SEGURIDAD
SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA

Foro 2019 SEGURIDAD DE INSTALACIONES VITALES

PROTECCIÓN FEDERAL

El pasado 25 de julio se llevó a cabo en el Casino Naval de la Ciudad de México, el **Foro Internacional "Seguridad de Instalaciones Vitales"** organizado por el Servicio de Protección Federal cuyo objetivo fue intercambiar mejores prácticas en materia de seguridad y protección de instalaciones y personas. En este magno evento participó la representación de 16 países, directivos de seguridad de 72 dependencias federales y estatales, 35 representantes de empresas con actividades relacionadas con el desarrollo nacional en materia de protección, así como Presidentes de las principales asociaciones de seguridad privada en México.

La inauguración fue encabezada por el Secretario de Seguridad y Protección Ciudadana, Dr. Francisco Alfonso Durazo Montaño, asistido por el Subsecretario de Seguridad Pública Mtro. Ricardo Mejía Berdeja, el Comisionado del Servicio de Protección Federal el Lic. José Pedro Vizuet Bocanegra y acompañado por el Director General de Departamento de Seguridad de Naciones Unidas (UNDSS) el Dr. Ricardo Aníbal Salas, Excelentísimo Embajador Sr. Aníbal Enrique Quiñonez Abarca, Representante de la Organización de los Estados Americanos (OEA) en México y el Presidente de ASIS Capítulo México, Lic. Pedro Alberto Sanabria Serrano.

El Doctor Durazo Montaño manifestó la importancia del intercambio de experiencias y mejores prácticas internacionales para implementar un mejor sistema de seguridad integral en Instalaciones vitales, primordial para el mantenimiento del orden público y la gobernabilidad del País. Resaltando la labor del Servicio de Protección Federal, ya que en 10 años de existencia se consolidó como referente nacional por su efectividad y profesionalismo en la protección de instalaciones vitales y gubernamentales, así mismo refirió que la seguridad pública debe de ser neutral, trabajando todas las fuerzas públicas y privadas por la paz y tranquilidad de los mexicanos, aportando todos los esfuerzos al cumplimiento de esta tarea.

Panelistas del Foro

El evento contó con la participación de reconocidos especialistas en la materia protección y seguridad:

1. Dr. Ricardo Aníbal Salas, Director General de Departamento de Seguridad de Naciones Unidas (UNDSS).
2. Luis Ochagavia Sánchez, Consejero de Interior de la Embajada de España en México.
3. Andy Hancock, Capitán de Navío de la Marina Real de Inglaterra.
4. Mtro. Luis Mateos, Representante de la Embajada Británica en México.
5. Royi Biller, Ex Mayor del Ejército Israelí y Representante de la Embajada del Estado de Israel en México.
6. Kandy Takahashi, Agregado de Policía en la Embajada de Brasil en México.
7. Richard "Kris" Cline Director Adjunto en Jefe del Servicio de Protección Federal de los Estados Unidos.
8. Lindsey E. Blair, Directora de Asuntos Intergubernamentales y Jeff Levine, Agente Especial adscritos a la misma dependencia norteamericana.
9. Ing. Francisco Urdaz, Especialista en Telecomunicaciones en Proyectos de Seguridad para Latinoamérica.
10. Ing. Enrique Guevara Ortiz, Director General del Centro Nacional de Prevención de Desastres (CENAPRED) de la Secretaría de Seguridad y Protección Ciudadana..

Dirección General de Profesionalización

En esta tercera edición del Foro Internacional, se sumaron más de 700 directivos y responsables de seguridad de Dependencias del Gobierno Federal, así como de algunos Estados de la República Mexicana, los que participan en este intercambio de ideas y experiencias por parte de destacados panelistas, cuyo propósito ha sido el dar a conocer la problemática que han enfrentado en la implementación de estrategias de seguridad en esta materia en sus países u organizaciones, así como las acciones que han llevado a cabo para resolverla con éxito.

El Foro Internacional ha permitido a los asistentes, conocer experiencias en materia de seguridad física de instalaciones, análisis de riesgos, ciber seguridad, tecnología, protección a funcionarios, regulación en la materia así como de esquemas de prevención de actos terroristas.

Las exposiciones y debates se dieron en torno a los siguientes temas:

1. Introducción al Sistema de Evaluación de Riesgos para la Seguridad y Protección de Instalaciones Estratégicas.

El Dr. Ricardo Aníbal Salas, Director General de Departamento de Seguridad de Naciones Unidas (UNDSS), integrante activo al servicio por 23 años en el Ejército de la República de Argentina, ha participado en Operaciones de Paz con la ONU, así mismo, desarrolló proyectos en materia de Seguridad y Protección en corporaciones privadas de alto reconocimiento en Argentina y Latinoamérica, refirió experiencias de las Naciones Unidas en la protección de la infraestructura crítica en los países donde se encuentran las más de 5,000 instalaciones de dicho organismo; el reto que implica brindar seguridad a los funcionarios y asistentes a sus sedes, en países incluso, en situaciones de conflicto. El desafío en materia de seguridad y protección es mayúsculo, toda vez que Naciones Unidas no puede mantener un esquema prohibicionista en sus controles de acceso, por el contrario, debe encargarse de establecer sistemas de seguridad que permitan el libre acceso de las personas al organismo, sin vulnerar las condiciones sociales o culturales, por lo que las medidas que sean implementadas deben ser las adecuadas de conformidad con las características de las regiones.

El Dr. Salas destacó la importancia de contar con un modelo de análisis de riesgo que permita mitigar los peligros asociados a las principales amenazas a los que se encuentran expuestos. En el caso de ONU son 5 las amenazas en las cuales se centran sus estrategias con el objeto de ser más efectivos, toda vez que si se dejará a la libre determinación del especialista, podrían ser muchas más las que se señalaran y dispersar la atención a las que podrían causar un mayor efecto en caso de llegar a materializarse. Resaltó la importancia de contar con opciones de mitigación que sean aptas, factibles y aceptables, ya que si bien el especialista de seguridad puede pensar en muchas que pudieran estar a su alcance, no todas cubren estos tres elementos, mismos que son indispensables tomar en cuenta. Finalmente, destacó que el factor humano es el elemento primordial de un sistema integral de seguridad, por ello la trascendencia de contar con personal capacitado.

2. La Protección de Infraestructuras Críticas en España.

Ponencia impartida por Luis Ochagavía Sánchez, Consejero del Interior de la Embajada de España en México, quien además es Comisario Principal de la Policía Nacional, destacó el avance en la legislación española en materia de protección de infraestructura crítica y de seguridad privada. Inició su participación puntualizando que la protección de la infraestructura crítica es un tema de gran importancia no sólo para España, sino para toda la Comunidad Europea, ya que están conscientes del daño o impacto que podría causar a la Comunidad si alguna de éstas fuese dañada mal intencionadamente.

Refirió que cada Estado miembro de la Comunidad Europea puede definir cuáles son sus infraestructuras críticas teniendo en cuenta los efectos cualitativos y cuantitativos que su interrupción o destrucción supondría, considerando como mínimo los siguientes aspectos:

- El área geográfica que podría resultar afectada por su pérdida o su indisponibilidad;
- La cantidad de población afectada;
- La importancia de las pérdidas económicas y/o degradación de los productos o servicios;
- El efecto medioambiental;
- Los efectos políticos;
- Los efectos psicológicos; y
- Las consecuencias para la salud pública.

Manifestó que conforme a los criterios anteriores es que se desarrollan, definen y aprueban instrumentos de planificación y protección nacional de infraestructuras críticas, a fin de designar a los operadores críticos, estableciéndoles sus objetivos y marcos de actuación.

En la definición de los actores de la protección intervienen los Ministerios y Organismos, las Delegaciones de Gobierno y las comunidades autónomas para conformar la Comisión Nacional para la Protección de las Infraestructuras Críticas, la cual detenta como parte de sus funciones: aprobar los Planes Estratégicos Sectoriales, designar a los operadores críticos y los marcos de actuación. En este sentido, los instrumentos de planificación se operan conforme al proceso de seguridad de las instalaciones.

3. Enfoque Británico para la Protección de la Infraestructura Nacional Crítica.

Andy Hancock, Capitán de Navío de la Marina Real de Inglaterra, en su conferencia destacó que la organización y la arquitectura del Reino Unido en materia de protección de infraestructura crítica se basa en la participación de autoridades de la Secretaría de Gobernación, el Centro de Protección de Infraestructura Nacional, la Secretaría de Contingencias Civiles, el Consejo Nacional de Seguridad (Amenazas, Riesgos, Resiliencia y Contingencias), el Ministerio Interior, la Oficina de Seguridad y Contra Terrorismo y la Policía.

En la implementación de protección a instalaciones vitales o infraestructura de seguridad, se establecen tres estrategias:

- Estrategia de Seguridad Nacional.
- Evaluación de Riesgos Nacionales.
- Estrategia Contra Terrorismo.

Aunado a que la Infraestructura Nacional considera como elementos críticos a los activos, instalaciones, sistemas, redes o procesos que en cuya pérdida puede generar un impacto perjudicial importante en la disponibilidad, integridad o prestación de servicios esenciales, incluidos aquellos servicios cuya estructura, de ser comprometida, podría resultar en una pérdida relevante de vidas o bien de víctimas, tomando en cuenta repercusiones económicas o sociales significativos; y/o un perjuicio grave en la Seguridad Nacional, Defensa Nacional o bien el funcionamiento del Estado.

Las amenazas de Seguridad Nacional incluyen:

- Terrorismo.
- Espionaje.
- Seguridad cibernética.
- Armas de Destrucción Masiva.

En la actualidad, se desarrollan diversas acciones para alcanzar la seguridad física, del personal, de los ciudadanos y cibernética, entre las que desatacan la detección de armas de amenaza, rastreo y monitoreo de intrusos y otras amenazas semejantes, el acceso a los sistemas de control y bloqueo, así como barreras físicas y activas que permiten negar o retrasar el progreso de adversarios, con la finalidad primordial de proteger a la población o activos del efecto de explosiones o ataques balísticos, para salvaguardar contra o limitar la propagación de material químico/biológico/radiológico o activos sensibles.

4. Confianza digital para proteger la infraestructura crítica.

Conferencia desarrollada por el Mtro. Luis Mateos Representante de la Embajada Británica en México; quien destacó el incremento exponencial de los sistemas digitales en el mundo, por ello el aumento en el manejo de instrumentos tecnológicos para la interconexión inalámbrica de dispositivos electrónicos. Este aumento debe ser proporcional a la obligación del estado y de los proveedores de estos servicios de ofrecer a los ciudadanos confianza y seguridad en el manejo de clases de dispositivos y de sus datos personales. Resaltó de manera especial el hecho de que en la actualidad "la información" es un activo crítico cuya protección debe ser garantizada y analizada, tanto por el gobierno como por los particulares, fundamentalmente si se trata de dependencias que tienen a cargo temas de seguridad nacional o pública.

Manifestó que las organizaciones deben enfocar su éxito en la Ciberseguridad conforme a la interacción entre la tecnología, los procesos y las personas, con el objetivo primordial de atender los riesgos sectoriales, la protección de los activos críticos y responder a los incidentes para no perder la confianza de los usuarios, pérdidas de operación, financieras o de reputación.

Refirió que la confianza digital debe ser holística, extendida, continuada y adelantada al futuro.

5. Inteligencia proactiva de ciberseguridad.

Ponencia desarrollada por el Ex Mayor del Ejército Israelí Royi Biller y Representante de la Embajada de Israel en México, quien expuso que todos los sistemas deben mantener una alerta temprana accionable, la cual debe proporcionar información para la toma de decisiones de la alta dirección en materia de seguridad, que nos permita dar respuesta a las interrogantes básicas de ¿quién?, ¿cuándo?, ¿cómo?, ¿en dónde? y ¿para qué?. Estos cuestionamientos deberán ser alimentados por las fuentes de inteligencia del Estado, con el objeto de prever probables riesgos a los sistemas de información.

Destacó que en la actualidad existen ataques a la seguridad que se presentan reiteradamente en publicaciones de páginas web maliciosas, envío y difusión de mensajes de phishing, cadena de ataque, que genera las fugas de información y la explotación de datos. La cadena de ataque en el caso de phishing, inicialmente se identifica con el blanco a explotar y analizar las posibilidades de ofensiva, posteriormente se efectúa el registro de dominio y el alta de servidor de correo (MX Record) y paquete hosting (A Record), para finalmente llevar la publicación maliciosa, el envío y difusión de mensajes de phishing.

6. Evaluación de Riesgos en Instalaciones Críticas.

La ponencia fue realizada por Richard “Kris” Cline y Lindsey E. Blair, Director Adjunto en Jefe y la Directora de Asuntos Intergubernamentales respectivamente, del Servicio de Protección Federal de los Estados Unidos, quienes expusieron que la función de la agencia federal de seguridad es proteger las instalaciones del gobierno de los EE. UU., empleados, contratistas y visitantes de dichas instalaciones. El Gobierno tiene la función de seguridad y protección de instalaciones estratégicas, la cual es otorgada bajo la aplicación de la ley al Secretario de Seguridad Nacional para la protección de propiedades públicas. Los servicios integrales que proporcionan principalmente son salvaguardar los servicios gubernamentales y a las comunidades en todos los estados y territorios de los Estados Unidos de Norteamérica, para lo cual realiza evaluaciones de seguridad en las instalaciones federales para identificar riesgos, el diseño, instalación y mantenimiento de contramedidas de seguridad, obteniendo datos que generan las condiciones que permiten mitigar las contingencias, y así proporcionar una respuesta inmediata y presencia visible en el cumplimiento de la Ley y en la supervisión a los guardias de seguridad que realizan el control de acceso e inspección de seguridad y verificaciones de antecedentes para empleados federales. Adicionalmente, se implementan investigaciones criminales, incluyendo amenazas a empleados e instalaciones federales y monitoreo de las alarmas de seguridad a través de centros de comunicación centralizados.

El proceso de gestión de riesgos ISC para instalaciones federales se realiza mediante un Estándar de Comité de Seguridad Interinstitucional que define los criterios y procesos que los responsables deben usar para determinar el nivel de seguridad de su instalación (FSL) y proporciona una fuente de contramedidas físicas para todas las instalaciones federales, este proceso debe aplicarse a todos los edificios e instalaciones en los Estados Unidos ocupados por empleados federales para actividades no militares.

Para la identificación de vulnerabilidades en la infraestructura federal, el FPS instauró un sistema a través de una página de internet de evaluación de seguridad de instalaciones, la cual se basa en una metodología de recopilación de datos a través de un conjunto de preguntas de evaluación, para el procesamiento de los datos a través de un algoritmo que determina las amenazas y vulnerabilidades, el cual emite un informe mediante el cual se establecen las medidas necesarias para mitigar las amenazas y vulnerabilidades.

Además, el Plan Nacional de Protección de Infraestructura establece un marco integral de administración de riesgos que define los roles y responsabilidades de protección de infraestructura crítica para el Departamento de Seguridad Nacional, Agencias Federales específicas del sector (SSA); y otros socios de seguridad federales, estatales, locales, tribales y del sector privado, aunado a que proporciona el enfoque coordinado que se utilizará para establecer las prioridades nacionales, los objetivos y los requisitos para la protección de la infraestructura, de modo que el financiamiento y los recursos se apliquen de la manera más efectiva.

7. Protección a la Infraestructura Crítica en Brasil.

Conferencia por Kandy Takahashi, Agregado de la Policía en la Embajada de Brasil en México, señaló que para el establecimiento de un sistema de protección y seguridad en Brasil, se analizan los instrumentos de estudio y planificación que permiten conocer el funcionamiento de la instalación, las vulnerabilidades que presenta, las consecuencias que podría traer su inactividad, así como las medidas estratégicas para su mantenimiento. En ese contexto, en Brasil consideran como infraestructura crítica a todas las instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción total o parcial, provoca un grave impacto social, ambiental, económico, político, internacional o de seguridad estatal o social.

La protección a la infraestructura crítica se define por las amenazas humanas, por desastres naturales o fallas en proyectos, por lo que la solución a estos problemas se determina mediante la implementación completa de políticas de seguridad y el balanceo de los dos extremos: riesgos limitados a niveles aceptables.

Destacó que Brasil fue el primer país sudamericano en implementar la política de protección de infraestructuras críticas, teniendo como precedente su aplicación en los Juegos Panamericanos de 2007, por lo que desde esa época se identificaron las partes más críticas de la industria de las telecomunicaciones para asignar de manera eficiente los recursos disponibles para la protección.

Aunado a lo anterior, mediante Decreto 6371 de febrero de 2008, se otorgó la asignación a la Cámara de Asuntos Exteriores, la Defensa Nacional y el Consejo de Gobierno como los responsables de definir la política de seguridad de la infraestructura crítica, la normativa interna y el sistema de gestión de estructura crítica, así como la unión de los sectores públicos y privados involucrados en la seguridad nacional, para minimizar los riesgos y el mapeo de vulnerabilidades.

8. Metodología de Riesgos en Instalaciones Críticas.

Ponencia desarrollada por el Sr. Jeff Levine, Agente Especial del Servicio de Protección Federal de los EUA, quien destacó que la seguridad de las instalaciones vitales es un tema de trascendencia que requiere de la participación de muchos actores, por lo que todas las organizaciones deben evaluar los riesgos de las instalaciones críticas, mediante una conciencia situacional para la identificación de activos críticos, con un enfoque operacional para identificar respuestas a incidentes y detección de la reducción de daño.

El proceso de evaluación de seguridad de instalaciones se basa en la recopilación de datos e investigación previa al sitio (detectando amenazas y vulnerabilidades de integración), en las visitas a la instalación y entrevistas, se elaboran y envían los informes para su aprobación. Este proceso es evaluado mediante la implementación de un calendario de organización interinstitucional, un portafolio de las instalaciones conforme a las restricciones regionales, geográficas y de tiempo, asignando una propuesta y determinación del nivel de seguridad de cada instalación, efectuando la investigación, análisis de riesgos y recopilación de datos, con la valoración de amenazas y de medidas de protección, identificando vulnerabilidades e integrando la conclusión del posible peligro, para formular los informes y el diseño, la ejecución, seguimiento y gestión de contramedidas, para mitigar los desafíos detectados.

La evaluación de medidas de protección sirve como una oportunidad para que el inspector y el agente especial observen y verifiquen la información recopilada durante la revisión inicial de la instalación.

9. Tecnología para la seguridad de infraestructura crítica.

Conferencia impartida por el Ing. Francisco Urdaz, quien es especialista en Telecomunicaciones y ha participado en el diseño e implementación de diversos proyectos de Seguridad para Latinoamérica, quien explicó que la concentración de personas en las principales ciudades del mundo, ha generado un punto crítico en la protección de la infraestructura, esto requiere que existan cada vez mejores sistemas de comunicación y datos.

Hizo mención de que la seguridad pública encuentra soporte en la tecnología inteligente, mediante una amplia gama de aplicaciones avanzadas que se encuentran en el mercado donde sus dispositivos móviles pueden ser conectados a centros de comando, y esto puede permitir brindar vigilancia predictiva, el mapeo de delitos en tiempo real, la vigilancia inteligente, optimización de respuesta a emergencias, cámaras con sujeción al cuerpo, sistemas de alerta temprana ante desastres, aplicaciones de alerta personal e inspecciones en edificios basadas en datos.

Un factor importante que refirió, es la administración de la información disponible, erradicando su aislamiento, sin precisión o repetida, que mantenga una gestión y flujo de trabajo, en correlación con otras fuentes, cuidando la cadena de custodia de la misión crítica.

10. Gestión Integral del Riesgo de Desastres.

Conferencia del Ing. Enrique Guevara Ortiz, Director General del Centro Nacional de Prevención de Desastres México (CENAPRED), desarrolló su ponencia relativa a la Gestión Integral del Riesgo de Desastres, manifestando que este tema nace de la evolución de la Protección Civil, la cual se dirige a la preparación y respuesta (reactiva), teniendo como objetivo evitar o disminuir el impacto de desastres (preventiva); con el objetivo de prever, reducir y controlar el riesgo de desastres (gestión integral del riesgo), siendo este último el proceso de planeación, participación, evaluación y toma de decisiones, basado en el conocimiento de los riesgos y su construcción social, que deriva en un modelo de intervención gubernamental y de la sociedad en su conjunto, para implementar políticas, estrategias y acciones. El fin último manifestó, es la previsión, reducción y control permanente del riesgo de desastre.

La gestión integral de riesgos reconoce que las contingencias no sólo son producto de las manifestaciones de la naturaleza o de las amenazas tecnológicas, sino producto de procesos, decisiones y acciones que derivan de los modelos de crecimiento económico y de desarrollo, así como a factores institucionales, culturales, sociales, políticos, económicos, ambientales, etc.

Señalando de manera importante que el riesgo de desastre es una condición latente y representa una probabilidad de daños y pérdidas en el futuro, que puede ser anticipada con acciones de prevención, mitigación y preparación, no debemos esperar que ocurra el desastre para actuar.

La identificación del riesgo de desastres se valora con tres componentes: el peligro, la vulnerabilidad y la exposición.

Dicho riesgo y de acuerdo a sus efectos, se atiende mediante gestión correctiva-prevención, reactiva-auxilio y prospectiva-previsión, de acuerdo a las causas y consecuencias que se presenten.

En conclusión, se señala que la seguridad depende de varios factores ubicación, entorno, estructura, personal, actividad, condiciones naturales, tecnológicas, humanas, destacando la importancia de su participación en la seguridad, resguardo y protección de instalaciones en el país, bajo esquemas definidos y homologados, la finalidad es promover el desarrollo, profesionalización y actualización de los profesionales del sector de la seguridad para fortalecer su actuación.

Dirección General de Profesionalización

Después de haber analizado las exposiciones y debates que se dieron acerca de la protección de instalaciones vitales podemos concluir que es necesario tener una rigurosa identificación de los riesgos e inseguridades, su alineación con la propia seguridad corporativa o institucional, que las instalaciones del gobierno federal cuenten invaluablemente con una evaluación de riesgos, cuyo resultado nos permita definir un plan de seguridad que atienda las necesidades de una dependencia, el cual debe definir claramente la relación que debe existir entre personas de seguridad, tecnología, protocolos, procedimientos y planes de resiliencia para en su caso, sobreponer la operación de la institución en caso de alguna crisis. Esto permitirá al Estado Mexicano mantener la operación de sus instituciones y la prestación de sus servicios a los ciudadanos.

Agradecemos la colaboración de nuestros patrocinadores:

IPS · Multiproseg · ASIS International Capítulo México 217 · tiLatina · Corporativo Almaba · Seguridad Privada · MOSEG · Embajada Británica en México · SEGMAN Detection Technologies · Motorola Solutions

Dirección General de Profesionalización