



**CYBSEC**<sup>S.A.</sup>  
Security Systems



## **INSTITUTO BANCARIO INTERNACIONAL** **Centro de Estudios Superiores**

*Resuelto No. 174 del 18 de diciembre de 2002 del Ministerio de Educación*

**ASOCIACIÓN BANCARIA DE PANAMÁ**

**Y**

**CYBSEC, S.A., Security Systems**  
Buenos Aires, República Argentina

**OFRECEN EL SEMINARIO - TALLER INTERNACIONAL**

## **“SEGURIDAD EN SAP”**

Fecha: 23 y 24 de abril de 2008

de 08:00 a.m. a 05:00 p.m.

25 de abril de 2008

de 08:00 a.m. a 12:00 m.d.

Duración: 20 Horas/Clases

Centro de Capacitación Tecnológico del Instituto Bancario Internacional  
Ciudad de Panamá, Rep. de Panamá

COSTO: US\$.950.00 (neto de impuestos)

**JUSTIFICACIÓN:** La gran mayoría de las Organizaciones medianas y grandes utilizan a SAP como software ERP. SAP pues les brinda un motor para la operación de las Compañías. La seguridad dentro de SAP es totalmente necesaria ya que a través de SAP pasan las transacciones financieras, autorizaciones, pagos, en resumen, información confidencial y crítica para la Empresa.

El seminario-taller internacional de Seguridad en SAP tiene el objetivo de explicar prácticamente las estrategias para asegurar, auditar y controlar la plataforma SAP.

**DIRIGIDO A:** Jefes, Administradores de BASIS SAP, Oficiales y Responsables de Seguridad Informática, Gerentes de Sistemas, Gerentes de Tecnología, Auditores de Sistemas, Responsables de Internet, Administradores de Redes, Programadores SAP, Administradores de Sistemas de Entidades Financieras y Empresas usuarias del sistema SAP.

**OBJETIVOS:** Los objetivos del Seminario son:

- Presentar a los asistentes los aspectos de seguridad del sistema SAP R/3.
- Utilizar las herramientas para administrar usuarios, roles y autorizaciones en forma segura y eficiente.
- Analizar las directivas de configuración segura de todos los componentes del sistema: Sistema Operativo, Base de Datos y SAP R/3.
- Aprender las mejores prácticas de seguridad en la configuración de los distintos servicios e interoperabilidad con otros sistemas de la Empresa.
- Conocer las técnicas utilizadas por los potenciales intrusos y las defensas para protegerse de los mismos.

**CUPOS LIMITADOS ESTRICTAMENTE PARA 21 PARTICIPANTES**

## **METODOLOGÍA:**

- El seminario será dictado de forma intensiva manteniendo un adecuado balance entre la teoría y la práctica en una red de computadoras que es utilizada como laboratorio.
- El método de "Estudio de Casos" permite que los asistentes, en grupos, participen en la simulación de situaciones reales en las que se pueden aplicar los conocimientos adquiridos a lo largo del seminario.
- El seminario será dictado por un Líder de Proyecto de CYBSEC S.A., que si bien ha sido entrenado en prácticas docentes, acredita la valiosa experiencia que significa mantener la seguridad real en múltiples y complejas plataformas informáticas.

**MATERIAL DE APOYO:** Los asistentes al seminario, recibirán:

- Una carpeta conteniendo el material didáctico desarrollado por CYBSEC.
- Bibliografía complementaria.
- Un CD-ROM conteniendo herramientas y documentación adicional.

## **PRE – REQUISITOS Y CONOCIMIENTOS SUGERIDOS PARA LOS PARTICIPANTES:**

Para el desarrollo del seminario - taller es indispensable que el participante traiga su propia notebook y deberá tener conocimientos básicos de:

- Plataformas informáticas (UNIX y Windows).
- Aplicación SAP.

**QUIÉN ES CYBSEC:** CYBSEC S.A. es una empresa que desde 1996 se dedica exclusivamente a prestar servicios profesionales especializados en Seguridad Informática. Su área de servicios cubre Latinoamérica, Europa y Estados Unidos y más de 250 clientes acreditan la trayectoria empresaria.

Por razones de objetividad y ética profesional, CYBSEC S.A. no representa, no vende ni está asociada con terceras empresas proveedoras de software y/o hardware.

CYBSEC S.A. ha capacitado a más de 1.100 profesionales de seguridad informática en toda Latinoamérica a través de sus centros de capacitación en Argentina, Ecuador y Panamá.

CYBSEC trabaja y asesora en seguridad en SAP desde el año 2001, bajo las plataformas UNIX, Windows y AS/400. Desde el año 2005 acredita una intensa actividad en la detección de vulnerabilidades y ha realizado aportes para la solución de las mismas.

En el año 2007 CYBSEC comenzó a trabajar directamente con SAP Ag Alemania, estableciéndose un contacto fluido y altamente constructivo con las áreas de seguridad informática propias de SAP.

Actualmente CYBSEC forma parte de la Global Security Alliance (GSA) de SAP, donde SAP Internacional incluye a CYBSEC como prestador de servicios de seguridad de la información.

**FACILITADOR:** **Mariano Núñez Di Croce**, Nacionalidad Argentina

Mariano es Consultor Senior de CYBSEC desde hace 4 años. En su trabajo habitual realiza Penetration Test y Evaluaciones de Seguridad a principales empresas y organismos internacionales. Su área de expertise principal es la seguridad de los sistemas SAP internos y externos.

Mariano es miembro también del CYBSEC-Labs, donde se encuentra realizando investigaciones sobre nuevas técnicas de intrusiones y defensas y ha descubierto más de veinte vulnerabilidades en productos de empresas como SAP y Microsoft.

Mariano ha realizado exposiciones y cursos en eventos internacionales en Latinoamérica, BlackHat Amsterdam, Hack.lu en Bélgica y DeepSec en Austria.

## CONTENIDO:

### 1. Breves conceptos de la Seguridad Informática de SAP

- ▣ Descripción de los componentes de SAP.
- ▣ Autenticación.
- ▣ Autorización.
- ▣ Encriptación.

### 2. Seguridad del Sistema Operativo ( Windows / UNIX )

- ▣ Usuarios y Grupos.
- ▣ Servicios.
- ▣ Taller práctico sobre la seguridad a nivel del sistema operativo Windows.
- ▣ Protección de recursos de SAP.
- ▣ Caso de estudio sobre seguridad en el sistema operativo.

### 3. Seguridad de la Base de Datos ( MS SQL Server / Oracle )

- ▣ Usuarios y Grupos. Passwords.
- ▣ Mecanismos de Autenticación segura.
- ▣ Encriptación.
- ▣ Privilegios de acceso.
- ▣ Taller práctico sobre la seguridad a nivel de Base de Datos SQL Server.

### 4. Seguridad global de SAP R/3

- ▣ Arquitectura del Sistema.
- ▣ La seguridad según SAPA.
- ▣ Transacciones.

### 5. SAP R/3: Seguridad del Sistema de Transportes

- ▣ Configuración del Sistema de Archivos.
- ▣ Landscapes.
- ▣ Configuración de Mandantes.

### 6. SAP R/3: Administración de Usuarios y Autenticación

- ▣ Manejo de Usuarios. Bloqueos.
- ▣ Perfiles y Roles.
- ▣ Tracing de Autorizaciones.
- ▣ Central User Administration (CUA) System.
- ▣ Autenticación.
- ▣ Taller sobre el manejo de usuarios.
- ▣ Caso de estudio del Societe Générale sobre uso de autorizaciones.
- ▣ Single Sign-On.

### 7. SAP R/3: Seguridad en las comunicaciones

- ▣ Topologías seguras.
- ▣ Configuración de filtros: Firewalls y SAP Router.
- ▣ Servicios.
- ▣ Encriptación mediante SSL y SNC.
- ▣ Instalación segura de aplicaciones.
- ▣ Principio del menor privilegio.
- ▣ Ejemplos para no imitar.

## **CONTENIDO: Continuación**

### **8. SAP R/3: Seguridad en la conectividad**

- ▣ La interfase RFC.
- ▣ Escenarios.
- ▣ Usuarios y Autorizaciones
- ▣ Encriptación.
- ▣ Trusted Systems.
- ▣ Seguridad en ICF.
- ▣ Autenticación y Autorización.
- ▣ Traces.
- ▣ Uso de SSL.
- ▣ Enterprise Portal.
- ▣ Autenticación y Autorización.
- ▣ Single Sing-On.
- ▣ Administración de Claves.
- ▣ Comunicación segura.
- ▣ Web Services.
- ▣ Autenticación.
- ▣ Certificados.
- ▣ WS Security.
- ▣ Taller de configuración de la conectividad.
- ▣ Caso de estudio sobre las vulnerabilidades de seguridad detectadas.

### **9. SAP R/3: Actualización del Sistema**

- ▣ Vulnerabilidades de SAP.
- ▣ El Service MarketPlace.
- ▣ Aplicación de Notas.
- ▣ Aplicación de Support Packages.
- ▣ Upgrade del Sistema.
- ▣ Principio del menor privilegio.
- ▣ Ejemplos para no imitar.

### **10. Análisis de Logs y Auditoría**

- ▣ Logs del Sistema Operativo.
- ▣ Logs de la Base de Datos.
- ▣ Logs de SAP.
- ▣ Taller de análisis de logs.
- ▣ Detección de Intrusiones.

### **11. Taller práctico sapyto**

- ▣ Uso del sapyto
- ▣ Herramientas para auditar SAP