BOLETÍN INFORMATIVO

CEAS MÉXICO

AÑO VI NÚMERO 3

JULIO - SEPTIEMBRE 2019

CONTENIDO

I. ACTIVIDADES DE CEAS MÉXICO

Curso de Formación de Monitoristas para Seguridad en Videovigilancia, nivel I (FOMVI I)

Del 23 de Septiembre al 3 de Octubre se impartió el curso del Nivel I del programa de Formación de Monitoristas para Seguridad en Videovigilancia (FOMVI I), al personal de la empresa DIMAC en Manzanillo, Colima.

Foro "Análisis y Prospectivas de la Seguridad Privada en México"

El viernes 27 de Septiembre se realizó el Foro "Análisis y Prospectivas de la Seguridad Privada en México", organizado por la Comisión de Defensa Nacional del Senado de la República, con la colaboración de la Confederación Nacional de Empresarios de Seguridad y Similares de las Empresas del Ramo (CONESPRYSIR) y CEAS México.

Taller de Manejo de Situaciones de Emergencia

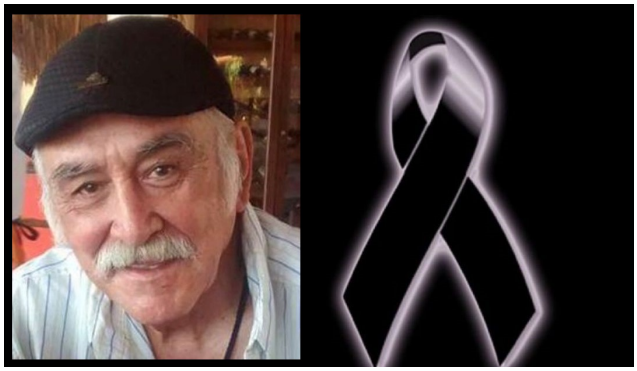
El domingo 08 de Septiembre se impartió el Taller de Manejo de Situaciones de Emergencia al personal de la empresa SAMAHE.

Conferencia “Seguridad y Sociedad” en la Gran Logia de Tamaulipas

El sábado 31 de Agosto se impartió la Conferencia-Debate “Seguridad y Sociedad”, en la Gran Logia de Tamaulipas, en Tampico, Tamaulipas.

In Memoriam Felipe Victoria Zepeda

El lunes 19 de Agosto falleció el destacado escritor y periodista Felipe Victoria Zepeda, Delegado de CEAS México en la ciudad y Puerto de Acapulco, en el Estado de Guerrero.



Conferencia “Panorama y Perspectivas de la Seguridad Privada en Mexico” con el Grupo María Luisa

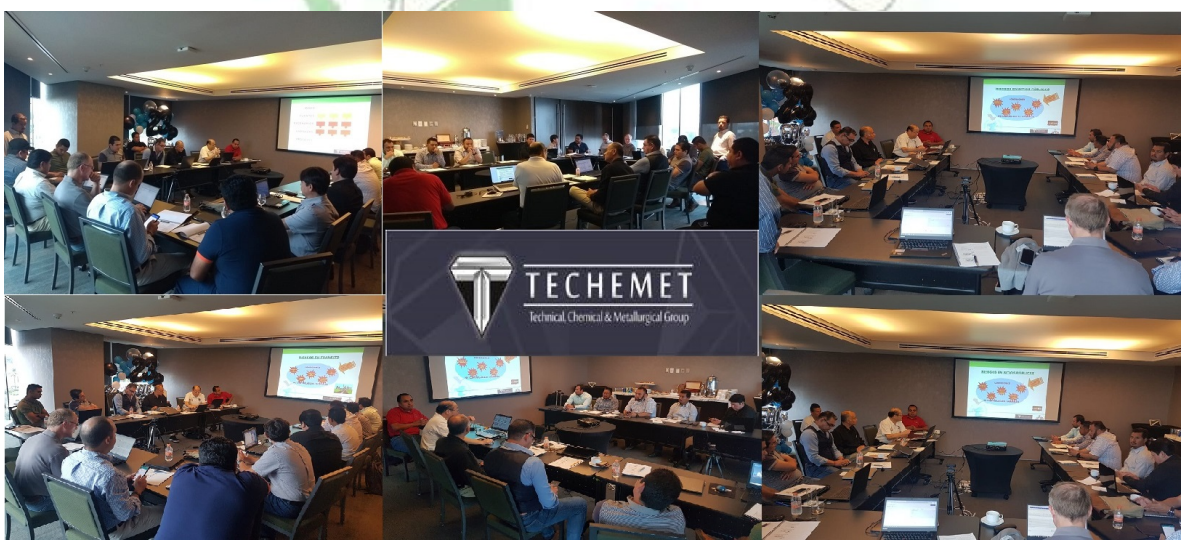
El viernes 16 de Agosto se impartió la Conferencia-Debate “Panorama y Perspectivas de la Seguridad Privada en México”, con el Grupo María Luisa, en la Ciudad de México.

Formación de Monitoristas para Seguridad en Geolocalización, nivel I (FORMOS I)

Del lunes 05 al viernes 09 de Agosto se impartió el nivel I del Programa de Formación de Monitoristas para Seguridad en Geolocalización (FORMOS I), para el personal de las empresas Especializados SAGOT, Farmacias Nacionales, Grupo SILA y TRACSA, organizado por Grupo SABE Consultores.

TALLER DE SEGURIDAD PERSONAL

El viernes 12 de Julio se impartió el TALLER DE SEGURIDAD PERSONAL, al personal de Mandos Medios de la empresa TECHEMET en Guadalajara, Jalisco.



II. EVENTOS DE CEAS MÉXICO

FECHA	CURSO	HORAS
4, 5, 6, 7 y 8 de Noviembre (*)	Formación de Monitoristas para Seguridad en Videovigilancia Nivel I (FOMVI I)	40
11, 12, 13, 14 y 15 de Noviembre (*)	Formación de Monitoristas para Seguridad en Geolocalización Nivel I (FORMOS I)	40
25, 26, 27 y 28 de Noviembre (*)	Formación de Mandos Operativos para Servicios de Seguridad (FORMAN) 1) Supervisión de Servicios de Seguridad (SUPSEG) 2) Servicio y Calidad para Seguridad (SERCAL)	32
2, 3 y 4 de Diciembre (*)	Formación de Monitoristas para Seguridad en Videovigilancia Nivel II (FOMVI II) / Centro Integrado de Mando y Asistencia para Servicios de Videovigilancia (CIMA/SVV)	24
9, 10 y 11 de Diciembre (*)	Formación de Monitoristas para Seguridad en Geolocalización Nivel II (FORMOS I) / Centro Integrado de Mando y Asistencia para Servicios de Geolocalización (CIMA/SGL)	24
5, 6, 11 y 12 de Diciembre (*)	Administración de Servicios de Seguridad (ASES)	32

(*) Este programa esta disponible para asistir a través de nuestra PILAR (Plataforma Interactiva en Línea para Asistencia Remota)

ESTOS CURSOS SE IMPARTEN EN COORDINACIÓN CON GRUPO SABE CONSULTORES. PARA MAYORES INFORMES, COMUNICARSE A LOS TELEFONOS (55) 5530-3336 Y (55) 5530-8712

III. PUBLICACIONES CEAS MÉXICO

CIBERSEGURIDAD PERSONAL, ¿QUIÉN ES EL ENEMIGO MÁS PELIGROSO?

La tecnología que antaño era de ciencia ficción, hoy se ha convertido en algo cotidiano. El reloj radioteléfono de Dick Tracy en las tiras cómicas de los años 30 del siglo pasado, hoy está en manos de casi todos, niños inclusive, con los teléfonos móviles. La tecnología no sólo ya está aquí, sino que se ha convertido en algo fundamental que nos da nuevas facilidades y comodidades de vida, pero también nuevas vulnerabilidades … y riesgos.

Las muy amplias y diversas facilidades y comodidades de conocimiento y comunicación disponibles en esta "*era de la información*" han alcanzado el nivel personal. Gracias al Internet de última generación, con tecnologías de 3G, 4G y próximamente 5G, y a dispositivos como computadoras personales, *tablets* y *smartphones*, de manera cotidiano estamos inmersos en un mar de manejo e intercambio de información de todo tipo, de negocio, de estudios, de entretenimiento … y de índole personal. Pero este mundo de ventajas también tiene un lado obscuro, y es la posibilidad de robo o simple acceso no autorizado a dicha información que pueda ser usado contra nuestros propios intereses o de alguien más.

Desde un punto de vista de seguridad, poner información "*en la Red*", en cualquier forma, ya sea desde una simple conversación o el intercambio de mensajes vía *SMS* o *Whatsapp*, el almacenamiento en "*la nube*", o la publicación en redes sociales, equivale a, usando una metáfora deportiva, "*poner un balón en el aire*", con lo cual, parafraseando a un conocido locutor deportivo "*pueden pasar tres cosas y dos de ellas son malas*", ya que puede ser que llegue a su destino, lo bueno, o que no llegue, lo malo, o que sea interceptado para ser usado de manera adversa, lo peor. Por ello es conveniente adoptar algunas medidas adicionales de protección, a pesar de que existan mecanismos de seguridad disponibles *per se* en los medios y dispositivos de acceso a Internet.

En general, los mecanismos de seguridad disponibles en los dispositivos de acceso, medios de comunicación y sitios en la Red suelen tener una efectividad razonable, pero al mismo tiempo, al ser ampliamente conocidos puede ser vulnerados, bajo el principio de que "*todo lo que la tecnología puede hacer, la misma u otra tecnología lo puede deshacer*", de tal suerte que no podrán detener a alguien interesado con la decisión y recursos para lograrlo, como es el caso de los *hackers*, aunque ante la cada día mayor complejidad y sofisticación de estos

mecanismos de seguridad, se puede pensar que se requiere de grandes inversiones y capacidades para ello, que sólo estarían al alcance de organizaciones o personas con gran solvencia económica que no tendrían interés en "*simples*" personas de poca relevancia.

Sin embargo, esto ya no es totalmente exacto, porque toda persona siempre tiene alguna forma de relevancia, tan solo por el hecho de tener algo que alguien más no tiene, por lo que deja de ser "*simple*", de tal manera que la ciberseguridad no debe ser exclusiva de los grandes corporativos, sino que se debe considerar como una cuestión a nivel personal. Y en este contexto, el problema crucial es que, aun cuando los mecanismos de seguridad fuesen muy efectivos, la mayor fuente de riesgo se ubica fuera de ellos, y es capaz de vulnerar aún el más complejo y sofisticado de estos mecanismos. Y para identificar a esta amenaza, no hay más que dirigir nuestros pasos y mirar en el espejo más próximo. Nosotros mismos que damos esa "*ocasión que hace al ladrón*".

Nosotros mismos somos nuestra mayor amenaza, porque anulamos la efectividad de los mecanismos de seguridad al ingresar a sitios no seguros en la Red atraídos por la curiosidad o el morbo de una oferta atractiva de alguna clase, respondemos a correos y mensajes que nos prometen ganancias fáciles motivados por nuestra propia avaricia, aceptando a desconocidos y publicamos toda clase de información personal incluso íntima, en las redes sociales, propias o ajenas, para satisfacer nuestra propia vanidad. Sin caer en cuenta que con ello proporcionamos información muy valiosa para una gran diversidad de posibles agresores, que llegan a conocer nuestros hábitos, intereses, conductas, fragilidades y debilidades.

Los agresores en la actualidad no necesitan ser tan sofisticados, ni requieren de complejos y costosos equipos de intercepción y vigilancia electrónica. Sólo tienen que ser dedicados y meticulosos explorando esa gran cantidad de información que nosotros mismos ponemos en la Red. Así pueden conocer los nombres, edades y ocupaciones de familiares y amigos, para las extorsiones telefónicas, las fechas de ausencias para los robos a casa-habitación, los perfiles y tendencias de intereses para los fraudes por correo electrónico, imágenes que pueden ser editadas y reproducidas, fechas de nacimientos y bodas, o nombres de mascotas, usadas como contraseña en correos o cuentas bancarias. Nosotros mismos exhibimos nuestras debilidades, vulnerabilidades y formas y momentos de exposición.

La ciberseguridad personal no necesariamente requiere de mecanismos de seguridad complejos, sofisticados … y costosos. La clave del éxito reside más en anular al enemigo más peligroso, nosotros mismos, no combatiendo sino dificultando, o al menos no facilitando los esfuerzos de posibles agresores. Y no se trata de aislarse del mundo. Eso no es posible en la actualidad. Se trata de

detenerse un momento y pensar. Pensar que a todo aquel con quien me vinculo en redes sociales, es un canal de difusión de mi información, que no se podrá controlar. Pensar quién podría conocer el dato, fecha o nombre, que usaré como contraseña. Pensar que cada pieza de información que colocamos en la Red, aún en espacios restringidos, es un "*balón en el aire*", que no tenemos la certeza dónde acabará.

Las perspectivas de éxito de cualquier mecanismo de ciberseguridad, en particular a nivel personal, están determinadas en mayor medida por la confianza y la confiabilidad de las personas, que por la tecnología. Porque una persona, incluso de nuestro círculo más cercano, puede ser de confianza, pero no confiable por ser indiscreto, o bien puede ser confiable, pero no de confianza porque tiene intereses propios no coincidentes con los nuestros. En este contexto, vale la pena pensar, parafraseando a un célebre conductor de un noticiero nocturno, ¿sabe usted que están haciendo sus hijos con su computadora o su celular?

El buen juez por su casa empieza

... CUANDO LOS SEGUNDOS CUENTAN

¿Cómo funciona la atención de Emergencias?

Para resolver un problema se necesita saber que hay un problema, de qué se trata, y tener la capacidad para resolverlo. La atención de Emergencias es un proceso de solución de problemas, pero con perspectivas de pérdidas inminentes, incluso vidas, lo que plantea una exigencia de rapidez en dicha atención … porque los segundos cuentan.

PANORAMA

El proceso para la atención de Emergencias se puede describir por el acrónimo **CDAI**, ya que comprende lo siguiente:

- ***C*aptación** de los hechos que ocurren en un entorno.
- ***D*etección** de una situación de Emergencia en los hechos captados.
- ***A*lertamiento** a las corporaciones pertinentes para atender el tipo de Emergencia detectada.
- ***I*ntervención** de las corporaciones alertadas para atender la Emergencia detectada.

De tal suerte que las posibilidades de éxito dependerán de que:

1. Se capten hechos en los que se pueden presentar o no una situación de emergencia, y se entreguen a quien pueda detectarla con certeza razonable.
2. Dentro de los hechos captados, se detecte la presencia de una situación de Emergencia.
3. Se emita un alertamiento a las corporaciones pertinentes para atender el tipo de Emergencia detectada.
4. Las corporaciones alertadas dispongan de la capacidad para atender la Emergencia detectada.

Todo ello en un marco de tiempo en el que sea posible evitar, detener e incluso revertir los daños o pérdidas.

En un contexto comunitario la captación de los hechos suele realizarse a través de los sistemas de vigilancia, como las alarmas o botones de pánico, la geolocalización o la videovigilancia, y de las personas presentes en el entorno en que ocurren.

Donde la "*capacidad de captación*" en el primer caso está determinada por el "*campo de cobertura*" de los dispositivos de los sistemas, y en el segundo caso, de que las personas presentes se percaten de los hechos, y que dispongan de algún medio de comunicación a una instancia con la capacidad de valorarlos, como puede ser el servicio telefónico 9-1-1.

Asimismo, la detección y el alertamiento suelen ser responsabilidad de los Centros de Atención de Emergencias (**CAE**), como los C2, C4 y C5, que cuentan con personal capacitado para valorar los hechos captados y detectar, con certeza razonable, una situación de Emergencia, tipificarla, y emitir el alertamiento a las corporaciones pertinentes para su atención. Donde la "*capacidad de detección y alertamiento*" está determinada principalmente por la cantidad y competencia (conocimientos, destrezas, habilidades y criterios) del personal operativo en estos Centros.

Finalmente, la intervención la realizan las corporaciones de asistencia, ya sean institucionales de policía o seguridad pública en general, las fuerzas armadas, protección civil, rescate y urgencias médicas, o privadas de naturaleza especializada, hidráulicas, eléctricas, de gas, ductos de combustible o salvaguarda nuclear. Donde la "*capacidad de intervención*" está determinada por la cantidad de recursos disponibles en las corporaciones alertadas, al momento de ocurrencia de una situación de Emergencia.

PERSPECTIVA

La atención de Emergencias, como cualquier otra actividad en un contexto social, enfrenta un problema de "*administración de recursos escasos*", en forma de perfiles **CDI,** de **Carencias** (*NO hay*), **Deficiencias** (*NO es lo adecuado*) e **Insuficiencias** (NO es suficiente). Problema que acota y compromete el potencial de efectividad operativa, y por ende las posibilidades de éxito. Algunos de estos factores, de manera enunciativa más no limitativa, son los siguientes:

Captación

1. Las capacidades y limitaciones funcionales de los dispositivos de los sistemas de vigilancia, en particular su afinidad con la forma física de los hechos que ocurren, por ejemplo, una cámara no puede captar una fuga de gas, y un sensor de gas no puede captar la maniobra de un carterista. Y un botón de pánico no se activa solo.
2. El campo de cobertura de los dispositivos de los sistemas de vigilancia, o el alcance de detección sensorial de las personas, por ejemplo, una cámara no puede captar lo que ocurre fuera de su campo visual, y una persona no puede ver lo que ocurre a su espalda, ni escuchar si tiene problemas auditivos.

3. La disponibilidad de medios de comunicación, así como el desconocimiento de las personas con quién o a dónde reportar los hechos, o bien su incapacidad para comunicarse, por ejemplo, discapacitados verbales o extranjeros con desconocimiento del idioma local.

Detección y Alertamiento

1. Saturación de información, por la concurrencia de múltiples hechos captados y entregados al **CAE**, por ejemplo, los mosaicos de más de 16 o 32 imágenes, o las llamadas del servicio telefónico 9-1-1, con un porcentaje superior al 60% de casos no procedentes, que dificultan la detección oportuna de situaciones de Emergencia.
2. Imprecisión de la información, por malfuncionamiento de los dispositivos de los sistemas de vigilancia, o limitaciones de expresión en las personas a través del servicio telefónico 9-1-1, por encontrarse en estado de conmoción y alteración emocional.
3. El perfil **CDI** en las competencias del personal operativo, para detectar situaciones de Emergencia, inmersas y mimetizadas en el cúmulo de hechos captados, así como seleccionar las corporaciones pertinentes para atender cada tipo de situación, y emitirles el alertamiento correspondiente.

Intervención

1. El perfil **CDI** de los recursos operativos de la corporación en el momento de recibir el alertamiento para atender una Emergencia, específicamente, el número de vehículos y elementos, disponibles para acudir con oportunidad al sitio de ocurrencia.
2. El sentido de obligatoriedad y nivel de prioridad asignada por la corporación a los alertamientos recibidos desde el **CAE**, es decir, si se considera obligado o no, y que tanta prioridad le da a dichos alertamientos.

CONCLUSIÓN

La atención de Emergencias es una cadena de trabajo de equipo, donde la falla de un eslabón hace fallar todo el proceso. Donde el recurso humano es el factor crucial, y en el que no valen los protagonismos individuales, sino el resultado final, sometido a falsas expectativas y generalizaciones, con el **CAE** como el componente más visible ante la ciudadanía. Un proceso sin héroes o aplausos, sólo pérdidas y por ello de villanos y culpables. De profesionales en las sombras, haciendo el mejor de los esfuerzos para atender con la mayor rapidez posible, porque saben que para preservar una vida … **los segundos cuentan**.

IV. NOVEDADES DE CEAS MÉXICO

PROGRAMAS CEAS MÉXICO

1. Se abre la posibilidad de participar en los cursos de los programas de CEAS México, a través de la **Plataforma Interactiva en Linea para Asistencia Remota (PILAR)**, cuando no sea posible trasladarse físicamente a la sede presencial.

2. Asimismo, se abre la posibilidad de efectuar pagos por medio de Tarjetas de Crédito y del sistema de pagos Paypal.

3. Para los programas n contemplados en el calendario de cursos abiertos, se podrán abrir grupos si existe un mínimo de 10 interesados, que podrán solicitar su registro por correo electrónico.

4. En todos los programas para profesionales se han integrando lineamientos para una eventual comparecencia ante las autoridades bajo la normatividad del Sistema de Justicia Penal Acusatorio, en virtud de que existe la posibilidad de que cualquier persona, incluso de un centro de monitoreo, pueda ser convocado como testigo.

5. En el programa de **Formación Básica de Oficiales de Seguridad** (**FOBOS**) se han integrado lineamientos para actuar como Auxiliar de Primer Respondiente en las tres modalidades. Adicionalmente para la modalidad de Protección de Instalaciones (Intramuros), su versión para la Ciudad de México y la versión de **Logistica de Seguridad** para Eventos, se han integrado lineamientos para el manejo de **Personas con Limitaciones de Movilidad**, así como para el manejo de **Personas con Discapacidad en emergencias**, de acuerdo a la norma **NOM-008-SEGOB-2015**. Y en la modalidad para seguridad pública se han integrado los lineamientos para actuación como **Primer Respondiente**.

6. En los programas de **Formación de Monitoristas para Seguridad** de todas las modalidades, Sistemas de Alarmas (**FOMSA**), Geolocalización (**FORMOS**) y Videovigilancia (**FOMVI**) se ha conformado una versión Intensiva para la modalidad de cursos dedicados, con una reconfiguración de las sesiones para reducir el tiempo presencial y facilitar el manejo de turnos del personal que asiste al curso.

7. En el nivel II del programa de Formación de Monitoristas para Seguridad (**FORMOS II**) se ha reorientado la temática hacia la afinación y mejora de las capacidades de observación y detección de riesgos.

Suscríbase a nuestro canal en Youtube http://www.youtube.com/user/ceasmexico/ y conozca nuestra Presentación Institucional https://www.youtube.com/watch?v=rwpZMXsK6gg , así como nuestro material de divulgación

Conozca más de nosotros visitando nuestra página web en www.ceasmexico.org.mx