**Programación de Eventos y Talleres Año 2019.**

**Segurmática en su 25 aniversario por una**

**Informatización Segura y Sostenible.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Adiestramiento** | **Profesor** | **Feb** | **Marz** | **Abril** | **mayo** | **Junio** | **Sept.** | **Nov.** |
| Taller “Metodología para el diseño de un sistema de gestión de la seguridad informática”400 CUP | Lic. Juan Carlos Moro Hernández | 25 al 28 |  |  |  |  | 9 al 12 |  |
| Taller on-line “Metodología para el diseño de un sistema de gestión de la seguridad informática”200 CUP | Lic. Juan Carlos Moro Hernández |  |  |  |  | 1 al 30 |  | 1 al 30 |
| Taller “Análisis de Riesgos”300 CUP | Lic. Juan Carlos Moro Hernández |  | 18 al 20 |  |  | 17 al 19 | 16 al 18 | 18 al 20 |
| Protocolo TCP/IP300 CUP | Roldan Rodríguez Ramirez |  | 25 al 27 |  |  | 24 al 26 | 23 al 25 | 25 al 27 |
| Taller on-line Principios de la Seguridad. Informática para Directivos 200 CUP | *Henry Raúl González Brito* |  |  | 22abriAl 24 de mayo |  |  |  |  |
| Puertas abiertas a los clientes  | *UEB TC* |  |  |  | 24Ses. Mañ |  |  |  |
| Intercambio con los distribuidores | *UEB TC-Desarrollo* |  |  |  | 24Ses.tarde |  |  |  |
| Taller por el Día de la SI previo al evento Informatica 2020Participantes 250 CUP, Ponentes 100 CUP | *UEB Desarrollo* |  |  |  |  |  |  | 27, 28 y 29 |

**Taller: Metodología para el diseño de un sistema de gestión de la Seguridad Informática.**

Fecha: 25 al 28 de febrero y 9 al 12 de septiembre

Hora: 9.00 am / 1.00 pm

Lugar: Instalación de Segurmática, Calle Zanja 261 esquina a Soledad. Centro Habana

Cuota de Inscripción: 400.00 CUP

**Sinopsis:**

El taller está orientado a las personas que responden por la seguridad informática en las entidades. El estudiante se familiarizará con la metodología que desde mediados del año 2013 publicó en su sitio, [www.cucert.cu](http://www.cucert.cu), la Oficina de Seguridad de Redes Informáticas.

Se detallan las cuatro etapas del sistema de gestión de la seguridad informática: planificación, implementación, verificación y actualización; incluyendo ejemplos que ilustran cómo actuar en cada una de ellas.

Además, se detalla la estructura actual del 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.

En el taller también se realizan demostraciones prácticas a partir de casos de estudio, que permitirán al estudiante consolidar los conocimientos adquiridos.

El profesor comparte su experiencia de años de trabajo en la actividad.

Se entrega certificado que avala su participación en el mismo.

**PROGRAMA:**

**Día 1**

 Presentación del Adiestramiento.- Introducción.

Sistema de Gestión de la Seguridad Informática.

* 1. Planificación.

Destacan:

* + - Compromiso de la Dirección
		- Preparación del equipo
		- Estimación de riesgos
		- Políticas de Seguridad Informática
	1. Implementación
		+ Programa de Desarrollo de la Seguridad Informática
		+ Factores críticos de éxito.
	2. Verificación
		+ Métodos e indicadores de medición.
	3. Actualización
		+ Mantenimiento, mejora y corrección.

**Día 2**

Estructura y Contenido del Plan de Seguridad Informática.

* 1. Aspectos que se mantienen y novedades.
	2. Vínculos con la resolución 127/07.
	3. Estructura del plan:
		+ 1. Alcance.
			2. Caracterización.
			3. Resultado del análisis de riesgos.
			4. Políticas de Seguridad Informática.
			5. Responsabilidades

Actividad Práctica vinculada a la estructura del plan estudiada.

**Día 3**

Estructura y contenido del plan (continuación).

 a. Estructura del plan (cont.)

6.Medidas y Procedimientos de Seguridad Informática

6.1. Clasificación y control de los bienes informáticos.

6.2. Del Personal.

6.3. Seguridad Física y Ambiental.

6.4. Seguridad de Operaciones.

6.5. Identificación, Autenticación y Control de Acceso.

6.6. Seguridad ante programas malignos.

6.7. Respaldo de la Información.

6.8. Seguridad en Redes.

6.9. Gestión de Incidentes de Seguridad.

7. Anexos

**Día 4**

 Actividad Práctica Medidas y Procedimientos del Plan de Seguridad y Examen.

**TALLER ONLINE METODOLOGÍA PARA EL DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA, DISPONIBLE EN LA PLATAFORMA EDUCATIVA DE JOVEN CLUB.**

Taller online, con certificación a vuelta de correo, que le permitirá sin moverse de su puesto de trabajo, conocer cómo gestionar de forma más segura la seguridad informática en su empresa**, teniendo en cuenta las Normas vigentes para el Sistema de Gestión de la Seguridad Informática (SGSI),** además le enseñaremos cómo se estructura el proceso de diseño, implementación y operación de un SGSI, incluyendo la estructura actual del plan de seguridad informática.

Se desarrollará sobre la plataforma virtual de Joven Club, y estará disponible para los alumnos que se matriculen, durante un mes para que tengan tiempo de estudiar a su ritmo (al menos dos horas diarias durante 8 días pudiera ser suficiente), donde podrá interactuar con los contenidos, videos, acceder a los cuestionarios y exámenes en línea previstos, que acreditarán su evaluación, además de contar con la atención personalizada del profesor Lic. Juan Carlos Moro Hernández especialista con muchos años de experiencia en esta actividad, que atenderá todas sus interrogantes.

Si aún no sabe cómo gestionar de forma segura la Seguridad Informática en su empresa, puede solicitar la matrícula dos meses antes de la convocatoria al taller, es decir:

|  |  |  |
| --- | --- | --- |
| **Convocatoria** | **Solicitud y gestión de Matrícula** | **Fecha de Realización** |
| Junio | 1ro de abril al 31 de mayo | 1ro al 30 de Junio |
| Noviembre | 1ro de septiembre al 31 de octubre | 1ro al 30 de Noviembre |

La solicitud se realizará al correo talleres@segurmatica.cu con el **Asunto**: Taller online para la **Gestión de la seguridad informática** y recibirá los modelos e información requeridos para la contratación y transferencia **bancaria. (**Precio del **Taller en línea:** 200 cup).

**Sinopsis:**

El taller en línea permitirá la participación en todo el país de las personas relacionadas con la seguridad informática en las entidades. El estudiante se familiarizará con la metodología aprobada y publicada en el sitio www.cucert.cu, de la Oficina de Seguridad de Redes Informáticas.

Durante el taller conocerá las cuatro etapas del sistema de gestión de la seguridad informática: planificación, implementación, verificación y actualización; incluyendo ejemplos que ilustran cómo actuar en cada una de ellas.

Le enseñaremos la 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 General de la República.

Durante el taller también se presentarán casos de estudio, que le permitirán consolidar los conocimientos adquiridos.

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

**Taller: Análisis de Riesgos.**

Fecha : 18 al 20 de marzo, 17 al 19 junio, 16 al 18 septiembre, 16 al 18 octubre y 18 al 20 nov

Hora: 9.00 am / 1.00 pm

Lugar: Instalación de Segurmática, Calle Zanja 261 esquina a Soledad. Centro Habana

Profesor : Lic Juan Carlos Moro Hernandez

Cuota de Inscripción: 300.00 CUP

**Sinopsis:**

El taller está orientado a las personas que responden por la seguridad informática en las entidades. El estudiante se familiarizará con el contenido de la norma ISO-IEC 27005 que proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una Organización.

Durante el taller conocerá las etapas requeridas para la realización del análisis de riesgos, se realizarán demostraciones prácticas a partir de casos de estudio, que permitirá al estudiante consolidar los conocimientos adquiridos.

El profesor comparte su experiencia de años de trabajo en la actividad.

Se entrega certificado que avala su participación en el mismo.

**PROGRAMA:**

**Día 1**

 Presentación del Taller.- Introducción.

El análisis de riesgos en las Normas ISO.

1. Norma ISO/IEC 27005.
* Información general.
* Visión general del proceso de gestión del riesgo.
* Evaluación del riesgo.
* Tratamiento del riesgo.
* Aceptación del riesgo.
* Comunicación de los riesgos.
* Monitoreo y revisión del riesgo.

**Día 2**

### Determinación de las necesidades de protección

### Caracterización del entorno informático.

1. Activos informáticos.
2. Importancia de los activos.
3. Amenazas que afectan a los activos
4. Probabilidad de ocurrencia de cada amenaza.

### Evaluación del estado actual de la seguridad.

### Resultados del análisis de riesgos.

Actividad Práctica vinculada con el tema.

**Día 3**

Ejercitación (donde según casos de estudio los estudiantes deberán establecer los elementos que requiere el análisis de riesgos).

**Taller: Fundamentos de TCP/IP.**

Fecha: del 25 al 27 de marzo, 24 al 26 junio, 23 al 25 de septiembre y 25 al 27 de noviembre

Hora: 9.00 am / 1.00 pm

Lugar: Instalación de Segurmática, Calle Zanja 261 esquina a Soledad. Centro Habana

Cuota de Inscripción: 300.00 CUP

**Sinopsis:**

Durante este taller los administradores de redes, especialistas de seguridad informática, directivos de tecnologías de la Información y la Comunicación, programadores, etc, conocerán los elementos básicos y de nivel medio en la familia de los protocolos de Internet (TCP/IP), su empleo y configuraciones en los diferentes servicios soportados sobre éste, con demostraciones prácticas que acompañados con la experiencia en años que en esa actividad posee el profesor, le permitirán consolidar los conocimientos que sobre estas temáticas se impartirán en el Taller Fundamentos de TCP/IP.

Profesor: Roldan Rodríguez Ramirez

Sinopsis:

El taller está orientado a los administradores de redes que comienzan a desempeñarse en esa actividad, los especialistas de seguridad informática, los directivos TIC, programadores, así como para cualquier otra profesión que se vincule de alguna manera con el trabajo en redes de datos. El estudiante adquirirá los conocimientos básicos y también de nivel medio en la familia de protocolos de Internet (TCP/IP).

TCP/IP es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP. El conocimiento de esta familia de protocolos, su empleo y configuraciones de diferentes servicios soportados sobre éste, es indispensable para cualquier profesional de la esfera informática.

En el taller el profesor realiza demostraciones prácticas de cómo configurar estos protocolos en Windows y Linux, mostrando el uso de algunas herramientas comúnmente empleadas para ello, compartiendo la experiencia de años de trabajo en esta actividad.

Se entrega certificado que avala su participación en el mismo.

Si está interesado solicite ahora mismo su matrícula al correo talleres@segurmatica.cu donde le atenderán y solicitarán los documentos requeridos para lograrlo.

**TALLER ONLINE PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA PARA DIRECTIVOS.**

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 evolución y situación actual de la seguridad informática en función de la protección de los servicios y redes de datos, permitiendo informarse de la respuesta que da la tecnología informática actual a la problemática de la seguridad en redes de datos, enfatizando su condición de Proceso y no de Producto.

El taller facilitará a los directivos de forma amena y sencilla, principios básicos en estas temáticas, necesarios en la toma de decisiones respecto a estrategias presentadas por el personal TIC de su entidad, para garantizar niveles razonables de seguridad informática en su entorno.

Se desarrollará sobre la plataforma virtual de Joven Club, y estará disponible durante un mes para que los alumnos matriculados, dispongan de tiempo suficiente que les facilite estudiar a su ritmo (al menos dos horas diarias durante 8 días pudiera ser suficiente), donde 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 del grupo de investigación de seguridad informática de la UCI* con muchos años de experiencia en esta actividad, que atenderá todas sus interrogantes, además de los especialistas de Segurmática.

Si usted es directivo de su entidad y aún no conoce los elementos básicos relacionados con la seguridad informática, aproveche la oportunidad que le ofrecemos de conocerlos de forma amena y sencilla diseñado especialmente para usted, puede solicitar la matrícula dos meses antes de la convocatoria al taller, es decir:

|  |  |  |
| --- | --- | --- |
|  | **Solicitud y gestión de Matrícula** | **Fecha de Realización** |
| Abril  | 1ro de feb al 21 de abril  | 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** y recibirá los modelos e información requeridos para la contratación y transferencia **bancaria. (**Precio del **Taller en línea:** 200 cup).

**Sinopsis:**

El taller en línea permitirá la participación en todo el país de los directivos y personal de entidades que participen en la toma de decisiones relacionada con la seguridad informática de su entorno. El estudiante se familiarizará con los principales factores que definen la ciberseguridad en el contexto actual. Conocerá que es un cortafuego, detectores de intrusiones, programas antivirus y sistemas víctimas, los principales conceptos de la criptografía moderna, algunos métodos y herramientas utilizadas en la administración de incidentes, principales controles de seguridad informática existentes, conceptos asociados a los sistemas SIEM, vulnerabilidades que afectan la seguridad en los dispositivos móviles, amenazas que afectan 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.

**LAS PUERTAS DE SEGURMÁTICA SE ABRIRÁN PARA COMPARTIR CON SUS CLIENTES EL PRÓXIMO** **VIERNES 24 DE MAYO.**

La empresa Segurmática tiene el gusto de invitar a sus clientes al encuentro PUERTAS ABIERTAS, con el objetivo de intercambiar opiniones, informarles acerca de los principales programas malignos que han circulado en el país, las mejoras de las nuevas versiones de los productos liberados e informaciones de interés que se compartirán. Promete ser un espacio oportuno para el debate e intercambio de buenas prácticas sobre el uso de nuestros productos y así como conocer el grado de satisfacción de nuestros clientes con los productos y servicios que prestamos.

Fecha: viernes 24 de mayo del 2019

Hora: 9.30 am / 12.00 m

Lugar : Instalación de Segurmática, Calle Zanja 261 esquina a Soledad. Centro Habana

Es necesario que confirme de su participación en el buzón talleres@segurmatica.cu con el Asunto: **Puertas abiertas** y en el texto del mensaje: Nombre y cargo de los participantes, pudieran participar hasta dos compañeros por cada cliente. Le esperamos.

No olvide escribirnos para confirmar de su participación hoy mismo, la capacidad del local limita la cantidad participantes. Usted recibirá a vuelta de correo confirmación de su solicitud de participación.