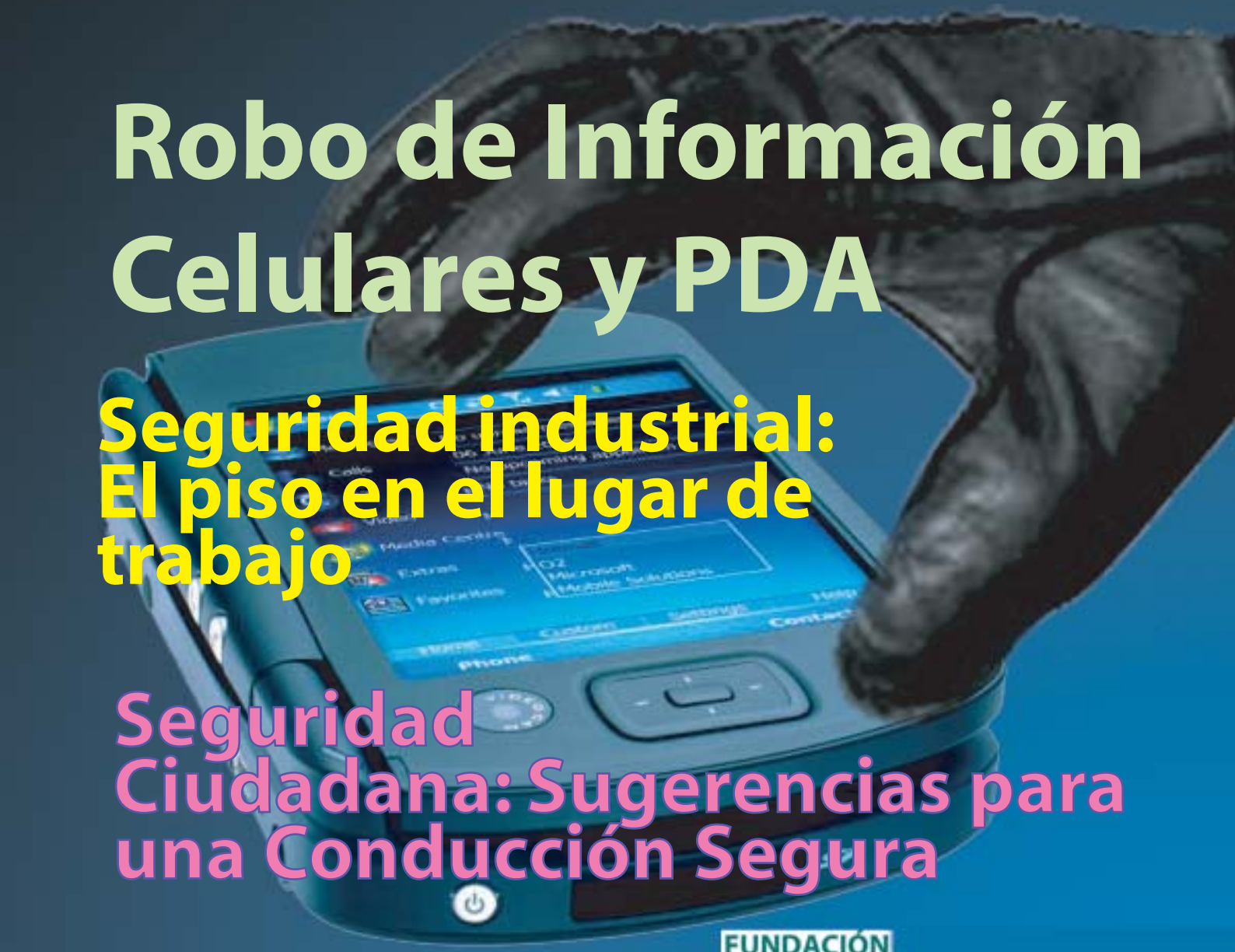
ARES

Revista Protección Integral

Año 1 Nº 6 Agosto 2008



Robo de Información Celulares y PDA

Seguridad industrial: El piso en el lugar de trabajo

Seguridad Ciudadana: Sugerencias para una Conducción Segura

FUNDACIÓN IPC Integrated protection concepts

Creando Cultura de Seguridad

FUNDACIÓN

IPC | Integrated protection concepts

Creando Cultura de Seguridad

¿SUS SERVICIOS DE SEGURIDAD AUMENTAN DE PRECIO PERO NO GENERAN VALOR?

No existe entendimiento entre las necesidades de protección física, seguridad industrial y sus objetivos de negocio?

Se ve obligado a cobrar más, pero su personal de seguridad física no genera valor agregado?

Debe justificar el nuevo precio, avalado por certificaciones profesionales.

LE INVITA AL SEMINARIO GRATUITO

"Como generar valor agregado a través del Personal Profesional de Protección"

Quito	**Septiembre 04**
Guayaquil	**Septiembre 09**
Manta	**Septiembre 10**

Confirme su cupo

(+593 2) 2923 600 | 601 ext. 122

E-mail: gaguirre@ipc.org.ec | www.ipc@org.ec

ministerio de educación ECUADOR

IFPO SUD AMERICA

CNCF Consejo Nacional de Capacitación y Formación Profesional

CISHT

Índice

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

EDITOR
Lic. María Fernanda Torres
e-mail: ftorres@ipc.org.ec

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

PRODUCTOS SECURITY

Gabriela Aguirre

e-mail: gaguirre@ipc.org.ec

PRODUCTOS SAFETY

Edwin Carrillo

e-mail: ecarrillo@ipc.org.ec

FUNDACIÓN IPC CONCEPTOS INTEGRADOS DE PROTECCIÓN

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

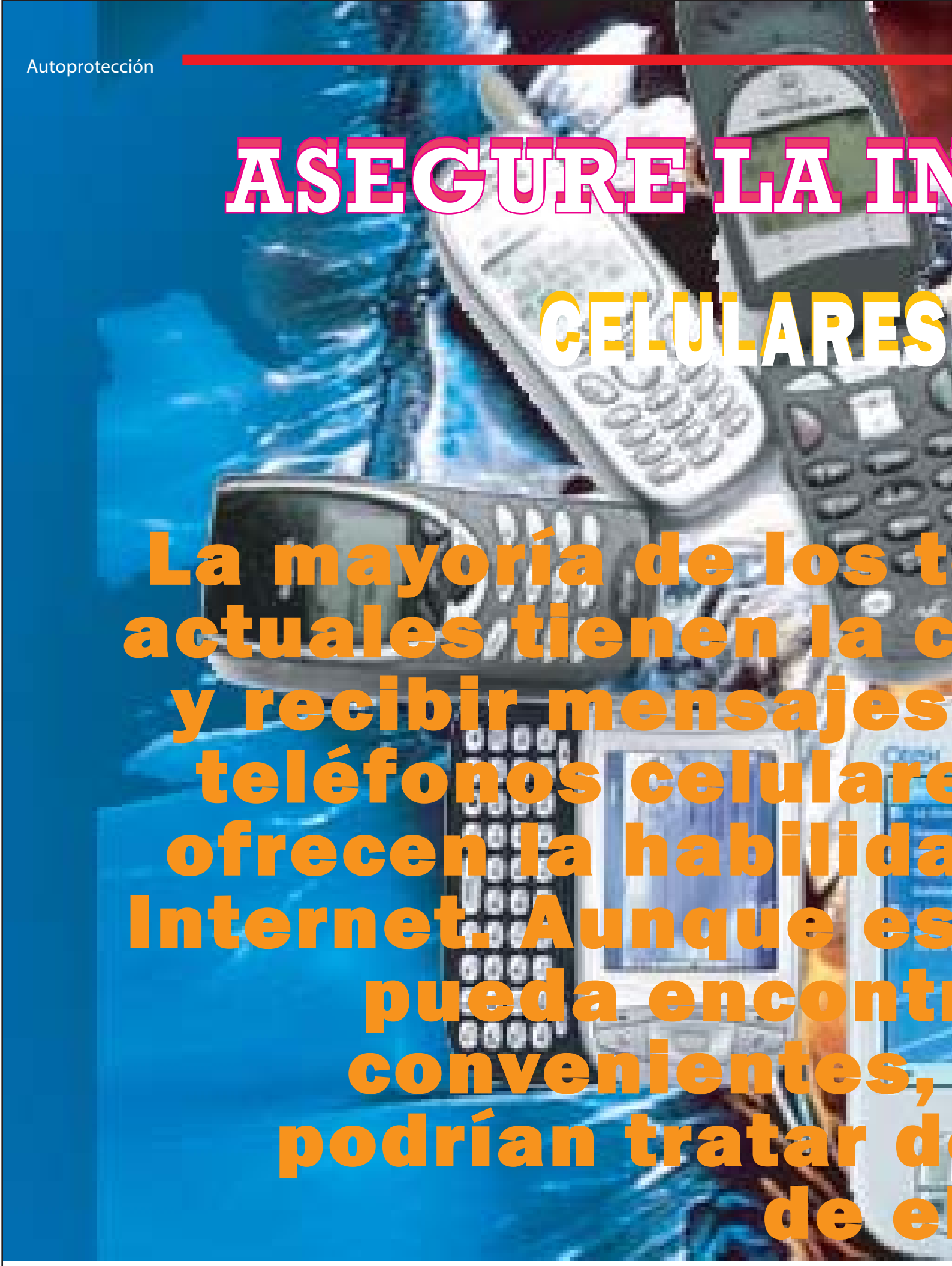
Tel: (593 9) 9 5417 322
Fax: (593 2) 2275 075
info@ipc.org.ec

www.ipc.org.ec

TIRAJE: 6500 suscriptores
12 países

Una organización del Grupo:

PROSEC INTERNATIONAL
Hacemos del Mundo un lugar más Seguro



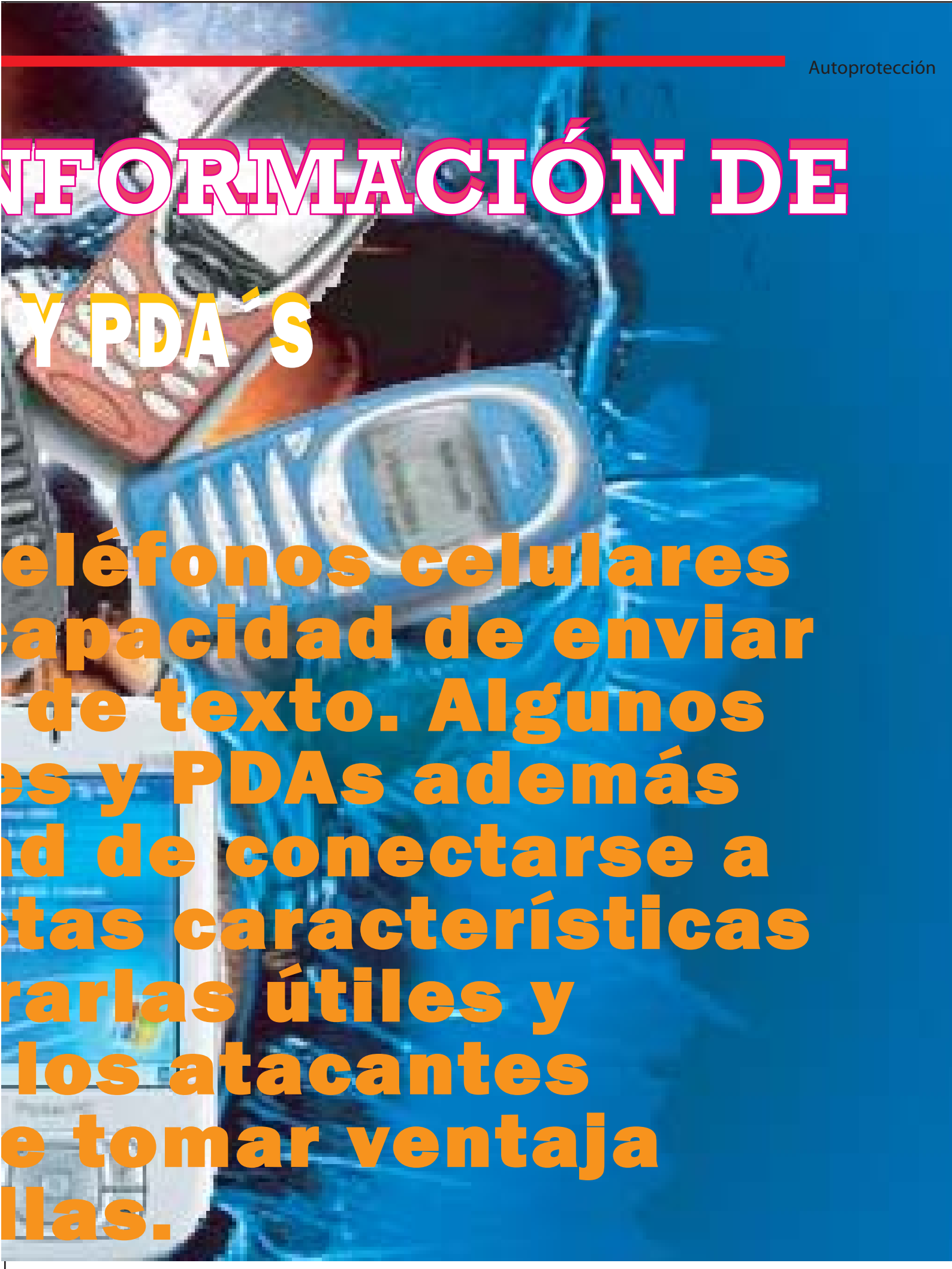
ASEGURE LA IN

CELULARES

La mayoría de los t
actuales tienen la c
y recibir mensajes
teléfonos celulare
ofrecen la habilida
Internet. Aunque es
pueda encont
convenientes,
podrían tratar d
de e

NFORMACIÓN DE

Y PDA´S



eléfonos celulares
apacidad de enviar
de texto. Algunos
es y PDAs además
id de conectarse a
tas características
rarlas útiles y
los atacantes
e tomar ventaja
llas.

De acuerdo a Eugenio Velásquez, Consultor de e-Business, Symantec existe un criterio generalizado de protección en el que si un usuario se conecta a la Internet, es más obvio que cuenta con una suite de seguridad (antivirus + firewall + antispyware) que vigila la conexión y protege de lo que pueda atacarle. Sin embargo, cuando navega desde un dispositivo celular o PDA, el control de protección desaparece. Se olvida que se está bajo el mismo riesgo a malware y ataques que cuando se lo hace desde una PC o Laptop. Como resultado, un atacante podría verse habilitado para conseguir lo siguiente:

Abusar de su servicio: La mayoría de los planes de teléfonos celulares limita el número de mensajes de texto que usted puede enviar y recibir. Si un atacante le envía un SPAM con mensajes de texto, sus gastos podrían verse aumentados. Un atacante además podría verse capacitado para infectar su teléfono o PDA con código malicioso que le permitiría usar su servicio. ***Como el contrato está a su nombre, usted será el responsable por el alza en su cuenta.***

Llevarlo hacia un sitio Web malicioso: Los atacantes están ahora enviando mensajes de texto a los teléfonos celulares. Estos mensajes, supuestamente de una compañía legítima, intentarán convencerlo de visitar un sitio malicioso diciéndole que existe un problema con su cuenta o estableciendo que usted se ha suscrito a un servicio. ***No entregue nunca información sensible.***

Usar su teléfono celular o PDA en un ataque: Los atacantes, que logran obtener el control de su servicio, podrían usar su teléfono celular o PDA para atacar a otros. Esto no solamente oculta la verdadera identidad del atacante, sino que permite al atacante aumentar el número de blancos.

Obtener acceso a la información de la cuenta: En algunas áreas, los teléfonos celulares son capaces de realizar ciertas transacciones. Si un atacante logra acceder a un teléfono que es usado para ese tipo de transacciones puede descubrir la información y usarla o venderla.

¿CÓMO PUEDO PROTEGERME?

Los siguientes consejos pueden serle de utilidad:

1. **Tome precauciones** para asegurar su teléfono celular y su PDA de la misma forma que usted asegura su computador.
2. **Cuídese** de publicar su número de teléfono celular y su dirección de correo electrónico.
3. **Sospeche** de URLs que sean enviadas en un mensaje de correo electrónico no deseado o en mensajes de texto.
4. **Sea cauteloso** de los programas que descarga. Hay muchos sitios que ofrecen juegos y otros programas que puede descargar a su teléfono celular o PDA.

Estos programas podrían incluir código malicioso.

5. **Evalúe** sus configuraciones de seguridad: Deshabilite Bluetooth cuando no lo esté usando para evitar acceso no autorizado.

OTRO TIPO DE CUIDADOS REFERENTES A SEGURIDAD FÍSICA

- Mantenga siempre a la vista su computadora portátil, PDA o celular, aún cuándo esté en la oficina. Guarde bajo llave y en un lugar seguro el celular y el PDA cuando no los esté usando.

- Mantenga su aparato portátil a la vista y a la mano cuando viaje. El robo de computadoras portátiles en los aeropuertos, trenes y restaurantes se ha convertido en una técnica muy popular de robo de información.

- De ser posible no guarde en éstos aparatos portátiles ninguna información confidencial de los clientes o empleados (como números de cuentas bancarias, códigos de cajeros automáticos, números de seguro social o información de tarjetas de crédito/débito)

- Si algún empleado (vendedor o vendedor de telemercadeo por ejemplo) requiere llevar en una computadora portátil, CD o memoria u otro aparato portátil, alguna información del cliente, del empleado u otros datos confidenciales fuera de las instalaciones de la empresa, insista y asegúrese de que la misma esté codificada o en clave.

- El código de acceso personal protege la entrada a la computadora portátil, a la agenda y al teléfono celular. Utilícelo también para proteger el acceso al Internet, correo electrónico, correo de voz y agendas.

- Apague los aparatos cuándo no se usen.

- No acepte ni baje información de fuentes o enlaces desconocidos.

- No comparta con nadie, sus aparatos portátiles de comunicación u organización.

- Copie periódicamente toda la información y guarde los discos y otros materiales de respaldo en un sitio cerrado que sea seguro

- Por ultimo, no dé por hecho que las computadoras portátiles son los únicos aparatos a los que se puede tener acceso. Los delincuentes también pueden infiltrarse en los teléfonos celulares y robar los archivos almacenados, contactos y correos de voz. De igual manera, los virus pueden dañar los teléfonos celulares. Los propietarios de los mismos deben preguntar en forma regular a sus proveedores sobre lo más novedoso en sistemas de seguridad para asegurarse que sus aparatos hayan sido configurados con la máxima seguridad.

CONCLUSIÓN

Es importante recordar que, como menciona Eugenio Velásquez, "todos los OS para móviles el de mayor riesgo y vulnerabilidad es Windows Mobile, al igual que su hermano mayor para PC, pero este tiene la ventaja de la gran compatibilidad que tiene con las múltiples herramientas de colaboración que trabajan sobre las plataformas de Exchange y SharePoint (que es lo que se usa en el ámbito corporativo y de negocios)"

Por tanto, pregúntese: ¿Para usted, qué es importante en su teléfono celular? ¿Realmente le importa qué sistema operativo lo haga funcionar?, ¿Es sensible a esto?; ¿es muy importante la colaboración que me ofrece Windows Mobile, y en ello llevo el coste de los riesgos de usarlo actualmente, al ser el más vulnerable de todos -aunque me protejo tanto como puedo-?

Fuente:

- Eugenio Velazquez, Consultor e-Business, Symantec, http://jevc.spaces.live.com

- Mindi McDowell, "Defending Cell Phones and PDAs Against Attack", 2004, Traducción: Luis Montenegro Mena, 2007, Version Original en inglés: http://www.us-cert.gov/cas/tips/ST06-007.html, Version Traducción: http://www.clcert.cl/show.php?xml=xml/consejos/doc_06-07.xml&xsl=xsl/consejos.xsl

Criterios para la Selección de Consultores

Por Carolina Ovalle Grisales

EL CONSULTOR, ASESOR, AUDITOR, ANALISTA ES UNA PERSONA QUE VENDE "CONFIANZA - SERIEDAD Y PROFESIONALISMO", ES QUIEN ACONSEJA O DA SU OPINIÓN SOBRE UN TEMA GENERAL O ESPECÍFICO DENTRO DE SU ESPECIALIDAD.

En el momento en que al interior de una compañía surge la necesidad de selección de consultores es necesario que previamente se definan algunos aspectos, entre ellos:

Competencias técnicas: Nivel de formación y conocimientos específicos que requiere el consultor. Estas competencias son el resultado de la educación formal, experiencia profesional dentro de un campo especializado o por la combinación de las anteriores.

Educación: nivel de escolaridad y especialidad de estudios requeridos. Ej. Bachillerato, años de universidad, técnico, licenciatura, maestría, doctorado.

Conocimientos y habilidades técnicas: conocimientos previos que debe tener el consultor para el adecuado desempeño. Ej. "Certificaciones Profesionales reconocidas internacionalmente, Licencias especializadas, idiomas (cuál y nivel), manejo de sistemas, legislación específica, manejo de equipos técnicos, habilidades (mercadeo, ventas, sector, etc.)

Competencias conductuales: conjunto de habilidades, valores, actitudes y motivaciones que se manifiestan en comportamientos que son observables, definibles y medibles para alcanzar un desempeño superior al promedio.

Tarifa por categoría: las cuales son el resultado del análisis de los factores anterioresy el mercado. De tal manera que la entidad pueda contar con bases firmes para la oferta que se le hará al consultor seleccionado.

Experiencia total laboral: este factor considera el tiempo de desempeño en las funciones o responsabilidades de un tema o área específica, para que una persona con los conocimientos específicos pueda desempeñarse en forma óptima.

Teniendo claramente definidos los pasos anteriores, se inicia el proceso de reclutamiento y preselección de hojas de vida que consiste en filtrar posibles candidatos teniendo en cuenta los factores mencionados. Una vez seleccionado el grupo de hojas de vida se debe corroborar, a través de una entrevista y pruebas psicotécnicas y técnicas, los siguientes puntos:

1. Disponibilidad: Oportunidad en la atención de solicitudes, tiempo en el que se puede contar con el consultor.

2. Experiencia y calidad: tiempo que lleva desarrollando su objeto social y buen resultado en la verificación de referencias.

3. Precio y facilidades de pago: costo del servicio.

4. Competencias Técnicas y conductuales

Carolina Ovalle es Gerente de Desarrollo Humano Consejo Colombiano de Seguridad (CCS)

CERTIFICACIÓN PARA OFICIALES BÁSICOS DE SEGURIDAD FÍSICA -BPSO-

Con especialización en Instituciones Educativas

CURSO TEÓRICO - PRÁCTICO

Inicia Septiembre 2008

80% al 95% de Finaciamiento con el Consejo Nacional de Capacitación

CNCF Consejo Nacional de Capacitación y Formación Profesional

IFPO

Informes Telf: (593 2) 2923 600| 601

E-mail: gaguirre@ipc.org.ec

EL PISO, EN AREAS DE TRABAJO

Por Juan Ricardo Mancera*
Consultor Consejo Colombiano de Seguridad

El piso es una superficie horizontal que se dispone para contar con un suelo firme y llano para caminar y trabajar sobre él. En todos los lugares donde se desarrolle actividad humana se cuenta con uno que debe satisfacer los requisitos y necesidades de acuerdo al tipo de labor que se adelante sobre él.

En los reportes de accidentalidad laboral se utiliza el término "caída del mismo nivel" cuando un trabajador se cae de sus propios pies al piso donde está parado; es de esperarse que se presente un significativo sub registro estadístico de este tipo de eventos, ya que normalmente ocasiona consecuencias que no pasan de un golpe leve o un susto y una sonora risa.

Sin embargo, cualquier resbalón tiene el potencial de hacer daño; cuando en varias oportunidades suceden resbalones sin importancia o pequeños tropiezos, es cuestión de esperar, pero llegará el momento y la víctima en que se materializarán graves consecuencias.

El mayor coeficiente de rozamiento o fricción entre una suela del calzado y el piso, proporciona la seguridad para disminuir las resbaladas. La fuerza de rozamiento Fr es aquella que se opone al movimiento relativo entre el cazador y el piso y se expresa mediante la ecuación:

$$Fr = \mu \times N$$

Donde μ es el coeficiente de rozamiento particular entre dos superficies y

N es la fuerza normal a la superficie, es decir la fuerza perpendicular al plano, originada por el peso.

Para calcular μ basta con colocar un pesa sobre el calzado y aplicar horizontalmente una fuerza mediante un dinamómetro para registrar la fuerza suficiente para vencer la fuerza de rozamiento estática.

Una fuerza de rozamiento estática (sin movimiento relativo) es mayor a la fuerza de rozamiento dinámica (en deslizamiento), por eso es más fácil mantener en movimiento un elemento que iniciar el movimiento desde el reposo.

La placa estructural que soporta un piso debe responder suficientemente (por rigidez y resistencia) a las necesidades de las cargas fija, flotantes y en movimiento que se aplicarán sobre el piso, teniendo en cuenta las dilataciones de las placas.

ALGUNOS ASPECTOS A TENER EN CUENTA PARA LA SELECCIÓN DE PISO

- Si se trata de una zona de circulación es necesario evaluar e tipo de tráfico (liviano o pesado) referido a su resistencia a la fricción.•

- La posible exposición a agentes químicos (ácidos, álcalis, grasas, etc.) que puedan comprometer sus condiciones de diseño y de servicio.• La inflamabilidad y la producción de humos tóxicos de combustión, en caso de incendio.•

- Las condiciones de humedad para el piso y la pendiente o inclinación para la evacuación o drenaje de líquidos a una cuneta o sifón de recolección, para su neutralización si es necesario.

- Propiedades de antideslizamiento de tribología para evitar caídas.

- Facilidad de limpieza en las uniones de las tabletas y esquinas; según la aplicación (cocinas, baños, laboratorios, etc.) se disminuyen los sitios de acumulación de suciedad mediante la aplicación de resinas y esquinas en media caña. Durante el mantenimiento se debe señalizar el área y disponer de un sendero alterno cuando se trate de horarios de tráfico peatonal.

- La conductividad eléctrica del piso en algunas aplicaciones es significativa para evitar que se generen cargas estáticas en los usuarios para la triboelectricidad entre el piso y las suelas de los zapatos, resultan molestas para las personas, fatales para los circuitos electrónicos y favorecen la acumulación de polvo.

- Es importante considerar el color del piso para armonizar el ambiente cromático del local, las propiedades reflectivas de la luz y la facilidad para el aseo.

- La facilidad de mantenimiento y la necesidad de hacerle tratamientos de decapado, sellado, aplicación de emulsiones y ceras antideslizantes.

- Analizar en la selección, las propiedades mecánicas del piso, posibilidad de caída de objetos pesados, circulación de ruedas, deslizamiento de cargas, tipo de calzado.

- Nada más absurdo que un piso resbaloso o que se vuelve resbaloso con la humedad y se encuentra expuesto a la misma. Lo importante de un piso NO es que sea brillante sino que sea seguro para los usuarios.

- Estudiar la conveniencia de instalar plataformas en las zonas de tránsito.

- La solución de continuidad, es decir, que no se tengan escalones o interrupciones en la superficie.

Un Regalo de Vida

Herramienta de Rescate

RESQME

2 EN 1

CORTA-CINTURONES
ROMPE - CRISTALES

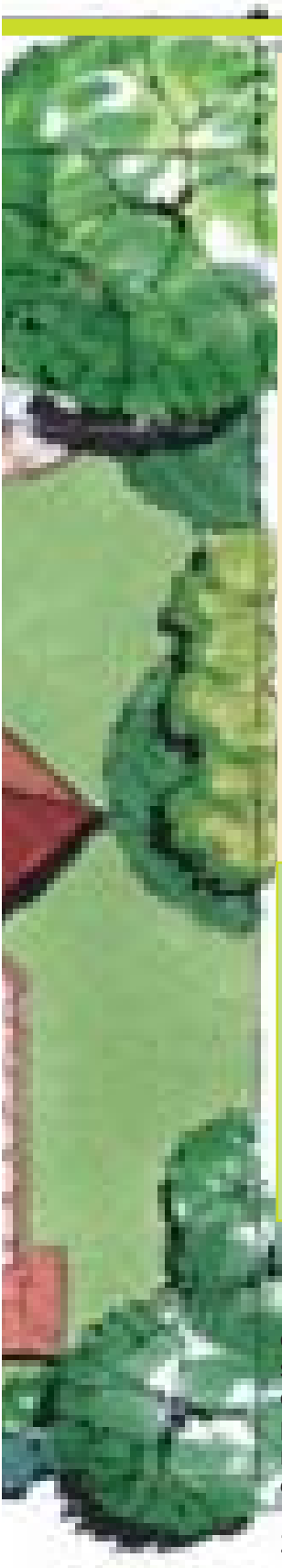
20,00 USD

INFORMES Y VENTAS

Info@protection-ecuador.com
Tef: (+593 2) 2923 600 | 601 ext. 124
Quito - Ecuador

Las falsas alarmas se reducirán en gran cantidad cuando los administradores generales o dueños de las estaciones centrales de monitoreo se preocupen en realidad por capacitar a su personal técnico en realizar excelentes instalaciones

MANEJO DE FALSAS ALARMAS



- ¿Usted sabia que las mayores causas de las alarmas falsas son:
1- errores del usuario;
2- errores de instalación o servicio
3- faltas del equipo

- ¿Usted sabia que mas de 80% de las alarmas falsas están relacionadas con los errores presentables del usuario?

- ¿Usted sabia que solo 20% de los usuarios de sistemas de alarmas causan 80% de todas las alarmas falsas?

- ¿Usted piensa que locaciones que tienen sistemas de alarma, tienen derecho a respuesta sin limitación?

- ¿Usted piensa que esta a mayor riesgo cuando la policía, después de estar acostumbrada a responder a las alarmas falsas, responde a un emergencia verdadera en su hogar?

¿QUÉ ES UNA FALSA ALARMA?

Una falsa alarma es la notificación de alarma a la central de monitoreo, que al responder no encuentran evidencia de una ofensa criminal o de un ofensa criminal que fue procurada.

CAUSAS COMUNES DE LAS FALSAS ALARMAS

1. Entrenamiento inadecuado de la gente que tiene permiso de acceso a su sistema de seguridad (niños, vecinos, encargados de la limpieza, agentes de propiedad, invitados, parientes, niñeras, personal de servicio y entregas, etc.)

2. Baterías débiles del sistema.

3. Puertas y ventanas que quedan abiertas, sin llave o que están flojas o sueltas.

4. Aire de los calentadores y del aire acondicionador que mueve las plantas, las cortinas, los globos, etc.

5. Animales domésticos que vagan.

¿CÓMO PREVENIR LAS FALSAS ALARMAS?

1. Antes de activar su sistema.

- Trabe todas las puertas y ventanas protegidas.

- Guarde los animales domésticos, globos, ventiladores calentadores, plantas, cortinas, decoraciones estaciónales, etc., lejos de áreas del sensor de movimiento.

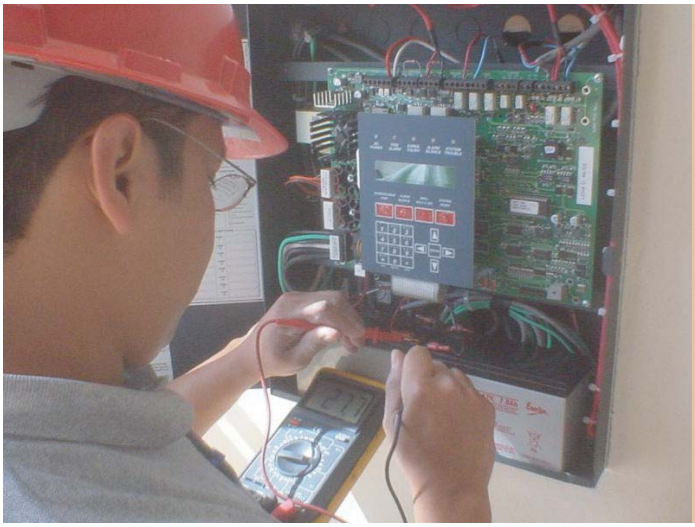
- Sepa cancelar la alarma si el sistema se activa.

2. Eduque a usuarios del sistema de alarma.

- Todos los usuarios, sostenedores dominantes o las personas con el acceso legal a su propiedad deben ser entrenadas a fondo en como usar su sistema, incluyendo el conocimiento de los códigos correctos para armar el sistema, las claves, los números de teléfonos y los procedimientos para cancelar activaciones accidentales de la alarma.

3. Asegúrese que la compañía de seguridad venga a inspeccionar y a mantener su sistema regularmente.

- El mantenimiento general puede ayudar prevenir muchas falsas alarmas.



4. Notifique a su compañía de seguridad si la alarma se activa o si:

- Piensa que su sistema NO está trabajando correctamente.

- Planea remodelar, incluyendo o substituyendo puertas o ventanas, drywall que cuelgan, pulir los pisos, instalar pisos en el ático o techos en el sótano, van a cambiar el sistema telefónico o instalar intercomunicadores, si va a poner apartaderos o ventiladores de techo, si va a instalar claraboyas o si va a fumigar, si va a instalar cables eléctricos o cualquier otra cosa cerca del panel de control del sistema o el teclado numéricos.

- Emplea ayuda doméstica, tendrá un nuevo animal, planea vender su casa, o está probando su sistema.

5. Entre en contacto con el coordinador de alarmas de su jurisdicción

6. **No olvide que la estación central de monitoreo NO debe solicitar la presencia Policial en casos de** interrupciones eléctricas, señales de batería baja o pérdida de conexiones de teléfono.

7. Reemplace los viejos sistemas con nuevos

- Usted ha cambiado de número telefónico o de dirección, o si alguna situación cambia, por ejemplo una persona lisiada ahora vive con usted.

sistemas de alto monitoreo de protección. Líneas telefónicas sucias o mojadas, las reparaciones de líneas telefónicas o interrupciones de servicio no requiere la respuesta de la policía.

8. Modernice los viejos sistemas de alarmas con equipos más nuevos que manejen los estandartes de la Security Industry Association (SIA) para reducir falsas alarmas.

Fuente:
http://www.ventasdeseguridad.com/i
http://www.sheriffleefl.org/spanish/alarms/

APLICABILIDAD De la tecnología VIDEO INTELIGENTE

EL GRADO DE MADUREZ ALCANZADO DURANTE LA ÚLTIMA DÉCADA POR LA TECNOLOGÍA DIGITAL, EN CUANTO A CAPTURA, CODIFICACIÓN, ALMACENAMIENTO Y TRANSMISIÓN DE INFORMACIÓN VISUAL HA SUPUESTO UN AVANCE EXTRAORDINARIO EN LAS PRESTACIONES Y CAPACIDAD DE LOS SISTEMAS DE VÍDEO - VIGILANCIA, A LA PAR QUE HA FACILITADO SU IMPLANTACIÓN A GRAN ESCALA

¿QUÉ ES VIDEO INTELIGENTE?

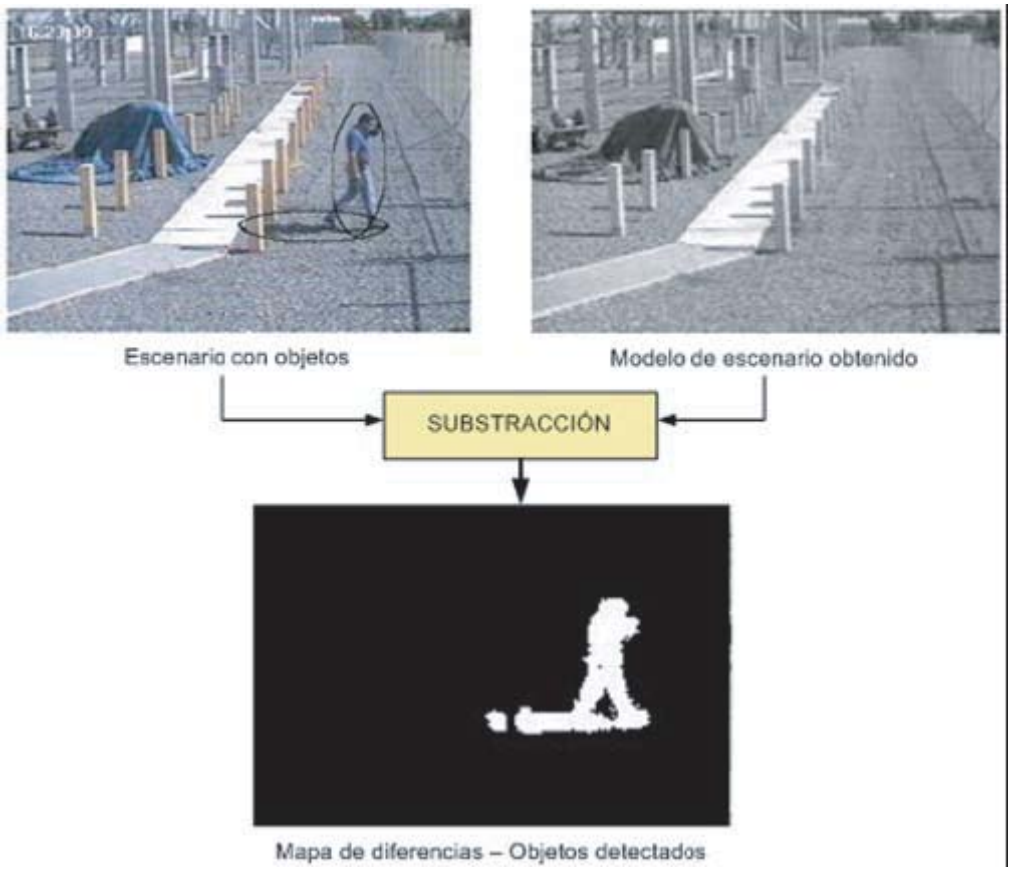
El video inteligente permite convertir los datos de video utilizando técnicas de procesamiento de imágenes en información procesable que será analizada mediante la aplicación de algoritmos basados en Inteligencia Artificial y Computer Vision Systems, con el objetivo de tomar decisiones automatizadas que contemplen las siguientes capacidades:

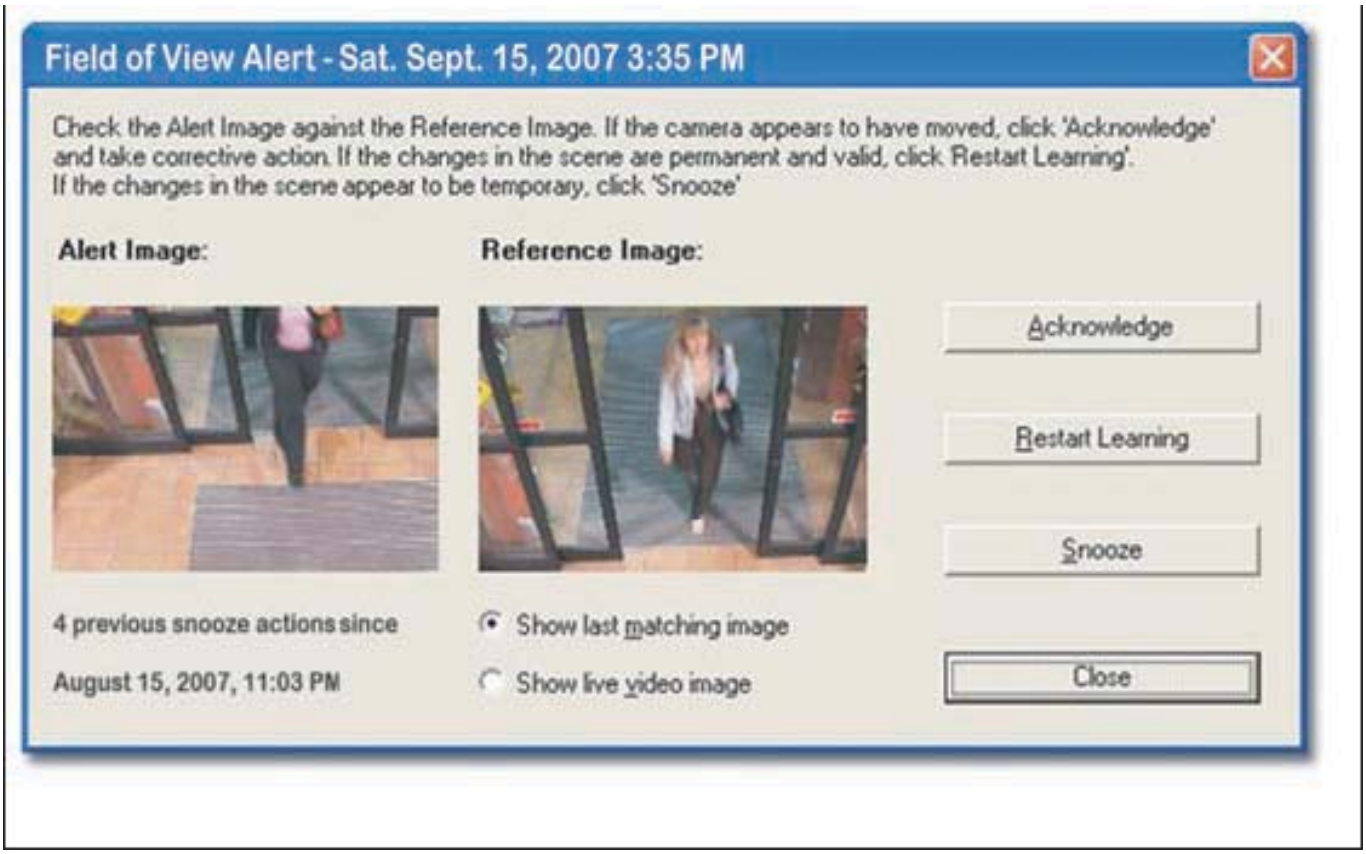
- Detección inteligente de movimientos.
- Detección y Clasificación de Objetos, como la identificación automática de siluetas humanas.
- Aprendizaje de escenas y eventos rutinarios.
- Detección de eventos inesperados.
- Comportamiento humano y vehicular.
- Reconocimiento de patrones.

El video inteligente se implementa frecuentemente para proveer protección y seguridad, pero también es una fuente valiosa de inteligencia visual para los usuarios en las instituciones financieras, comercios, transporte, y otros sectores como el comercial y el gubernamental. Combinando el poder de la analítica de video con otras aplicaciones empresariales, tales como los sistemas de reportes de transacciones de cajeros automáticos (ATM) y de punto de venta (POS), se alcanza un nuevo nivel de optimización de negocio.

Cuando se trata de la solución basada en hardware, sus características proporcionan una solución más eficaz en este tema, ya que el algoritmo es capaz de "ver" un intruso incluso cuando se está moviendo a muy baja velocidad. Esta capacidad está incluida en el sistema de origen, que fue desarrollado con fines militares: es imprescindible cuando se trata de proteger un perímetro altamente sensible o pasible a la intrusión que el sistema detecte hasta el más mínimo movimiento, por espaciado en el tiempo que éste sea.

Una aproximación, más eficiente, al reto de analizar el contenido de una secuencia de video se basa en la aplicación de algoritmos capaces de construir un modelo del escenario estático donde interactúan los objetos. En este caso, la relación total de objetos presentes en la escena (móviles o estáticos) se obtendrá comparando las distintas imágenes con el modelo de escenario (ver imagen abajo)





El monitoreo del campo visual alerta al personal de seguridad sobre los cambios de posicionamiento que la cámara sufre con el tiempo, comúnmente atribuibles a un problema de montaje. Algoritmos inteligentes aprenden el campo visual deseado y alertan al personal de seguridad cuando detectan desviaciones en la visión, generalmente causadas por vibraciones, golpes accidentales o simplemente porque el montaje esté suelto. Darse cuenta a tiempo de tales irregularidades, le permite al personal de seguridad corregir estos problemas de forma proactiva y eficiente, evitándoles la decepción de encontrarse con que la cobertura y la calidad del video no son las óptimas.

En el gráfico superior podemos apreciar que el Sistema de Vídeo Inteligente le permite al personal de seguridad corregir de forma proactiva los cambios en el campo de visión de una cámara o reaccionar de inmediato a una obstrucción accidental o premeditada.

Fuente:

http://www.alava-ing.es/EPORTAL_DOCS/GENERAL/SALESFORCEV2/DOC-cw465d59d83ece5/CuadernosSeguridadMayo07articulo.pdf

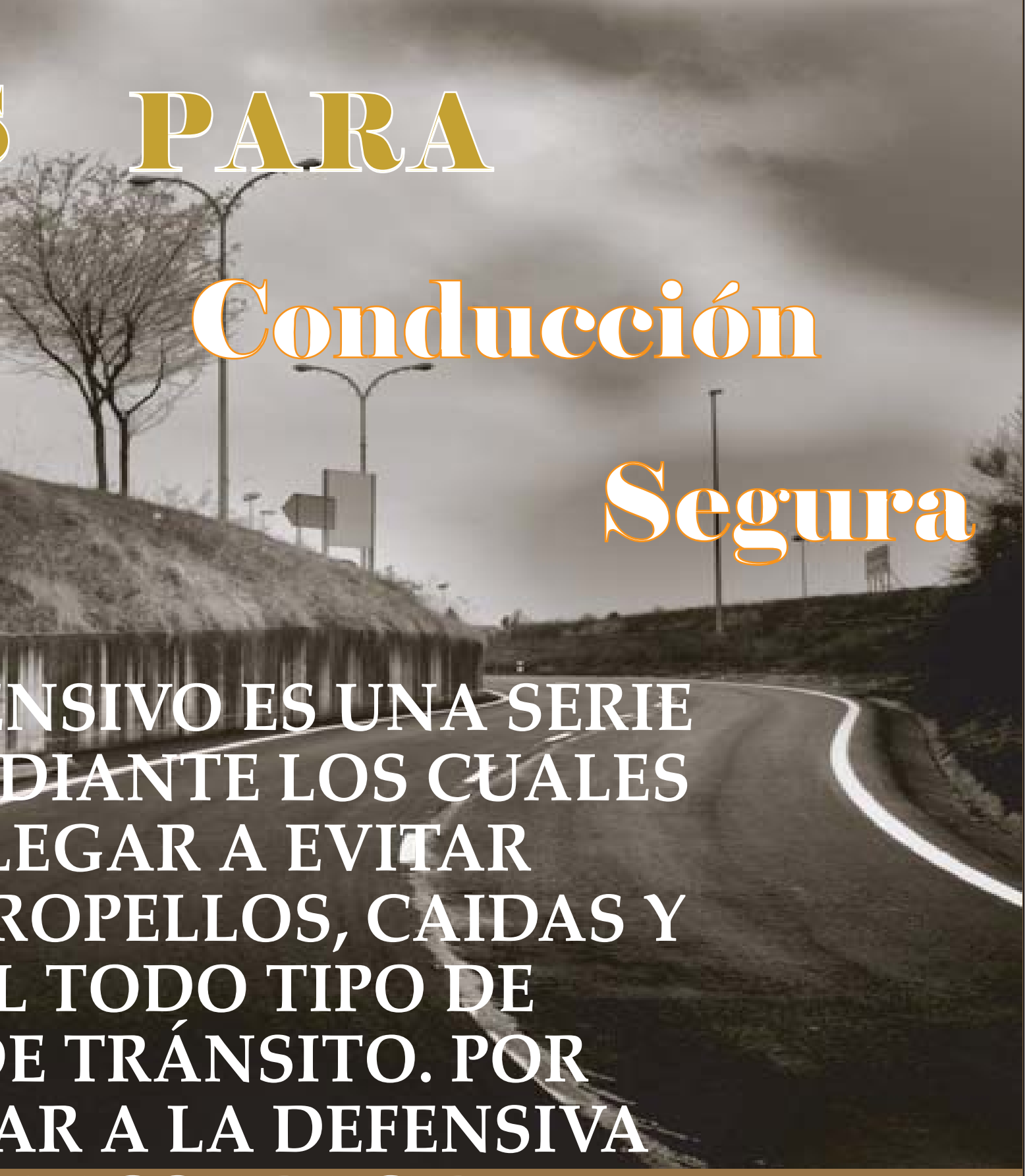
http://www.intekio.com/material/Informe_VI_rnds.pdf

http://www.marchnetworks.com/User_Files/Downloads/Resources/VideoAnalytics_DS_SP_09-07.pdf

SUGERENCIAS

una

EL MANEJO DEFE
DE HÁBITOS, MEI
SE PUEDE LI
COLISIONES, ATI
EN GENERA
ACCIDENTE D
TANTO, MANEJA
CONSISTE
PREVINIENDO L
PE



S PARA

Conducción

Segura

NSIVO ES UNA SERIE
DIANTE LOS CUALES
LEGAR A EVITAR
ROPELLOS, CAIDAS Y
L TODO TIPO DE
DE TRÁNSITO. POR
AR A LA DEFENSIVA
EN CONDUCIR,
AS SITUACIONES DE
LIGRO

CONDUCCIÓN DEFENSIVA

Hagamos este ejercicio: ubiquémonos en el lugar de otro conductor.

Muy poca gente sabe lo que es conducir vehículos de distinta clase. Ya sea que nuestros empleados conduzcan una motocicleta, un tractor lento. Un camión con acopiado, o un sedan de lujo, siempre pueden aprender de los conductores a su alrededor. Aquellos conductores que manejan distinta clase de vehículos quizá sean los que más conocimiento tengan para transmitirlo.

Pensemos por un instante. Aunque nos hayamos encontrado con alguno de estos vehículos, o quizás con todos, solo podemos entender de qué se trata su conducción si nos sentamos detrás del volante. La vista de la carretera, así como la capacidad de esquivar o frenar repentinamente, varía según cada vehículo.

Sin embargo, tener un poco de paciencia y contar con información, nos puede servir de mucho al compartir la vía pública con vehículos de distinto tamaño. Como conductores, necesitamos tener en cuenta las capacidades y limitaciones de todos los vehículos a nuestro alrededores.

CONDUCIR DEFENSIVAMENTE NOS PERMITE TENER EL CONTROL

Debido a que conducir una motocicleta es mucho más peligroso que conducir un automóvil o un camión, el National Safety Council recomienda que los demás conductores mantengan una distancia de seguimiento mayor a la usual entre su vehículo y una motocicleta. "También hay que tener mucho cuidado al conducir cerca de ciclistas o motociclistas que no usen cascos o equipos de protección personal", recomienda Jim Salomón, Gerente de Capacitación y desarrollo de programas del NSC.

Conducir defensivamente implica mantener un espacio de seguridad entre nuestro vehículo y los demás usuarios viales, hacer que los demás conductores noten la presencia de nuestro vehículo, y tener tiempo suficiente para tomar decisiones.

El curso de Conducción Defensiva del National Safety Council recomienda estas tres tácticas al acercarnos a un vehículo lento:

- Mantener la distancia suficiente para ver qué sucede alrededor del vehiculo
- No perder la paciencia
- Cuando sea seguro pasar, dejar mucho espacio entre nosotros y el vehículo lento.

En la carretera, los conductores de vehículos pequeños deben tener en cuenta que, un camión que gira en una dirección, puede moverse primero en dirección contraria para hacer la maniobra. Los conductores profesionales de camiones, tractores y camiones con acoplados saben que sus vehículos empujan aire por delante y alrededor de los mismos, generando un vacío por detrás. Los camioneros le llaman turbulencia. Los conductores inexpertos, o que conducen un vehículo alquilado, quizás no sepan cómo actuar ante una turbulencia y pueden salirse de la carretera o virar en dirección del tránsito que viene en el carril contrario.

Si usted no es un profesional de la Conducción considera las siguientes recomendaciones, en las vías de circulación:

• Respete en todo momento las señales de circulación, aún conociendo la carretera.

Estos son algunos consejos del National Safety Council para conducir defensivamente cerca de vehículos grandes o pequeños:

• No conducir en los puntos ciegos de los vehículos grandes.
• No conducir pegados al vehículo; una vez que le rebasamos, no ingresar al carril demasiado rápido.
• No forzar el sobrepaso

EXTREME LAS PRECAUCIONES CUANDO SE ENCUENTRE:

• Un cruce de carreteras.
• Cambios de rasante.
• Curvas con escasa visibilidad.
• Pasos a nivel.
• Si se encuentra con un banco de niebla, circule lentamente, utilizando las luces antiniebla (traseras y delanteras) y sin hacer uso de las "largas", ya que éstas pueden deslumbrarle.
• Cuando el viento sople con fuerza, modere su velocidad, agarre el volante con ambas manos de forma firme y evite movimientos bruscos.
• En caso de lluvia, reduzca la velocidad y emplee los frenos lo menos posible. Si la lluvia es muy fuerte y el limpiaparabrisas no garantiza una buena visibilidad, detenga el coche en lugar seguro y espere hasta que amaine.
• Si debe circular sobre hielo, utilice el embrague y el freno de forma suave, mantenga la dirección firme y en caso necesario haga uso de las cadenas.

CONDICIÓN DE LOS VEHÍCULOS

Cuide en todo momento el estado de su vehículo, no sólo cuando deba realizar largos desplazamientos.
Recuerde pasar la Revisión vehicular obligatoria o voluntariamente, ya sea por la edad del automóvil o por haber sufrido un accidente que haya podido afectar al motor, transmisión o bastidor.

SIEMPRE ATENCIÓN A:

• Los sistemas de seguridad activa:

El estado de los neumáticos (deformaciones, desgaste y presión).
El correcto funcionamiento de la dirección.
Las posibles anomalías de la suspensión (amortiguadores).
La efectividad de los frenos (discos, pastillas, tambores, zapatas, latiguillos, bombines y líquido).
El correcto funcionamiento, reglaje y limpieza de todas las lámparas que conforman el alumbrado.
El posible deterioro de los limpiaparabrisas.

• Los sistemas de seguridad pasiva.
El estado y correcto funcionamiento de los cinturones de seguridad, airbag, chasis y carrocería.
• Otros sistemas.
• Disponga en el coche de los triángulos de señalización reflectante y el chaleco reflectante.
• El buen estado del motor, la transmisión y la batería.

FACTOR HUMANO
Conduzca siempre con precaución. Cuando deba maniobrar, señalice con suficiente antelación su intención y compruebe que los demás se han percatado de su advertencia.

• Circule siempre por el carril que proceda y bien centrado en el. Mantenga la distancia de seguridad o separación cuando circule detrás de otro vehículo, en previsión de que este frene bruscamente

• Los adelantamientos son la maniobra de mayor peligrosidad: avise de su intención y cerciórese que puede hacerlo con total seguridad y en el menor tiempo posible.

• Si va a ser adelantado, no incremente su velocidad y facilite el adelantamiento.

• No se detenga de forma repentina. Señalícelo con antelación y no dificulte la circulación.

• Respete los semáforos y recuerde que la luz amarilla nos indica que debemos parar, no que todavía podemos pasar.

• Debe esperar a que los peatones hayan alcanzado la acera para avanzar, aunque el semáforo ya esté verde.

• No utilice el teléfono móvil o cualquier otro sistema de comunicación mientras conduce, salvo que el desarrollo de la comunicación tenga lugar sin emplear las manos, cascos, auriculares o instrumentos similares.

• Cuando conduzca de noche, realice correctamente los cambios de luces, procurando no deslumbrar a los demás.

• No olvide que el cinturón de seguridad no es una opción voluntaria. No olvide que es obligatorio el uso del cinturón de seguridad para todos los pasajeros y en cualquier tipo de recorrido urbano o interurbano y por corto que éste sea. Habitúese a utilizarlo en cualquier trayecto

• Recuerde que debe disponer del chaleco reflectante homologado y utilizarlo en condiciones de luminosidad insuficiente.

• Utilice los triángulos de señalización cuando la parada de su vehículo pueda ocasionar riesgo a terceros.

• El alcohol, incluso ingerido en pequeñas cantidades, influye negativamente en la conducción. Recuerde que el mayor peligro de accidente grave se da cuando el grado de alcoholemia es intermedio, debido al estado de euforia en el que se encuentra el conductor.

• Muchos medicamentos pueden ser peligrosos a la hora de conducir. No se automedique y lea siempre los prospectos.

• En caso de viajes largos, descanse cada dos horas aproximadamente, tome bebidas refrescantes y comidas ligeras que no favorezcan el sueño.

No lance ningún objeto por la ventanilla, puede provocar un accidente o un incendio si se trata de colillas.

• Recuerde conducir con tranquilidad:
No se fije una hora de llegada.
No se deje influir por el hecho de que otros vayan a mayor velocidad.
No es bueno destacar, ni por ir demasiado rápido, ni demasiado despacio.
Comprenda las advertencias y los errores de los demás.

• Cumplir las normas de circulación no sólo evita sanciones: evita accidentes.

NO ES SUFICIENTE CONOCER EL CÓDIGO DE CIRCULACIÓN, HAY QUE CUMPLIRLO

CICLOMOTORES Y MOTOCICLETAS

• Utilice un casco reglamentario, puede salvarle la vida.

• No aproveche la movilidad de su vehículo para provocar situaciones de riesgo en los embotellamientos y semáforos.

• Tenga siempre presente que cualquier colisión puede transformarse en un accidente grave.

Vehículos de usos múltiples

• No cargue el vehículo con un peso mayor al que tenga asignado. Reparta el peso de la carga y asegure su estabilidad.

• Tenga siempre en cuenta que su vehículo es una máquina pesada, peligrosa y poco maniobrable.

Fuente:
Conducción defensiva, National Safety Council de Estados Unidos de Norteamérica

Sepa cómo actuar

SI SU VEHICULO ES DETENIDO POR LA POLICIA

1) En caso de ser un auto patrullero de inmediato recomendamos anotar el numero de registro del vehiculo pintado en el mismo

2) Poner seguro en todas las puertas del vehiculo. Abrir única y parcialmente la ventana del conductor para que se pueda entregar los documentos del vehiculo y la licencia de conducir en caso de ser requerido por el policía.

3) ANTES DE ENTREGAR NADA, EXIGIR LA IDENTIFICACION DEL POLICIA, que en general debe llevar en el pecho de modo visible, y ANOTARLA, así como la hora de la detención. Usted debe exigir al supuesto policía sus documentos. No se deje intimidar; manténgase firme, sin ser atrevido o descortés.

4) POR NINGUNA CIRCUNSTANCIA SE BAJE DEL VEHICULO NI ABRA LA PUERTA AL POLICIA.

5) Si el policía manifiesta que el vehiculo tiene orden de captura, indicarle que el vehiculo deberá ser llevado a la comisaría mas cercana, pero manejado por el propietario. Nunca, POR NINGUN MOTIVO, entregue el vehiculo a la policía.

6) Usted NO debe permitir NUNCA la revisión del vehiculo (abrir la maletera u otro acto similar). Tampoco debe, NUNCA, entregar las llaves del mismo para que pueda ser revisada la maletera u otra parte de su auto.
Para poder hacer esta revisión, indispensablemente, la policía deberá presentarle a usted previamente una Orden de Cateo emitida por el Juez. Su automóvil es una PROPIEDAD PRIVADA, igual que SU CASA; nadie tiene derecho a invadirla, revisarla o atropellarla.
(Por ejemplo, si usted permite que revisen su maletero, un mal policía -que alguno existe- podría fácilmente "sembrarle" drogas, armas u otros elementos).

7) Al llegar a la Comisaría bajarse del vehiculo y cerrarlo. NO entregar las llaves a la policía en modo alguno, aunque se lo pidan o "exijan". Solicitar firmemente al comisario LA PRESENCIA DE UN FISCAL.

8) Si usted no tiene teléfono celular, solicite el uso de la línea telefónica para llamar a sus familiares. Esto DEBE ser cumplido por la policía. Si a usted lo detienen llame por celular de inmediato a dos o más familiares, del número del policía que debe tener en su uniforme y describa el hecho.

Fuente: *http://www.forodeseguridad.com/artic/prevenc/3066.ht*

Recuerde:
MUY IMPORTANTE!
Por: César Ortiz Anderson,
Presidente de APROSEC del Perú.

1. Un policía no puede detener a nadie si no es por un flagrante delito.

2. Si no se ha cometido una falta y la documentación esta en regla, un policía necesita una Orden de Captura y una Orden de Cateo (ambas, no basta una) para intervenir un vehiculo.

3. La persona intervenida tiene derecho a pedir un abogado y los policías necesitan la indispensable presencia física de un fiscal para poder hacer una intervención a un vehiculo cualquiera.

4. Los policías tienen la absoluta obligación de identificarse.

5. Si le dicen que hay que ir a una comisaría, hay que exigir ir a la más cercana.

MUY IMPORTANTE: GUARDAR UNA COPIA DE ESTE ESCRITO EN SU AUTOMOVIL, POR SU TRANQUILIDAD y SEGURIDAD

CURSO DE CONDUCCIÓN EVASIVA

FUNDACIÓN

IPC | Integrated protection concepts

Creando Cultura de Seguridad

Aprenda a manejar técnicas de conducción que le permitan escapar de una acción ofensiva, preservando la integridad de los atacados.

Septiembre 2008

Quito - Ecuador

Informes

Fundación Conceptos Integrados de Protección - IPC -
Av. Eloy Alfaro N35 144 y Portugal
Telf. (+593 2) 2923 600| 601 ext. 124
E-mail: info@ipc.org.ec
www.ipc.org.ec

CONTROLE EL ROBO De Información En Su Empresa

"Dime qué quieres y te conseguiré la información que requieras". Si de la información depende el futuro de su empresa, prevéngase: cuatro de cada 10 ejecutivos ignora medidas de prevención de robo de datos y de las soluciones disponibles para prevenirlos

La escasa práctica de salvaguarda especializada de la información, el alto costo de los sistemas de seguridad, así como la falta de un diagnóstico nacional sobre pérdidas por este delito y de medidas de protección y persecución, hace que las empresas ecuatorianas sean altamente susceptibles de padecer el espionaje industrial.

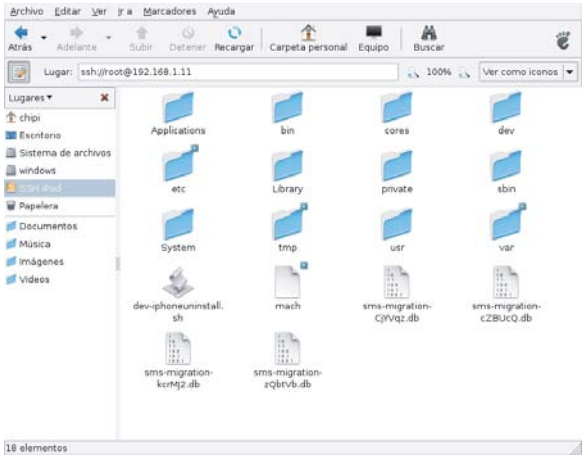
El robo de información de Petrobras en Brasil, la ruptura de seguridad de la página Web de la Presidencia del Ecuador –por un aficionado-, entre otros a nivel local e internacional ponen al descubierto una industria global que, si hacemos referencia a las compañías estadounidenses, solo en un año le ha quitado información privilegiada y propiedad intelectual por un valor de USD 59 billones, según una encuesta de la

American Society of Industrial Security (Sociedad Americana de Seguridad Industrial) y Price Waterhouse Coopers, publicada en el año 2002. Un cálculo estimado indica que las cifras actuales ascienden a USD 100 billones.

Para especialistas del área esta amenaza, creciente en América Latina, exige se desarrollen políticas para el diseño y planificación estrategica para contrarrestar este tipo de amenazas. Principalmente por la subestimación a la competencia desleal, pues contrariamente a lo que ocurre con los bienes tangibles, que se pueden ver si han sido robados, es posible que por años se le haya estado sustrayendo a una compañía su propiedad intelectual o su ventaja competitiva y que nadie se dé cuenta.

La competencia puede sacar ventajas en el mercado constantemente, ya sea haciendo una oferta más baja en una licitación o simplemente desarrollando innovaciones más económicas o más rápidamente. Sus secretos corporativos en manos de la competencia significan conocimiento que puede volverse en su contra.

Por supuesto que el espionaje corporativo no se limita a los actores globales y a una inversión técnica masiva. Es posible que los espías profesionales descubran el perfil de una pequeña compañía obteniendo sus conversaciones privadas, documentos desechados, memos, proyectos y desechos de material de viajes



¿QUIÉN VENDE LA INFORMACIÓN?

Uno de los factores críticos a la hora de gestionar la seguridad de información en las organizaciones es el **factor humano**. Según datos de un cálculo estimativo, dos tercios del total del espionaje corporativo en los EE.UU. son desarrollados por los propios empleados.

Especialistas en sabotaje electrónico, sostienen que el enlace más débil con respecto a la protección de datos comerciales vitales es el **trabajador** mismo. Así, se puede colocar firewalls (cortafuegos) en cada una de las computadoras pero en realidad todo depende de cada persona, de su lealtad para con la empresa y sus valores y necesidades satisfechas.

Aún así es frecuente observar como por norma general los esfuerzos de seguridad técnica suelen ser muy considerados, pero sin embargo, la seguridad del factor humano es menospreciada o en el peor de los casos, pasada por alto. En estos casos, hablamos del enemigo que está dentro, bien sea por la intencionalidad de sus actos o por negligencia en el tratamiento de los activos de la información.

La idea de controlar al personal no está relacionada con la restricción de la libertad y la comodidad de los empleados en las organizaciones: se trata de imponer puntos de control en el factor humano que opera con la información, de modo que se eviten fugas de información, errores en el manejo de datos, brechas en la confidencialidad y que la protección de aspectos importantes, como los secretos industriales y "know-now" de los negocios, sea una realidad no sujeta a posibles fisuras causadas por el espionaje industrial o la competencia desleal.

¿QUE HACER?

1. Protección Técnica de aquellos datos guardados en una computadora. Es necesario desarrollar un programa de capacitación de seguridad para los empleados.

2. Considerar la seguridad de información y no la seguridad de IT, y ello debe formar parte de las principales responsabilidades del área de administración de la compañía. Ello implica un cambio cultural en el modo de pensar.

Todas estas son buenas pautas a seguir por todo tipo de compañía, sea pequeña o mediana, ya que son las personas menos pensadas las que puedan estar recolectando información sobre las actividades y los planes de su compañía más allá de límites insospechados.

CONTRAESPIONAJE

Para protegerse de los intrusos en los sistemas de información se pueden aplicar una serie de medidas:

1. Que los empleados firmen cláusulas de confidencialidad en sus contratos de trabajo para que no divulguen información estratégica a la que tienen acceso, lo que se aplica a un cierto periodo aún si dejan de pertenecer a la compañía.

2. Elaborar estudios de control de confianza de los nuevos empleados para advertir qué tan proclives son a cometer actos de espionaje y robo de información confidencial.

3. No dejar documentos importantes sobre los escritorios ni en las pantallas de las computadoras.

4. Borrar siempre los pizarrones de las salas de juntas.

5. Evaluar riesgo y vulnerabilidad de su empresa ante los competidores.

6. Establecer una limpieza de oficinas de los principales ejecutivos y tecnificarla para tomar medidas preventivas.

7. Buscar áreas seguras para las reuniones de trabajo.

8. Apegarse a los estándares de seguridad informática, que certifica las empresas en función de sus metodologías y estándares de protección de información.

Fuente:
http://www.seguridad-la.com/artic/segcorp/7208.htm
http://www.jornada.unam.mx/2006/02/06/6n1sec.html

La firma electrónica, como la firma ológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido o garantizar que no se pueda modificar su contenido.

FIRMA DIGITAL
CLAVE DEL COMERCIO ELECTRONICO

La aparición y desarrollo de las redes telemáticas, de las que Internet es el ejemplo más notorio, ha supuesto la posibilidad de intercambiar entre personas distantes geográficamente mensajes de todo tipo, incluidos los mensajes de contenido contractual. Estos mensajes plantean el problema de acreditar tanto la autenticidad como la autoría de los mismos. Pero partamos de lo básico:

¿QUÉ ES Y PARA QUÉ SIRVE LA FIRMA DIGITAL?

Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

Concretamente, para que dos personas (ya sean dos empresarios o un empresario y un consumidor) puedan intercambiar entre ellos mensajes electrónicos de carácter comercial que sean

mínimamente fiables y puedan, en consecuencia, dar a las partes contratantes la confianza y la seguridad que necesita el tráfico comercial, esos mensajes deben cumplir los siguientes requisitos:

1. Identidad, que implica poder atribuir de forma indubitada el mensaje electrónico recibido a una determinada persona como autora del mensaje.

2. Integridad, que implica la certeza de que el mensaje recibido por B (receptor) es exactamente el mismo mensaje emitido por A (emisor), sin que haya sufrido alteración alguna durante el proceso de transmisión de A hacia B.

3. No repudiación o no rechazo en origen, que implica que el emisor del mensaje (A) no pueda negar en ningún caso que el mensaje ha sido enviado por él.

4. Confidencialidad, que no es un requisito esencial de la firma digital sino accesorio de la misma. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

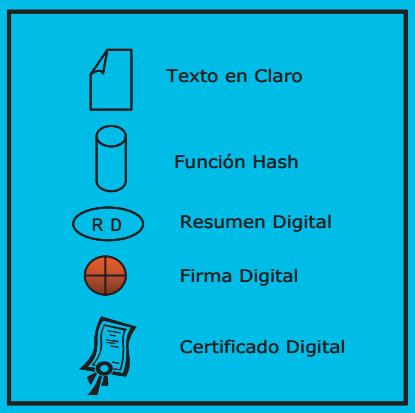
VALOR JURÍDICO DE LA FIRMA DIGITAL

Si efectivamente el tejido telemático nos conduce a aprovechar las ventajas del correo electrónico, navegación en el Internet u ofertar productos y servicios a través de portales o páginas en la red (marketing virtual), es efectivo que esta fase debe encontrar reciprocidad, con la adquisición de artículos de todo tipo, pago de impuesto o servicios básicos. En este marco, el comercio electrónico, definido como "cualquier forma de transacción comercial en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo", debe verse avalado por una firma digital. Por lo que resulta primordial generar confianza en el usuario de Internet y ofrecer seguridad jurídica a las operaciones económicas.

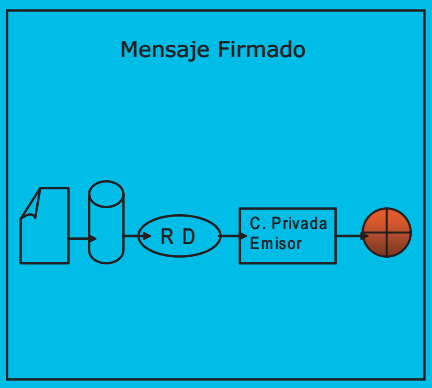
En la legislación Ecuatoriana, el tema de la firma digital, se encuentra mencionada en la **Ley de Comercio Electrónico** que equipara la validez de la firma manuscrita con la firma electrónica. Y como mencionara, la Dra. María Cristina Vallejo Ramírez, Abogada y Especialista Superior en Derecho Financiero y Bursátil, se lo puede presentar dentro de juicio,

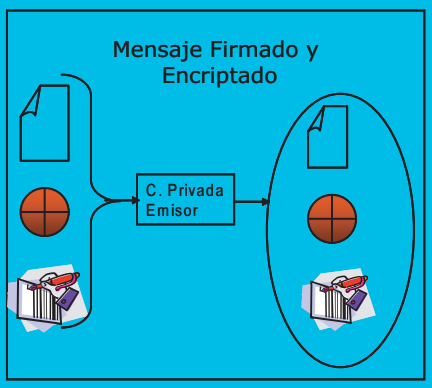
OPERATIVIDAD DE LA FIRMA DIGITAL

Para enviar un texto con la firma electrónica se necesitan 2 personas: EMISOR Y RECEPTOR.



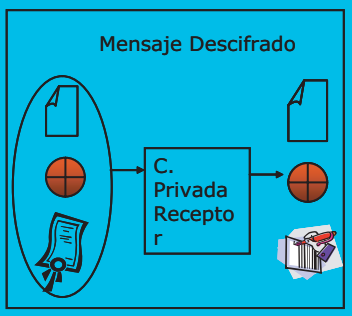
1.- El emisor elabora un texto, para evitar que sea muy extenso, utiliza el dispositivo de creación de firma y aplica sobre el texto la función "hash" es el algoritmo matemático que comprime el mensaje, obteniendo el resumen digital, posteriormente el emisor aplica al resumen su clave privada (Datos de creación de firma), obteniendo de este modo su FIRMA ELECTRÓNICA.

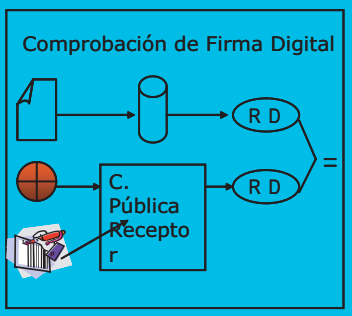




2.- El dispositivo de creación de firma agrupa 3 elementos: texto, firma electrónica y certificado digital conteniendo la clave pública del emisor, que previamente habrá sido solicitado y expedido por una Autoridad de Certificación, son encriptados con la clave pública del receptor y remitidos a través de Internet.

3. El receptor recibe los datos el receptor, coloca su clave privada sobre los datos encriptados y obtiene el texto, la firma electrónica y el certificado digital, conteniendo la clave pública del emisor. Para comprobar que la firma y el documento son auténticos, se toma la clave pública del emisor.





Superior en Derecho Financiero y Bursátil, se lo puede presentar dentro de juicio, siempre y cuando esté basado en un certificado reconocido y haya sido producida mediante un dispositivo seguro de creación de firma.

Con relación a la impugnación del certificado o de firma electrónica, el Artículo 54 Inciso segundo de la Ley de Comercio Electrónico Ecuatoriano, dispone que el "Juez o Tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados.

Por su parte, el efecto legal que se persigue está íntimamente vinculado con la confianza que tenga la Autoridad de Certificación.

CONCLUSIONES

El desarrollo del comercio electrónico y la firma digital, juegan un papel determinante en la recuperación de la confianza y seguridad de los usuarios, que sienten en las comunicaciones electrónicas una apertura al mundo actual. En el Ecuador, la "era digital", está empezando a despuntar, pero lamentablemente, no todos tienen acceso a la información. Así, apenas el 2% de la sociedad ecuatoriana utiliza Internet en forma directa, por lo que todavía está lejano el B2B, business to business (negocios entre empresas) B2C, business to consumer (negocios entre empresas y consumidores) o el C2C (Consumer to consumer) que es el comercio minorista.

Es importante resaltar, que la firma digital, es un instrumento que permite la adaptación a este nuevo paradigma socio-económico-cultural, porque posibilita la expansión del comercio dentro de esta nueva economía digital globalizada y, en el ámbito administrativo o gubernamental, optimiza la eficiencia a un bajo costo, con intervención y participación de los ciudadanos.

El esquema de este sistema se puede resumir en los siguientes pasos:

1. A cada usuario se le asigna un número entero que funciona como su clave pública.

2. Cada usuario posee una clave privada que solo él conoce, y que es distinta para cada uno y es diferente de la clave pública.

3. Existe un directorio de claves públicas que pueden ser conocidas a través de Internet. Este directorio está abierto para todas las personas.

4. El emisor envía el mensaje encriptándolo con la clave pública del receptor o destinatario, el mismo mensaje se firma con la clave privada del emisor.

El destinatario sólo podrá abrir el mensaje con la clave pública del emisor para constatar la veracidad de la firma y podrá descifrar el mensaje con su clave privada (es decir la del receptor).

El éxito de este sistema, se debe a que garantiza la seguridad y confidencialidad de las comunicaciones telemáticas. En otras palabras, la firma basada en RSA (algoritmo asimétrico cifrador) provoca que el contenido del mensaje sea IRREVERSIBLE, ÚNICO e INVARIABLE. Además facilita una perfecta identificación de remitente y destinatario. Esta última función, se realiza a través de los llamados "terceros de confianza", que han sido denominados "Notarios Electrónicos", quien es el depositario único y exclusivo de declaraciones de voluntad (acuerdos entre partes) en la contratación electrónica.

Fuente:

http://www.proasetel.com/paginas/articulos/utilizacion_firma.htm
http://www.marklaw.com.ec/Newspage.asp?MnidNum=24
http://www.tuguialegal.com/firmadigital1.htm

CURSOS Y EVENTOS

AGOSTO – SEPTIEMBRE

EVENTO - CURSO	FECHA	LUGAR
Seminario Gratuito "Cómo Generar valor Agregado a traves de Personal Profesional de Protección"	Septiembre 09 Septiembre 04 Septiembre 10	Guayaquil Quito Manta
Feria Internacional de Seguridad	Agosto 23 a Septiembre 23	Quito –Ecuador-
Curso Práctico de Conducción Evasiva	Agosto - Septiembre	Quito –Ecuador-
Curso de Brigadistas para Manejo de Emergencias	Septiembre	Quito –Ecuador-
Curso para Oficiales Básicos de Protección en Instituciones Educativas	Septiembre	Quito –Ecuador-
Protección de Personalidades	Septiembre 15 - 20	Buenos Aires –Argentina-
Diplomado en Alta Dirección de Seguridad Corporativa	Septiembre 22 - 26	Buenos Aires –Argentina-

PLAN DE EM

Necesi

y em

PARTE FINAL

En la edición anterior nos enfocamos en tratar el tema de las Estructura del Plan de Autoprotección, en esta edición, nos enfocaremos en el Plan de Emergencia

PLAN DE EMERGENCIA

El plan de emergencia define la secuencia de acciones a realizar para el control inicial de las emergencias que pueden producirse. Este plan debe responder a las preguntas:
¿Qué se hará?
¿Cuándo se hará?
¿Cómo y dónde se hará?
¿Quién lo hará?

1. **Clasificación de las Emergencias**

Por su gravedad se clasifican en función de las dificultades existentes para su control y sus posibles consecuencias en:

a. Conato de emergencia. Es una emergencia que puede ser controlada de manera sencilla por el personal del local, dependencia o sector.
b. Emergencia parcial. Emergencia que requiere para su control la actuación de equipos especiales del sector. No afectará normalmente a sectores colindantes.

MERGENCIA

dad industrial

mpresarial

c. Emergencia general. Emergencia para cuyo control será necesaria la actuación de todos los equipos y medios de protección propios y medios externos. Comportará generalmente evacuaciones totales o parciales.

Por la disponibilidad de medios humanos los planes de actuación en emergencias podrán clasificarse en:

- **Diurno.** A turno completo y en condiciones normales de funcionamiento
- **Nocturno**
- **Festivo**
- **Vacacional**.

La disponibilidad de medios humanos puede influir evidentemente sobre el grado de emergencia que se está tratando. Como ejemplo de ello se podría exponer que un mismo tipo de fuego durante una jornada normal daría lugar a una emergencia parcial y por la noche su tratamiento sería diferente.

2. Acciones a realizar

Se pueden diferenciar las siguientes:

a. Alerta, cuyas funciones son las siguientes:
Poner en acción a los equipos interiores de primera intervención
Informar a los restantes equipos de emergencia y las ayudas exteriores.

b. Alarma, para la evacuación de los ocupantes.

c. Intervención. Toda operación de control de la emergencia.

d. Apoyo, para la recepción e información a los servicios de ayuda exterior.

3. Equipos de emergencia

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.

PLAN DE EMERGENCIA

EMERGENCIAS	ACCIONES A REALIZAR	EQUIPOS DE EMERGENCIA	SEC
Conato de Emergencia	Alerta	Jefe de emergencia Jefe de Intervención	
Emergencia Parcial	Alarma	Primera Intervención	Ope
Emergencia General	Intervención	Segunda Intervención (FF.PP)	Esqu
Post Emergencia	Apoyo	Alarma y Evacuación Primeros Auxilios	

Jefe de Emergencia –J.E-

Trabaja desde el Centro de Comunicaciones del establecimiento y en función de la información que le facilite el jefe de Intervención sobre la evolución de la emergencia enviará al área siniestrada las ayudas internas disponibles y recabará las externas que sean necesarias para el control de la misma.

- Es la máxima autoridad en el establecimiento durante las emergencias.
- El Jefe de Emergencia decide el momento de la evacuación del establecimiento.

Jefe de intervención –J.I-

Valorará la emergencia y asumirá la dirección y coordinación de los equipos de intervención en la escena.
Sus funciones serán las siguientes:

- Dirigirá las operaciones de extinción en el punto de la emergencia, donde representa la máxima autoridad.
- Informará al Jefe de emergencia sobre la evolución de la emergencia.
- El Jefe de Intervención tendrá un profundo conocimiento en materia de seguridad y planes de Autoprotección.

Equipo de primera Intervención (E.P.I.)

- Sus miembros con la formación adecuada acudirán al lugar donde se ha producido la emergencia con el objeto de intentar su control.
- Sus principales misiones serán las siguientes:

a. Importante labor preventiva, ya que se conocerán las normas fundamentales de la prevención de incendios y demás emergencias.

b. Combatir conatos de incendio con extintores portátiles (medio de primera intervención) en su zona de actuación (planta, sector, etc.)

c. Apoyar a los componentes de Equipo de Segunda Intervención cuando les sea requerido.

- La actuación de los miembros de este equipo será siempre por parejas.

Equipo de segunda Intervención (E.S.I.)

Sus miembros con la formación adecuada, actuarán cuando dada su gravedad, la emergencia no pueda ser controlada por los equipos de primera intervención y prestarán apoyo a los servicios exteriores cuando sea necesario.

- Este equipo representa la

CUENCIA DE ACCIONES

raciones a realizar

uema de Operaciones

máxima capacidad extintora del establecimiento.
- Su ámbito de actuación será cualquier punto del establecimiento donde se pueda producir una emergencia.

Equipo de alarma y evacuación (E.A.E.)
Sus miembros realizan acciones encaminadas a asegurar una evacuación total y ordenada de su sector y asegurar que se ha dado la alarma

Las misiones fundamentales del mismo serían las siguientes:

a. Preparar la evacuación, comprobando que las vías de evacuación están expeditas.
b. Dirigir el flujo.
- Hacia las vías de evacuación
- Controlando la velocidad de la evacuación e impidiendo las aglomeraciones en las salidas y accesos a escaleras.
- Impidiendo la utilización de los ascensores en caso de incendio.

c. Comprobación de la evacuación de sus zonas.
Sus miembros prestarán los primeros auxilios a los lesionados por las emergencias.

EQUIPOS DE EMERGENCIA

Composición de los Equipos de Emergencia

Para conocer la composición de los equipos de emergencia se deben tener en consideración, entre otros, los siguientes aspectos:
- Características del Edificio
- Características de los Ocupantes del Edificio
- Nivel de Ocupación
- Nivel de riesgo de las actividades llevadas a cabo.

4. Desarrollo del plan

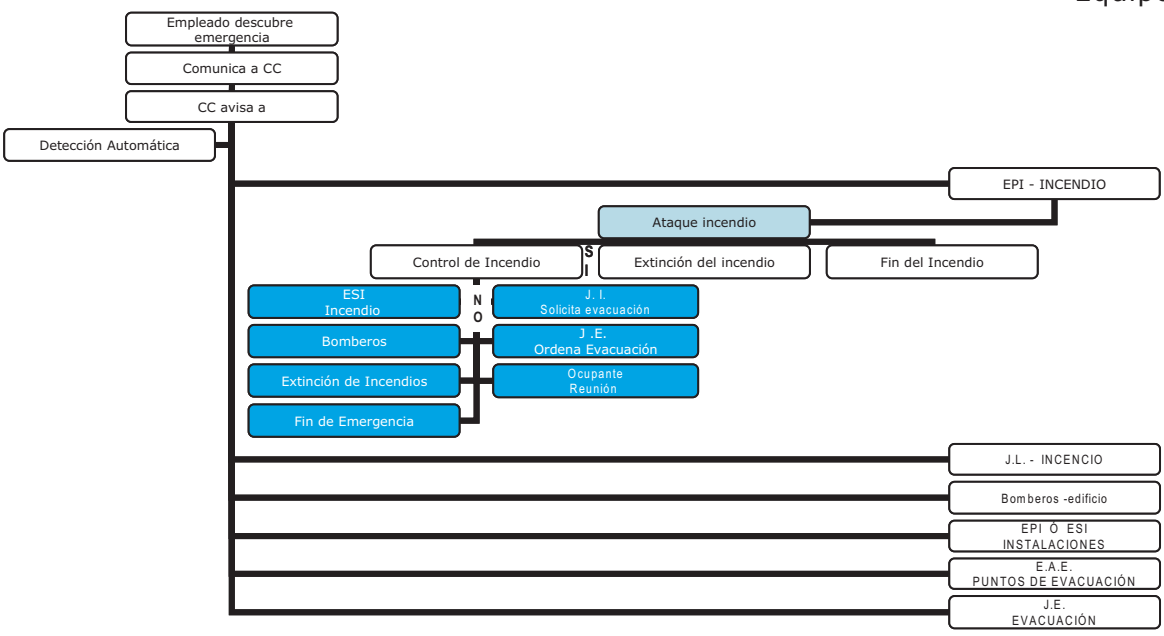
Se diseñarán esquemas operacionales con la secuencia de actuaciones a llevar a cabo en cada una de las acciones de los planes citados en función de la gravedad de la emergencia, el lugar, y el personal disponible para realizar tareas de autoprotección. Cuando la complejidad lo aconseje se elaborarán esquemas operacionales parciales.

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.

EQUIPOS DE EMERGENCIA

JEFE DE EMERGENCIA	JEFE DE INTERVENCIÓN
➢ Se sitúa en el punto de la Emergencia ➢ Máxima autoridad. ➢ Decide el momento de la evacuación ➢ Ordena investigación del accidente. ➢ Es permanentemente localizable.	➢ Se sitúa en el punto (escena) de la Emergencia. ➢ Informa al Jefe de Emergencia. ➢ Dirige las operaciones de reacción y respuesta.

Como ejemplo de esta aplicación veamos un esquema resumido de las actuaciones a llevar a cabo en una situación emergencia:



Fuente:
Técnicas de prevención de riesgos laborales: Seguridad- Plan de Autoporotección

¿Cree que su personal está preparado para prevenir situaciones imprevistas como incendios, inundaciones y terremotos?

Si su respuesta es NO...
Con una inversión de 26,00 USD,
PARTICIPE EN EL

CURSO IN COMPANY
BRIGADISTAS PARA MANEJO DE EMERGENCIAS

AGOSTO - SEPTIEMBRE OCTUBRE

ORGANIZA

FUNDACIÓN CONCEPTOS INTEGRADOS DE PROTECCION -IPC-

FUNDACIÓN IPC Integrated protection concepts
Creando Cultura de Seguridad

CISHT

CNCF Consejo Nacional de Capacitacion y Formacion Profesional