

Centro de Estudios La Piedad

Asociación del Personal de los Organismos de Control

**COMO AUDITAR LA TECNOLOGÍA INFORMÁTICA**

**(Sin ser técnicos)**

# Datos generales de la entidad

ASOCIACIÓN DEL PERSONAL DE LOS ORGANISMOS DE CONTROL – CENTRO DE ESTUDIOS LA PIEDAD - Inscripción Registro de Prestadores del Sistema Nacional de Capacitación Nº 37-6114797-6

# Denominación de la actividad a acreditar

Cómo auditar la tecnología informática (sin ser técnicos).

# Fundamentación General:

El Centro de Estudios La Piedad, de la Asociación del Personal de los Organismos de Control, ha identificado un conjunto de necesidades y demandas de capacitación del personal profesional que integra equipos de auditoría en instituciones gubernamentales y que muchas veces carece de formación específica en materia de tecnologías de la información.

Los organismos de control del Estado Nacional, Provincial y Municipal, enfrentan el desafío de llevar a cabo auditorías eficaces sobre la gestión de las organizaciones gubernamentales. Estas a su vez, reflejando un fenómeno que afecta prácticamente a todas las organizaciones, han incorporado en los últimos años recursos tecnológicos tanto en su gestión interna como en la prestación de servicios al ciudadano, al punto de convertirse algunas de ellas en modelos sociales de uso de modernas tecnologías para el cumplimiento de su función.

En efecto, desde fines del siglo XX y hasta la fecha, los sistemas informáticos se han constituido en una de las herramientas más poderosas para gestionar la información de la Organización, siendo uno de los elementos más vitales y necesarios en la generación de valor para todos los involucrados.

Hoy las tecnologías de la información y las comunicaciones (TIC) se encuentran incorporadas en la gestión integral de la organización. En consecuencia, coayudan a la toma de decisiones y al proceso operativo, basadas en datos e información proporcionada con calidad, en tiempo y forma.

La información es de la organización y para la organización y se ha convertido en un activo real de la misma, tan tangibles como un servidor, una base de datos, el stock o las materias primas. Las inversiones informáticas demandan ser analizadas y evaluadas eficientemente incluyendo no sólo el resultado de las mismas, sino también el software y el hardware. Del mismo modo, los recursos tecnológicos y humanos has de protegerse de modo global y particular.

Las organizaciones públicas son parte de esta realidad y hoy prácticamente no existe en ellas ningún dato o documento, que en algún momento de su ciclo de vida, no haya formado parte de un proceso de tratamiento electrónico.

Esto exige que quienes se desempeñan en áreas de auditoría, aún sin ser especialistas, deban conocer cómo funcionan estos recursos informáticos y se encuentren en condiciones de evaluar los riesgos que implican estas capacidades de procesamiento de la información. En este marco, deben también desarrollar la habilidad de formular recomendaciones para minimizar los riesgos a través de controles eficientes y efectivos, contribuyendo con ellas a una mejor gestión de la organización auditada.

Alrededor de esta temática se desarrolla este curso virtual que tiene por objetivo dotar, a quienes lo realicen, del conocimiento y herramientas para entender las principales características del procesamiento electrónico de la información así como las implicancias de las tecnologías de la información y las comunicaciones para el desarrollo de la auditoría.

# Perfil de los destinatarios de la actividad

Este curso está orientado a:

* Personal de Auditoría y Áreas de Control con responsabilidades en el desarrollo y verificación de controles internos.
* Personal responsable en el control de procesos informáticos.
* Auditores con experiencia inicial en tareas de Auditoría.

# Objetivos

**General**

El Curso tiene como objetivo general que los participantes adquieran herramientas que les permitan comprender el impacto que tiene la incorporación de las tecnologías de la información y las comunicaciones en la gestión de los organismos y sus implicancias en las tareas de auditoría e implementación de controles.

###### Específicos

* Entender los fundamentos de una auditoría informática;
* Adquirir el conocimiento básico para abordar auditorías en áreas técnicas.
* Lograr desarrollar un Plan de Auditoría con Programas de auditoría informática.
* Poder evaluar los riesgos asociados a los recursos informáticos vinculados a los sistemas existentes;
* Conocer las principales normas con implicancias para las tecnologías de la información.
* Identificar los controles aplicables frente a los riesgos detectados y se encuentren en condiciones de verificar su existencia y efectividad;

# Contenidos

#### 

#### Módulo 1: Introducción a la auditoría de sistemas y a los controles informáticos.

Terminología de Auditoría Informática. El entorno informático. Necesidad e importancia de la Auditoría Informática. Conceptos de Seguridad de Tecnologías de Información. Ciclo de Auditoría. Plan de Auditoría. Programa de Auditoría. Riesgos de Auditoría. Controles: Concepto y clasificación, Controles general de TI, Controles de aplicación. Evidencia de Auditoría. Pruebas de cumplimiento y sustantivas. El informe de Auditoría

#### Módulo 2: Riesgo

Importancia de la información. Actores y responsabilidades. Concepto y tipos de riesgos. Principio de los riesgos. Principales amenazas. Marcos y estándares de gestión de riesgos. Factores y escenarios de riesgo. Proceso de gestión de riesgo. Importancia de la Auditoría.

#### Módulo 3: Sistema de control interno y organización del área informática

El sistema de control interno. Organización del área de sistemas. Concepto de Seguridad de la Información. Roles y perfiles del área informática. Políticas, normas y procedimientos. Estándares tecnológicos nacionales e internacionales aplicables.

#### Módulo 4: Auditoría en el ciclo de vida de desarrollo de sistemas.

Riesgos en los aplicativos. Auditoría del ciclo de vida de los sistemas. Modelo de madurez del desarrollo de sistemas. Herramientas de auditoría para incorporar en los procesos.

#### Módulo 5: Auditorías de Planes de contingencia.

Planes de Contingencia. Qué se necesita para recuperarse de un desastre. Pruebas del Plan de Contingencia. Programa de Auditoría para evaluar un Plan de Contingencia.

#### Módulo 6: Cumplimiento

Auditoría de Cumplimiento. Leyes aplicables: Firma Digital, Habeas Data, Delito Informático, Propiedad intelectual. Normativa interna.

# Estrategias metodológicas y recursos didácticos

#### El Curso es de naturaleza virtual e interactiva. El acceso al Curso se realizará a partir de la página web http//:www.lapiedad.org.ar, Sector Campus Virtual – Capacitación a distancia, que permite ingresar a la plataforma http://campus.apoc.org.ar/. Los cursantes inscriptos contarán con nombre de usuario y contraseña.

Los recursos didácticos utilizados en el curso son:

1. Presentaciones de cada módulo.
2. Notas complementarias por módulo.
3. Cuestionarios de evaluación multiple choice por módulo tipo.
4. Material de lectura.
5. Foro de debate.

Recorrer y completar los objetivos de aprendizajes de cada módulo habilita a acceder al módulo siguiente.

# Bibliografía

**Normativas de lectura obligatoria**

* Ley Nro. 25506 de Firma Digital http://www.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
* Ley Nro. 25036 de Propiedad Intelectual

http://www. infoleg.mecon.gov.ar/txtnorma/54178.htm

* Ley Nro. 25326 de Habeas Data

http://www .infoleg.mecon.gov.ar/txtnorma/64790.htm

* Ley Nro. 26.388 Delito Informático http://www.infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=141790

# Recomendada

#### 

*“Normas Internacionales y Nacionales vinculadas a la Seguridad Informática* -2009 *–* Marcia Maggiore y Patricia Prandini – Editorial Osmar Buyatti

*Auditoría en Informática, 2da edición* – Enrique Hernández Hernández – Editorial Cecsa

*¿Qué es la seguridad informática? – 2014* - Dr. Hugo Scolnik – Ed. Paidos

*Information Technology Control and Audit –* Fourth Edition – Senft, Gallegos y Davis - Editorial CRC Press

*Lectura en portal de la Asociación de Auditoría y Control de Sistemas de Información ( ISACA)*: http://www.isaca.org/spanish/Pages/default.aspx

* [COBIT 4.1 (Spanish)](http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf)
* [Código de Ética Profesional de ISACA](http://www.isaca.org/About-ISACA/History/Espanol/Documents/ISACA-Code-of-Ethics-Spanish.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2001 Estatuto de Auditoría](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2001_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2002_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2003 Independencia Profesional](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2003_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2004_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2005_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2006 Competencia](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2006_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2007 Afirmaciones](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2007_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2008 Criterios](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2008_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2201 Planificación de la asignación](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2201_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2202_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2203_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2204 Materialidad](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2204_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2205 Evidencia](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2205_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2206_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2207_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2208 Muestreo](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2208_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2401 Reportes](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2401_gui_Spa_0415.pdf)
* [Guías de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2402_gui_Spa_0415.pdf)
* [Acortando la brecha entre el acceso y la seguridad en grandes conjuntos de datos](http://www.isaca.org/Journal/archives/2014/Volume-6/Documents/Bridging-the-Gap-Between-Access-and-Security-in-Big-Data_joa_Spa_1114.pdf)
* [La función de seguridad de la información](http://www.isaca.org/Journal/archives/2014/Volume-6/Documents/The-Information-Security-Function_joa_Spa_1114.pdf)
* [Controles Estratégicos y Operacionales de la TI](http://www.isaca.org/Journal/archives/2014/Volume-2/Documents/IT-Strategic-and-Operational-Controls_joa_Spa_0414.pdf)
* [La Inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo](http://www.isaca.org/Journal/archives/2013/Volume-6/Documents/Information-Insecurity_jrn_Spanish_1113.pdf)
* [Medición y elaboración de informes de riesgos tecnológicos](http://www.isaca.org/Journal/Documents/11v6-Technology-Risk-Measurement-and-Reporting-spanish.pdf)
* [La integridad de los datos: el aspecto más relegado de la seguridad de la información](http://www.isaca.org/Journal/Documents/11v6-Data-Integrity-Information-Securitys-Poor-Relation-spanish.pdf)
* [Cómo el Auditor de TI Puede Hacer Contribuciones Sustanciales a una Auditoria Financiera](http://www.isaca.org/Journal/archives/2011/Volume-1/Documents/jpdf11v1-how-the-IT-auditor-spanish.pdf)
* [Prevención de fuga de datos](http://www.isaca.org/Knowledge-Center/Research/Documents/Data-Leak-Prevention_whp_Spa_0211.pdf)
* [Alineando Cobit 4.1, ITIL v3 y ISO 27002 en beneficio de la empresa v2,7](http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf)
* [Marco de Riesgos de TI](http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Spa_0610.pdf)

# Evaluación de los aprendizajes

#### Los participantes serán evaluados en función de haber completado las lecturas de las Notas y de las presentaciones de filminas, haber participado en los foros de discusión y aprobado el cuestionario Multiple Choice de cada Módulo.

# Perfil de los instructores:

**Jorge N. Nunes**

Especialista en auditoría, seguridad, control de Sistemas de información y evaluación de riesgos y controles. Desarrollo e implementación del Sistema de Gestión de Auditoría por Procesos.

Participación en proyectos de Aseguramiento, Control y Seguridad de Sistemas de Información. Mejoras de Procesos y Buen Gobierno de TI. Políticas y Procedimientos. Marcos de Control Interno y de TI, ITIL e ISO. Participación, con la Dirección Nacional de Datos Personales, de la normativa regulatoria de la Ley de Habeas Data.

Capacitador y conferencista nacional e internacional de Auditoría, procesos, riesgos y controles informáticos. Capacitador en Metodología COBIT.

### Gerente Departamental de Organización y Procesos del Banco de la Nación Argentina.

### Director de la Empresa COELSA (Compensadora Electrónica S. A.).

### Ex Subgerente Departamental de Auditoría de Sistemas del Banco de la Nación Argentina.

### Ex Gerente de Auditoría de Sistemas en la Administración Nacional de Seguridad Social (Anses).

### Docencia

### Universidad Católica Argentina (UCA): Profesor de la materia “Auditoría de Sistemas” para la carrera de Ingeniería Informática.

### Universidad Nacional de San Martín (UNSAM) Profesor de la materia “Auditoría de Sistemas” para la Maestría en Auditoría Gubernamental.

### Certificado Internacionalmente en Auditoría de Sistemas -Certified Information System Auditor, CISA - Otorgada mundialmente por la Asociación de Auditoría y Control de Sistemas de Información (ISACA – Information Systems Audit and Control Association).

### Ex Presidente del Capítulo Buenos Aires de la Information Systems Audit & Control Association –ISACA- (Periodo 2001/2005). Actualmente responsable de la Comisión de Nominaciones.

# Patricia Prandini

Es Contadora Pública y Magister en Seguridad Informática de la Universidad de Buenos Aires (UBA) y Master of Accounting Science con especialización en Sistemas de Información de la Universidad de Illinois, EEUU. Tiene certificaciones internacionales en Auditoría de Sistemas y (CISA) y Riesgo (CRISC) de ISACA y fue Presidente del Capítulo Buenos Aires de dicha Asociación (2010 a 2012). Es Docente de Auditoría de Sistemas y Seguridad Informática en la UBA y la Universidad Nacional de San Martín. En su carrera profesional participó en el desarrollo de la Infraestructura de Firma Digital de la República Argentina, en el primer equipo de respuesta a incidentes de seguridad informática (ArCERT) y en el primer portal gubernamental. Ha publicado diversos artículos en revistas nacionales e internacionales.

# Requisitos de asistencia y aprobación

Cumplimentar las obligaciones del 100% de los módulos a lo largo de seis (6) semanas y resolver los Cuestionarios Múltiple Choice.

# Duración en horas

Se estima que el tiempo efectivo y requerido para cumplimentar con las obligaciones del curso es de 30 horas reloj, distribuidas a lo largo de seis (6) semanas.

# Cronograma

El curso comenzará a dictarse el día 14 de Agosto de 2017, finalizando el 22 de Septiembre de 2017.

# Lugar de realización

Centro de Estudios La Piedad – Asociación del Personal de los Organismos de Control. Capital Federal, Bartolomé Mitre 1419 1º B, Ciudad Autónoma de Buenos Aires.