Continuamos desarrollando conceptos acerca de las certificaciones internacionales a las que puede acceder un profesional de la seguridad, revalidando sus conocimientos. En esta oportunidad, les ofrecemos un examen tipo para certificar PSP.

Examen de competencias

José María Piscione
Chairman 2011 Capítulo ASIS 215
jmpiscione@cepi.com.ar

Desde hace varios números venimos desarrollando la temática necesaria para que el profesional de la seguridad tenga un cabal conocimiento de las certificaciones internacionales de Asis, así como de los diferentes puntos de interés que constituyen parte del aprendizaje del profesional.

ASIS Argentina otorgará **media beca** para el curso PSP de 85 horas que comienza el 5 de marzo de 2012 a aquellos lectores que aprueben el examen incluido en esta edición. Les solicitamos enviar sus consultas sobre el programa y el resultado a *info@cepi.com.ar*

Programa de Protección Física para Profesionales de la Seguridad

• **Fundamentos:** La Seguridad Física como un sistema de contramedidas tangibles, diseñado para proteger a las personas y a los activos físicos, lógicos, y operacionales de una organización, de amenazas identificadas, debe cumplir con una serie de requisitos crecientemente exigentes y soportados por estándares y mejores prácticas para acompañar las prácticas diligentes de gobernancia corporativa.

Si se puede acceder físicamente a un sistema de computación, podrá obtener de un modo u otro, acceso lógico a la información que contiene, no limitada al centro de cómputos, sino que diseminada por la organización. Lo mismo sucede con el conocimiento y las personas que trabajan en la organización y con los datos y la información que se involucran en los procesos: resulta necesario asegurar su protección, y la información más allá de sus estaciones de trabajo.

Dominar los principios, procesos y tecnologías de protección física que controlen la seguridad de las personas y bienes de la organización; el acceso a la organización, las estaciones de trabajo, salas de servidores, áreas restringidas, áreas administrativas y operativas para aplicar a las necesidades ,adaptando las estrategias a los requerimientos del ámbito tecnológico, social y cultural.

Un atacante puede emplear tanto medios electrónicos como físicos para ganar acceso a información, por lo que las salvaguardas lógicas y físicas deben interoperar para ayudar a la organización a gerenciar el riesgo. Actualmente pueden operar salvaguardas de ambas disciplinas, las de seguridad lógica y las de seguridad física en conjunto, con una creciente convergencia, comunicando y compartiendo datos que dan respuestas alineadas a los requerimientos de gobernancia, procesos, gente y tecnología de maneras más costo-efectivas para un nivel de seguridad incrementado.

• **Misión del Curso:** Brindar los conocimientos técnicos, prácticos y de fundamentación teórica al nivel de requerimientos correspondientes a las mejores prácticas profesionales en seguridad y exigibles para demostrar competencias a nivel gerencial, necesarios para manejar efectivamente los conceptos básicos de la protección física de las personas, bienes tangibles e intangibles de la organización en todas sus formas; y conocer los criterios, métodos, tecnologías y las aplicaciones prácticas mediante una metodología de alto nivel aplicado a ese cuerpo de conocimientos.

• **Objetivos:** Finalizado el curso, los asistentes deberán poder manejar estrategias, tácticas, conocer y poder referenciarse en forma actualizada a los distintos componentes de un Plan Seguridad Física.

• **Metodología procedimental:** El curso PSP se desarrollará en 85 horas cátedra distribuidas en 17 clases semanales de 5 horas cátedra cada una, los días lunes en el horario de 8.30 a 13.30, comenzando el primer lunes de marzo. Se entregará diplomas de certificación a los asistentes y certificación adicional de competencias adquiridas a los que aprueben el examen final el último día hábil de junio.

Las clases serán teórico-prácticas interactivas y presenciales, promoviendo la participación y el aporte de experiencia de los asistentes. El método de evaluación será a través de un examen final tipo "múltiple choice", similar a los que se toman para las certificaciones de posgrado en seguridad la Profesionales Certificados en Protección Física (PSP) de la institución líder mundial en seguridad: ASIS International (www.asisonline.org)

Para tener en cuenta

- ¿Cuáles son los requisitos formales para certificarse PSP?

Seis o más años de experiencia full-time en Protección Física.

- ¿Hay un examen final?

Sí, puede acreditar su experiencia rindiendo en castellano el examen internacional de Profesional en Protección Física PSP en Buenos Aires.

- ¿Y luego?

Certificando que los conocimientos requeridos, habrá abierto el camino formal conforme al estándar ISO 17024:2003 para su desarrollo continuo como Profesional de Protección Física.

- ¿Sobre qué temas trata el examen PSP?

El examen trata sobre tres grandes temas denominados "Dominios" y sus competencias específicas relevantes. Estos Dominios son:

1. Relevamiento de Seguridad Física.
2. Aplicación, Diseños e Integración de Sistemas de Seguridad Física.
3. Implementación de Medidas de Protección Física.

- ¿Por dónde se comienza?

En el Curso de preparación comienza con la primer competencia del "Dominio 1" con algunas preguntas. Su nivel de respuesta correcta le dará la idea del nivel a escala internacional de sus conocimientos en cada competencia.

- ¿Cómo se aprueba?

A través de las clases el profesional va encontrando las respuestas correctas que le falten a las preguntas que no contestó bien.

Continúa en página 172

Cuando llegue a un nivel de aprobación del 80% estará en condiciones de rendir el examen final de validez internacional.

- ¿Como pueden los lectores de RDNS probar sus conocimientos?

Los lectores interesados pueden responder las preguntas del nivel de las del examen PSP. Para que sea una muestra representativa y útil, deberán responder unas 30.

A continuación, ofrecemos un Examen Tipo para Certificación Internacional en Protección Física PSP, modalidad *multiple choice*, que deberá ser contestado para acceder a la media beca del curso.

1. Una lista de las clases de amenazas que afectan los bienes tangibles e intangibles que se protegen mediante sistemas de protección física se conoce como:
a. Un perfil de evento de pérdida.
b. La lista de criticidad del evento de pérdida.
c. La tabla de cálculo de la tasa de seguro.
d. Listado de vulnerabilidades de los activos.

2. Los Controles Técnicos de Acceso Físico incluyen:
a. Política de seguridad de la organización.
b. Iluminación.
c. Concientización del Personal.
d. Plan de Reanudación de las Operaciones después de un Desastre.

3. La Protección Física mediante el Diseño Ambiental incluye:
a. Protección Eléctrica.
b. Guardias con capacidad de servicio e información adaptados a los requerimientos específicos del ambiente para el que se ha diseñado el servicio.
c. Cámaras de video de buen diseño y aptas para condiciones ambientales.
d. Iluminación.

4. Se consideran Amenazas en un sistema de Protección Física:
a. Interrupción en la provisión de servicios informáticos.
b. La obsolescencia de inventarios.
c. La pérdida de mercados.
d. Los juicios comerciales contra la empresa.

5. La Amenaza Humana más común es:
a. Hurto y Robo
b. Sabotaje y Vandalismo
c. Fraudes, malversación y espionaje.
d. Errores, desperdicio y abuso de recursos.

6. Son controles administrativos asociados a la planificación de los requerimientos de las instalaciones de Protección Física:
a. Lograr que se cumplan en tiempo y costo.
b. Diseñar una instalación segura.
c. Formar un equipo de trabajo multidisciplinario.
d. Proveer un sistema integrado de seguridad.

7. Son controles asociados a la Administración de la Seguridad en Instalaciones:
a. Diseñar una instalación segura.
b. Formar un equipo de trabajo multidisciplinario.
c. Proveer un sistema integrado de seguridad.
d. Rastros de Auditoria.

8. El más importante control de personal asociado a la Administración de la Seguridad es/son:
a. Seguimiento continuo de empleados
b. Revisiones precontratación.
c. Mantener un ambiente de trabajo motivante.
d. Revisiones post-contratación.

9. Resulta más difícil modificar mediante medidas de protección física la oportunidad de pérdidas debidas a la ubicación y accesos, en lugares:
a. Donde se comparte la propiedad.
b. Con accesos de emergencia.
c. Con indebida protección perimetral.
d. Con elevadas tasas de crimen local.

10. ¿Qué puede no considerarse como requerimiento de Electricidad de back-up en un centro de cómputos crítico?
a. Iluminación de la red eléctrica.
b. Sistemas de control de acceso físico.
c. Sistemas de protección/ detección de incendios.
d. HVAC

11. En una compañía operando a un margen del 5%, ¿qué cantidad de ventas debería generar para compensar la pérdida anual de $100.000 en incidentes?
a. 2.000.000
b. 1.800.000
c. 2.400.000
d. 5.000.000

12. El anti passback es:
a. Un método que impide la adulteración de las tarjetas.
b. Una característica de un sistema de control de accesos que impide que una tarjeta ingrese dos veces sin haber salido de un recinto.
c. La forma de evitar el empleo de tarjetas de identificación prestadas para ingresar.
d. La imposibilidad de salir de un recinto al cual no se entró.

13. Se llama cerradura fail safe a aquella que:
a. Se abre automáticamente en caso de falla.
b. Es a prueba de fallas.
c. Es apta para intemperie.
d. Se libera ante un corte de energía de red.

14. ¿Qué sucede con el Índice de falso rechazo y el Índice de falsa aceptación al aumentar el umbral de sensibilidad de un dispositivo biométrico?
a. Ambos suben.
b. El primero sube y el segundo baja.
c. El primero baja y el segundo sube.
d. No varían.

15. El grado de protección deseado para toda instalación está basado, como premisa, en el análisis de los dos factores fundamentales siguientes:
a. Costos y condiciones ambientales.
b. Condición crítica y vulnerabilidad.
c. Costos y vulnerabilidad.
d. Costos y condición crítica.

16. El proceso empleado por el gerente de seguridad para establecer las prioridades para la protección de activos se conoce como:
a. Encuesta de seguridad.
b. Encuesta de vulnerabilidad.
c. Análisis de riesgos.
d. Revisión de inspección.

17. La mayoría de las alarmas:
a. No toman acción ni notifican la acción que debería ser tomada.
b. No toman acción y notifican la acción que debería ser tomada.
c. Sólo toman acción sin notificar la acción que debería ser tomada.
d. Toman acción además de notificar la acción que debería ser tomada.

18. ¿Cuáles son los tres elementos para determinar el valor de un activo?
a. Alguna medida de valor relativo, vulnerabilidad a ataque y medida existentes de seguridad física vigentes.
b. Criticidad para el usuario, dificultad o periodo de tiempo para reemplazo y alguna medida de valor relativo.
c. El costo del activo, valor de publicidad para un grupo de amenazas específicas y dificultad o período de tiempo para reemplazo.
d. El costo del activo para reemplazo, criticidad para el usuario y valor para un grupo de amenazas específicas.

19. Una pantalla de alta definición permite

Continúa en página 176

mejorar la calidad del display de la imagen multiplexada. Si esta multiplexación es a un quad de 4 vistas en un monitor de 400 TVL, el operador apreciará vistas de:
a. 1600 TVL
b. 400 TVL
c. 200 TVL
d. 100TVL

20. Normalmente se conviene que un Objetivo Estratégico de un programa de Seguridad Física es:
a. Disuadir, Desviar, Denegar o Demorar el Acceso.
b. Detectar y Denunciar (Anunciar), Despertar (Anunciar el Problema) y Disponer (Responder / Arrestar si corresponde).
c. Disuadir, Demorar, Detectar, Detener (aprender) y Documentar (evidencia).
d. Controlar el Acceso.

21. Elija la apreciación más exactamente descripta acerca de la utilidad del Video en el Contexto de la Definición General de Soluciones de Seguridad Física (como de" sistemas de contramedidas tangibles diseñados para proteger los activos físicos y operacionales de una organización de amenazas identificadas"):
a. …que específicamente provee la disuasión y el desvío de un % pérdidas y de siniestros en el grado en que estén dadas las condiciones para ello… durante determinado período de tiempo y dependiendo de varios otros sub factores; información visual de algo que está pasando o de algo que sucedió.
b. …que específicamente provee información visual de algo que está pasando; o de algo que sucedió.
c. …que específicamente identifica amenazas, identificables según el requerimiento del caso, ya sea como personas, objetos, acciones u escenarios.
d. …que específicamente disuadirá un % pérdidas y siniestros en el grado en que estén dadas las condiciones para ello.

22. Son los componentes generalmente aceptados como los primordiales y de mayor costo efectividad preventiva de la Seguridad Física:
a. El video en todas sus formas CCTV, video IP, híbrido.
b. El control de accesos físico.
c. La vigilancia y respuesta profesional
d. La protección de los activos tangibles e intangibles de la organización.

23. La capacidad de procesar monitoreo de alarmas, credencialización, control de acceso y video digital será normalmente más segura y costo-efectiva:
a. Desde sus propias aplicaciones individuales a través de múltiples bases de datos.
b. Todos compartiendo la misma aplicación a través de la misma base de datos.
c. Todos compartiendo la misma aplicación a través de múltiples bases de datos.
d. Todos desde cualquier aplicación desde cualquier base de datos.

24. ¿Cuál de las siguientes afirmaciones describe mejor control de dos tarjetas?
a. Un Tarjetahabiente puede solamente tener hasta dos tarjetas activas en un momento dado,
b. Un tarjetahabiente puede solamente tener dos tarjetas en un momento dado.
c. Un tarjetahabiente puede tener más de dos tarjetas emitidas siempre que sea con distintos números de credencial que le sean asociadas.
d. Dos números de credencial diferentes y válidos necesitan ser presentados a una lectora dentro de N segundos con el propósito de obtener un acceso garantizado.

25. Cuando usa anti-passback local con tarjetas inteligentes de lecto-escritura, ¿dónde se da seguimiento a los tarjetahabientes?
a. En la base de datos.
b. En el servidor de enlace.
c. En el controlador de acceso.
d. En la misma tarjeta.

26. ¿Cuáles son los medios más seguros y costo efectivos para controlar de manera correctiva el piggy- backing y tail-gating?
a. Emitir una única credencial por usuario y mantener actualizadas las bases de datos de credenciales.
b. Acceder con tarjeta a la vista y guardia en el lugar.
c. Sustituir puertas y molinetes críticos por esclusas o puertas giratorias de diseño y enclavamiento especiales y sensorizados.
d. Emplear sistemas integrados de seguridad electrónica.

27. Son elementos efectivos para detección en el diseño de un sistema de administración de la seguridad:
a. Los guardias.
b. Las barreras.
c. Los sistemas de control de accesos.
d. Los micrófonos.

28. El Profesional de Seguridad Informática debe comprender Conceptos Generales de Protección y de Sistemas de Administración de Seguridad física Integrados que deben ser usados para mitigar vulnerabilidades identificadas; conceptos generales que constituyen requisitos tales como la comprensión de las fases del plan de seguridad, las que incluyen necesariamente:
a. Evaluación de Vulnerabilidad, Diseño del Programa de Seguridad Física, Implementación, Mantenimiento.
b. La Fase de implantación de las soluciones aprobadas y el proceso que permite asegurarse de que la efectividad de las soluciones no se deteriore, y que las soluciones se ajusten a la dinámica de las circunstancias, aún cuando cambie la naturaleza de las necesidades de seguridad.
c. La fase en la cual se realiza la Identificación de activos, amenazas, riesgos y vulnerabilidades; así como restricciones tales como costo, problemas operacionales y cultura.
d. La fase de evaluación y diseño del sistema integrado de seguridad física.

29. ¿Cuál es la solución más costo-efectiva de emplearse lectores de tarjetas de acceso físico/lógico?
a. Dado que no todos los Sistemas de Control de Acceso aceptan códigos de tarjetas de 32 bits de longitud, aceptar el requerimiento de algunos sistemas de truncar los 32 bits a 24 bits incrementándose, pero de manera muy remota, la posibilidad de encontrar tarjetas duplicadas.
b. Leer formatos no estándar.
c. Leer el CSN de una tarjeta inteligente con algún tipo de formato estándar, encriptado AES.
d. Implementar una aplicación de control de acceso en un sector de la tarjeta de manera que para poder leer el código de la tarjeta se necesiten las llaves del sector.

30. Para ser exitoso como solución el sistema Biométrico Real debe ser:
a. Aceptable de parte de los usuarios, preciso, mínimo nivel de error; seguro, no falsificable, libre de fraude y con capacidad de ser empleado 1 a 1 y 1 a N en configuraciones de 1, 2 o 3 factores.
b. Rápido, confiable, duradero, resistente y de bajo mantenimiento. Autónomo, posee memoria de registros y transacciones, monitoreo de alarmas y control de accesos, integrable: permite su integración a sistemas de terceros y Económico.
c. Al igual que los sistemas tarjetas lector o en combinación con éstos, fundamentalmente dependiente del uso requerido.
d. 1 y 2 son ciertos■