www.segurmatica.cu
e-mail: talleres@segurmatica.cu
Calle Zanja No. 651 esq. A Soledad, La Habana,
Cuba, Telf.: 78703536 ext 101, 133 al 136

TALLER: PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA PARA DIRECTIVOS

Profesor principal: MSC. Henry Raúl González Brito: Universidad de las Ciencias Informáticas (UCI), La Habana, Cuba.

Graduado de la carrera de Ingeniería Informática en el año 2005 en la Universidad de Camagüey y la Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE). Tiene un Máster en Gestión de Proyectos Informáticos y un Diplomado en Inteligencia Tecnológica. Ha trabajado en proyectos relacionados con ERP en software libre, inteligencia tecnológica y evaluación de la seguridad en aplicaciones web. Actualmente es metodólogo y coordinador de la Especialidad de Posgrado en Seguridad Informática en la UCI. Profesor del claustro de las maestrías de Informática Avanzada, Calidad de Software e Informática Médica Aplicada. Forma parte además del comité académico de la carrera de ciclo corto de
Administración de Redes y Seguridad Informática. Se desempeña como jefe del proyecto "Metodología Ágil para Pruebas de Penetración en Aplicaciones web (MAPPAW)" registrado en el Programa de Prioridad Nacional de Ciencia, Tecnología e Innovación "Informatización de la Sociedad" y coordina el grupo de investigación de seguridad informática de la UCI. Sus áreas de investigación actuales están relacionadas con las metodologías de pruebas de penetración, seguridad en aplicaciones web y detección de comportamientos anómalos en peticiones HTTP. Otros colaboradores: Especialistas de la OSRI y Segurmática.

CONVOCATORIA:

Taller online, con certificación a vuelta de correo, que le permitirá, sin moverse de su puesto de trabajo, a directivos y personal en general de las entidades cubanas, actualizarse sobre la situación y tendencias actuales de la seguridad informática en función de la protección de los servicios y redes de datos. Los conocimientos adquiridos le ayudarán a comprender y analizar, bajo un enfoque holístico y tecnológico, los principales conceptos, soluciones y prácticas que conforman el estado del arte en este campo.

Las actividades y materiales del taller facilitarán, de forma amena y sencilla, los principios esenciales que un directivo, independiente de su formación universitaria, necesita conocer para analizar y tomar decisiones respecto al estado y estrategia de la gestión de la seguridad informática en su entidad, con vistas a mantener o alcanzar niveles razonables de seguridad informática en su entorno.

www.segurmatica.cu
e-mail: talleres@segurmatica.cu
Calle Zanja No. 651 esq. A Soledad, La Habana,
Cuba, Telf.: 78703536 ext 101, 133 al 136

Se desarrollará sobre la plataforma virtual de Joven Club, y estará disponible durante un mes para que los interesados, dispongan de tiempo suficiente que les facilite estudiar a su ritmo (al menos dos horas diarias durante 10 días pudieran ser suficiente). Les recomendamos visualizar de manera colectiva por equipos de estudios, los materiales audiovisuales que ofrecemos, en horarios programados internamente en las entidades, que promueva la participación de los matriculados.

Durante el taller podrá interactuar con los contenidos, videos, acceder a los cuestionarios y examen en línea previsto, que acreditarán su evaluación, además de contar con la atención personalizada del profesor de Universidad de las Ciencias Informáticas (UCI) Henry Raúl González Brito, Máster en Gestión de Proyectos Informáticos y Diplomado en Inteligencia Tecnológica, actualmente coordinador de la Especialidad de Posgrado en Seguridad Informática con muchos años de experiencia en esta actividad, que atenderá sus interrogantes, además de los especialistas de Segurmática.

Pueden comenzar a solicitar su matrícula desde el 1ro de febrero:

Solicitud y gestión de Matrícula	**Fecha de realización del taller**
Del 1ro de febrero al 21 de abril	Del 22 de abril al 24 de mayo

La solicitud se realizará al correo talleres@segurmatica.cu con el **Asunto**: **TALLER ONLINE PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA PARA DIRECTIVOS** (Precio del Taller en línea: **200 CUP**).

SINOPSIS:

El presente curso tiene un enfoque amplio y está dirigido a directivos y personal en general, de entidades cubanas que necesitan actualizarse sobre la evolución y situación actual de la seguridad informática en función de la protección de los servicios y redes de datos. Su propósito no es enseñar a instalar herramientas de seguridad o establecer configuraciones seguras en servidores de producción.

Los participantes se familiarizarán con los principales componentes que definen la ciberseguridad en el contexto actual. Conocerá cuales son las funciones del cortafuego, sistemas de detección de intrusiones, mecanismo y estrategias de copias de respaldo,

programas antivirus y otros sistemas de seguridad. Las principales aplicaciones de la criptografía moderna, estrategias, métodos y procedimientos utilizadas en la administración de incidentes, estándares y controles de seguridad informática, evaluaciones de seguridad, sistemas de gestión eventos e información de seguridad (SIEM), vulnerabilidades y gestión de la seguridad en dispositivos móviles y aplicaciones web, amenazas a la seguridad en redes sociales, normativas y regulaciones vigentes relacionadas con la seguridad informática en el país.
Durante el taller también se presentan casos de estudio, que le permitirán consolidar los conocimientos adquiridos.

Al aprobar las actividades en línea propuestas se le envía, por correo electrónico, el certificado que avala su participación en el mismo.

PROGRAMA

No	Actividad	Contenidos principales.	Objetivos
1	Introducción a la Seguridad Informática	Situación actual. Conceptos básicos de seguridad informática, amenaza, vulnerabilidad, control, riesgo, impacto. Propiedades de la Información. Relaciones entre conceptos. Protocolos de red. Modelos de seguridad informática. Problemas actuales de la seguridad informática. Ataques informáticos. Botnets.	Caracterizar los principales factores que definen la ciberseguridad en el contexto actual. Explicar los principales conceptos, principios y modelos de la seguridad informática. Describir los tipos de ataques y vulnerabilidades asociadas que se producen en redes de datos.

2	Mecanismos de Seguridad Informática	Seguridad en redes. Estrategia para la Defensa en Profundidad. Cortafuegos. Sistemas de detección de intrusiones (IDS). Protección contra programas dañinos. Configuración segura de	Caracterizar los cortafuegos, detectores de intrusiones, programas antivirus y sistemas víctimas. Describir los principales componentes del proceso de copia de seguridad. Enumerar las fases de la

No	Actividad	Contenidos principales.	Objetivos
		sistemas operativos y servicios. Respaldo de información y planes de contingencias. Sistemas víctimas (Honeypot)	vigilancia tecnológica. Caracterizar estrategias de seguridad.
3	Papel de la criptografía en la Seguridad Informática	Introducción a la criptografía clásica, cripto-sistemas simétricos y asimétricos. Función resumen. Firma Digital. Infraestructura de llave pública. Aplicaciones de la criptografía para la protección de la información.	▪ Enumerar los principales conceptos de la criptografía moderna. ▪ Describir y valorar las aplicaciones de la criptografía en los procesos de la entidad. ▪ Caracterizar la infraestructura de llave pública y la firma digital.

4	Gestión de Incidentes de Seguridad Informática	Políticas y procedimientos para la gestión de incidentes. Elaboración de estrategias de respuesta a incidentes. Medidas y procedimientos. Definición de equipos de respuesta a incidentes. Fuentes para el descubrimiento de indicios de incidentes. Análisis de registros de auditoría (logs). Notificación y evaluación de incidentes. Parámetros de evaluación de incidentes. Métodos y herramientas para la contención de incidentes. Recuperación del incidente. Seguimiento de	▪ Caracterizar los principales métodos y herramientas utilizadas en la ▪ administración de incidentes. Enumerar métodos y herramientas para la recolección, procesamiento y mantenimiento de la evidencia digital.

No	Actividad	Contenidos principales.	Objetivos
		incidentes. Conceptos de Informática Forense. Evidencia Digital.	
5	Evaluaciones de Seguridad	Auditorías de seguridad, Evaluaciones de vulnerabilidades, Pruebas de Penetración. Papel de los distintos tipos de evaluaciones de seguridad para garantizar la seguridad de la entidad.	▪ Caracterizar los diferentes tipos de evaluaciones de seguridad. ▪ Enumerar los métodos y herramientas adecuados para realizar una evaluación de seguridad según la infraestructura.

			▪ Describir métodos de solución a las vulnerabilidades y debilidades encontradas.
6	Estándares y controles de seguridad	Definición de controles de seguridad, principales normas y estándares internacionales. Desarrollo seguro.	▪ Describir estándares para la gestión de la seguridad de redes. ▪ Enumerar los principales controles de seguridad informática.
7	Gestión de la seguridad informática	Gestión de Políticas de Seguridad Informática. Diseño y evaluación de Políticas de Seguridad Informática. Sistemas SIEM.	▪ Caracterizar la Gestión de Políticas de Seguridad Informática. ▪ Caracterizar los principales conceptos asociados a los sistemas SIEM.
8	Seguridad en aplicaciones web y móviles.	Principales vulnerabilidades web y móviles. Controles proactivos. Políticas BYOD.	▪ Caracterizar las principales vulnerabilidades que afectan la seguridad en los dispositivos móviles. ▪ Enumerar las principales políticas para gestión de la seguridad en dispositivos
No	**Actividad**	**Contenidos principales.**	**Objetivos**
			móviles para uso profesional.
9	Seguridad en redes sociales	Ciber-bulling, ciberacoso, ciber-extorsión. Phinshing. Uso seguro de redes sociales.	▪ Describir las principales amenazas que afectan la seguridad en redes sociales. ▪ Aplicar buenas prácticas de protección en perfiles e interacciones en redes sociales.

10	Normativas y regulaciones cubanas de seguridad informática.	Estructura actual que debe tener el plan de seguridad informática, partiendo de las diferencias con su antecesora, su vínculo con la Resolución 127/07 del Ministerio de Comunicaciones, y ejemplos de aspectos que se pueden incluir en cada capítulo, para cumplir además con lo establecido al respecto, en la resolución 60 de la Contraloría. Otras cuestiones que proponga SEGURMÁTICA.	▪ Enumerar las normativas y regulaciones vigentes, relacionadas con la seguridad informática en el país. ▪ Caracterizar los principales componentes de la Resolución 127/07 del Ministerio de Comunicaciones.