Alfaro N35 144 y Portugal

Telf. (593 2) 2923 600 | 601 - Cel. 098104457

E-mail: info@ipc.org.ec