**Capacitación en CePETel 2021**

Desde la Secretaria Técnica comenzamos con los cursos de capacitación a distancia iniciado en abril. En esta ocasión invitamos a participar:

**Seguridad en las Tecnologías de la Información (IT)**

**Clases**: 10 de 3 hs c/u de 18:30 a 21:30 hs.

**Días que se cursa**: miércoles 12, 19, 26 de mayo; 2, 9, 16, 23 y 30 de junio; 7 y 14 de julio.

**Modalidad: a distancia** (requiere conectarse a la plataforma Zoom en los días y horarios indicados precedentemente).

**Docente**: Marcelo Bugallo

**La capacitación es:**

* **Sin cargo para afiliados y su grupo familiar directo.**
* **Sin cargo para encuadrados con convenio CePETel.**
* **Con cargo al universo no contemplado en los anteriores.**

**Informes: enviar correo a** [tecnico@cepetel.org.ar](mailto:tecnico@cepetel.org.ar)

**Inscripción (hasta el 30 de abril)**: ingresar al formulario (se solicita utilizar una cuenta de correo personal)

https://forms.gle/JrLywoMxjzyvzaS36

**Objetivos**

Este curso permitirá a los participantes adquirir conocimientos sobre conceptos, características, tipos, fases de implementación, normativas y aplicaciones de utilización de la Seguridad en las Tecnologías de la Información (IT).

**Programa**

**Capítulo 01 – Seguridad Básica**

* ¿Qué es la Seguridad de la Información?
* Terminología de la Seguridad Informática
* Tríada de la Seguridad Informática (Tríada CIA)
* Frases célebres de la Seguridad Informática
* Vulnerability Research
* Etapas del proceso de Hacking
* Terminologías de Hacking
* Hacktivismo
* Casos de Hackers
* Perfil del Hacker

**Capítulo 02 – Seguridad en el Desarrollo**

* Introducción a la Seguridad en el Desarrollo
* Sistemas inseguros
* Tendencia de la Seguridad de los sistemas
* Modelo Espiral
* Fracasos comunes de los proyectos
* Problemática: aplicaciones inseguras
* Variables de entornos / ambientes
* Acceso a los entornos
* Control de cambios y versiones
* Segregación de funciones
* ¿Qué loguear y dónde?
* Arquitecturas de sistemas
* Firewall de base de datos
* ¿En qué nos afectan y dónde están las vulnerabilidades?
* ¿Qué podemos hacer para prevenirnos?

**Capítulo 03 – Fase Inicial**

* Arquitectura de software
* Estilos arquitectónicos
* Application Security
* Lenguaje de interfaz de datos
* Integridad – Ocurrencia
* Servicios de integridad
* Base de datos relacionales: componentes
* Structural Query Language (SQL): características
* SQL: comandos básicos
* OLAP (Online Analytical Processing)
* Data Warehouse & Data Mining
* Problemas de seguridad
* Amenazas y vulnerabilidades: agregación e interferencias

**Capítulo 04 – Fase Final**

* Métodos de desarrollo de sistemas (software)
* Fases del ciclo de vida de un sistema
* Modelo IDEAL
* Ley Sarbanes – Oxley (SOX)
* Estándar COSO
* Consideraciones previas a la implementación de ISO / IEC 27001
* Conceptos básicos de seguridad de la información
* Estándares de la Serie 27000
* Estándares sobre la visión general y vocabularios
* Estándares sobre especificación de requisitos
* Estándares sobre guías generales
* Estándares sobre guías para sectores específicos

**Capítulo 05 - Serie Normas ISO 27000 (Conceptos)**

* Conceptos básicos de la Seguridad de la Información:
* Seguridad
* Información
* Confidencialidad
* Integridad
* Disponibilidad
* Intencionalidad
* Amenaza
* Ataque
* Riesgo
* Probabilidad
* Impacto
* Objetivo del control
* Sistema de gestión de seguridad de la información
* Mejores prácticas

**Capítulo 06 – Casos de utilización de IT Seguridad**

* Seguridad en aplicaciones y sistemas virtuales.
* Hacking y análisis forense.
* Seguridad en redes y comunicaciones virtuales.
* Seguridad Perimetral.
* Certificados y firma digital.
* DNIe
* eAdministración
* eComercio

### Metodología: Actividades de Aprendizaje

La metodología de aprendizaje consiste en presentaciones en powerpoint con material teórico – práctico; impulsando una participación activa de los asistentes.

**Acerca del docente**

Marcelo Bugallo se desempeña a la fecha en IFX Networks como Ingeniero de Negocios en Elaboración y diseño de soluciones de tecnología cloud pública y privada, enlaces de datos y soluciones de ciberseguridad.

Ejerce la docencia en la Universidad de Palermo como docente presencial y a distancia de la materia Seguridad en Redes de la carrera Ing. en Informática; y también lo hace en Universidad Nacional de Avellaneda como docente de Seguridad de los Sistemas Informáticos en la carrera de Ingeniería en Informática.

Tiene estudios en Diplomatura en Seguridad de la Información (UTN-FRBA), Diplomatura en Emprendimiento e Innovación (EAN), Diplomatura en Marketing (EAN),

Curso de certificación LPI (Open Source & Debian Linux Expert) en CentralTech, Curso de certificación CCNA (Cisco Certified Network Associate) Fundación Proydesa, entre otros cursos y certificaciones.