Seguridad en los Sistemas de Información
Ordenanza 1877

Datos administrativos de la asignatura			
Departamento:	Ingeniería en Sistemas de Información	Carrera	Ingeniería en Sistemas de Información
Asignatura:	Seguridad en los Sistemas de Información		
Nivel de la carrera	Quinto Nivel	Duración	Cuatrimestral
Bloque curricular:	Tecnologías Aplicadas	Área	Sistemas de Información
Carga horaria presencial semanal:	6 hs.cátedra (4,5 hs reloj)	Carga Horaria total:	96 hs.Cátedra (72 hs. Reloj)
Profesor/es Titular/Asociado/Adjunto :	Eduardo Galeazzi (Resp.)	Dedicación:	Adjunto 1DS (Int.)
Auxiliar/es de 1°/JTP:		Dedicación:	

PROPÓSITO

Brindar al futuro profesional las habilitades, métodos, procedimientos de análisis y gestión necesarios para analizar, diseñar, implementar, operar, mantener, controlar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) con el fin de proteger la continuidad operativa, la confiabilidad y confidencialidad de la información y el aporte de información a las decisiones gerenciales, actuando con ética, responsabilidad profesional y compromiso social y ambiental.

Objetivos secundarios

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos de seguridad.
- Identificar y ser capaz de justipreciar los riesgos en un escenario organizacional, técnico, social y normativo determinado., elaborando planes de contingencia y recuperación.
- Implementar y operar un SGSI, que permita además gestionar los riesgos asociados a la seguridad de la información, monitoreando y revisando su desempeño y efectividad, proponiendo mejoras continuas en base a la medición de objetivos.
- Formar habilidades necesarias para revisar con efectividad los controles relativos a los sistemas de información y contribuir de manera eficiente en la gestión de la organización.
- Aplicar metodologías que permitan resolver situaciones concretas en el campo de la auditoría Informática, evaluando su resultado e impacto en la organización.
- Comprender el proceso de peritaje informático y el tratamiento de evidencias.
- Comunicarse efectivamente y aprender en forma continua y autónoma.

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Objetivos establecidos en el DC

- Aplicar modelos de referencia en la gestión de la seguridad de la información según normas vigentes.
- Planificar controles de seguridad basados en la gestión de riesgo.
- Desarrollar un plan de seguridad asegurando la continuidad del negocio.
- Comprender el proceso de auditoría y tratamiento de evidencias.

RESULTADOS DE APRENDIZAJE

RA	Unidad temática	Definición	Aporta a
RA1	U1	**Aplica** correctamente los conceptos generales de seguridad en los sistemas de información en sus dimensiones físicas, lógicas, relativas a RRHH, políticas gerenciales, normativas; en su expresión oral y escrita en el marco de un proyecto de seguridad en el que deba actuar.	CG-1 Identifica CE-2.1 Seguridad CE-3.1 Reconocer normas CG-7 Comunicación efectiva
RA2	U1 – U2	**Especifica** el **BCP** (Business Recovery Plan) y el **DRP** (Disaster Recovery Plan) realizando análisis de riesgos, con el objetivo de mejorar la capacidad de gestión de las contingencias, asegurar la continuidad del negocio o actividad propia de la empresa y elaborar informes a la gerencia.	CG-1 Identifica, formula CG-2 Concibe CG-3 Planifica, controla CE 1.1 Especificar CE 2.1 Seguridad CE 3.1 Reconocer métricas y normas CG-8 Saber ser
RA3	U3	**Gestiona (**planifica, implementa, controla) un SGSI (Sistema de Gestión de la Seguridad de la información), con el objetivo de establecer un proceso de mejora continua de los niveles de seguridad informática en cualquier organización.	CG-1 Identifica, formula, resuelve CG-2 Concibe, diseña, desarrolla CG-3 Gestiona, planifica, ejecuta, controla CG-4 Utiliza técnicas CG-5 Potencial CE 2.1 Seguridad CE 3.1 Reconocer métricas y normas CE 4.1 Mejora continua del plan CE 5.1 Dirigir y gestionar CG-6 Trabajo en equipo CG-7 Comunicación efectiva CG-8 Saber ser
RA4	U4	**Implementa** planes de **Auditoría** informática; con el objetivo de realizar comprobaciones, documentar resultados, medir desvíos y elaborar/criticar informes de auditoría.	CG-1 Identifica, formula, resuelve CG-2 Concibe, diseña, desarrolla CG-3 Controla CG-4 Utiliza técnicas

DIRECCIÓN ACADÉMICA
COPIA FIEL DEL ORIGINAL
MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

			CE 2.1 Seguridad CE 3.1 Reconocer métricas y normas CE 4.1 Resultados de la auditoría CE 5.1 Dirigir y gestionar CG-6 Trabajo en equipo CG-7 Comunicación efectiva CG-8 Saber ser
RA5	U5	Realiza pericias y arbitrajes mediante la aplicación de los marcos legales y técnicos y la utilización de métodos apropiados de recolección de evidencias y elaboración de informes con el fin de poder desempeñarse como auxiliar de la Justicia o la Gerencia.	CG-1 Resuelve CG-4 Utiliza técnicas CE 2.1 Seguridad CE 3.1 Reconocer normas CE 4.1 Resultados de la pericia CE 7.1 Realizar pericias y arbitrajes CG-7 Comunicación efectiva CG-8 Saber ser
RA6	Todas	**Participa** activa y colaborativamente en la resolución de trabajos individuales y en equipo aplicando las competencias adquiridas en el tiempo y la forma solicitadas.	CG-6 Trabajo en equipo CG-7 Comunicación efectiva CG-8 Saber ser

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Asignaturas correlativas previas
Para cursar, el estudiante debe tener: Cursada: • Redes de Daros • Administración de Sistemas de Información Aprobada • Desarrollo de Software • Comunicación de Datos

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL
MARÍA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

DESCRIPCIÓN de la MEDIACION PEDAGOGICA. Metodología de enseñanza
Se busca desarrollar el potencial del estudiante en las tres áreas del saber (conocer, hacer y ser). Se dictarán clases expositivas dialogadas en forma presencial. Se estima un 30% del tiempo dedicado al análisis y discusión de casos reales, ejemplos del ejercicio profesional, lecturas, elaboración y discusión trabajos de proyecto en comisiones. El desarrollo de la materia incluirá la presentación de los temas a tratar desde el punto de vista teórico para brindar los fundamentos de conocimientos básicos requeridos en forma expositiva y dialogada, complementando con actividades y lecturas seleccionadas y sugeridas. Se aplicarán los conocimientos adquiridos aplicándolos en uno o más casos de estudio (*) y la inclusión de espacios de trabajos prácticos a modo de taller para familiarizar a los alumnos con las metodologías, técnicas y herramientas analizadas. (*) Se procura que los estudiantes analicen empresas reales cuando se tiene acceso a ellas, caso contrario se los apoya en la definición de situaciones simuladas. Invitaremos a profesionales especialistas en determinadas temáticas, para fortalecer la profundización y comprensión de algunos temas, abriendo a nuevas visiones. Se prevé tiempo para clases de repaso previas a las evaluaciones parciales con el fin de aclarar, profundizar y discutir las interrelaciones entre los temas previamente presentados.
RECOMENDACIONES PARA EL ESTUDIO
La característica transversal de la Seguridad a todos los aspectos de la gestión de los Sistemas de Información es un desafío y al mismo tiempo una oportunidad de nivelar y cruzar conocimientos y conceptos vistos en asignaturas previas. Visualizar y comprender esas relaciones es deseable y conveniente, para lo cual es muy recomendable llevar la materia al día. Se estima que el alumno debe disponer en promedio 2hs a 3hs semanales adicionales a las clases formalmente establecidas. Esto le permitirá realizar las lecturas recomendadas, monografías y TP's como un proceso continuo de aprendizaje, logrando una mejor asimilación de los conceptos y su aplicación, para poder alcanzar los resultados buscados.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

CRITERIOS DE EVALUACIÓN de los Resultados de Aprendizaje. Rúbrica
Se interpreta por SABER, como conjunto del SABER **CONOCER (teoría)**, SABER **HACER (práctica)** Y SABER **SER (desempeño, actitud)**. La presente rúbrica resume las expectativas y logros esperados del estudiante, considerando un perfil de egreso que persigue la conjunción de un amplio conocimiento tecnológico, la capacidad de resolver problemas aplicando técnicas y herramientas, en el marco de un eficiente y ético desempeño profesional; social y ambientalmente responsable.
Peso: Todos los RA tienen el mismo peso: 20%.

RA	No alcanza los saberes mínimos	Alcanza mínimamente los saberes	Alcanza satisfactoriamente los saberes	Alcanza muy satisfactoriamente los saberes
RA1 Conceptos de Seguridad de la Información U 1	No conoce los conceptos básicos y normas y/o no es capaz de utilizarlos / relacionarlos correctamente.	Conoce las definiciones en forma individual, pero tiene dificultad para articularlas correcta y apropiadamente.	Conoce las definiciones en forma individual, y puede articularlas correcta y apropiadamente.	Conoce las definiciones en forma individual, y puede articularlas muy criteriosa y justificadamente, aplicándolas a casos reales.
RA2 Análisis de riesgos y continuidad de negocio U 2	No reconoce las amenazas y riesgos o las acciones necesarias para su gestión.	Identifica amenazas y riesgos, pero no alcanza a ponderar su impacto y criticidad en el S.I.	Identifica amenazas y riesgos, ponderando su impacto y criticidad en el S.I.	Identifica amenazas y riesgos, ponderando muy criteriosa y justificadamente su impacto y criticidad en un S.I. determinado.
RA3 Gestión de riesgos U 3	No conoce o no alcanza a aplicar las técnicas, controles y herramientas apropiadas para gestionar un S.G.S.I.	Conoce y aplica mínimamente las estrategias, técnicas, controles y herramientas apropiadas para gestionar un S.G.S.I.	Conoce y aplica correctamente las estrategias, técnicas, controles y herramientas apropiadas para gestionar un S.G.S.I.	Conoce y aplica correctamente las estrategias, técnicas, controles y herramientas; siendo flexible, práctico e innovador para gestionar un S.G.S.I. determinado.
RA4 Auditoría U 4	No reconoce los conceptos necesarios para gestionar una auditoría y/o comprender el rol del auditor.	Reconoce los conceptos, pero no alcanza a poder planificar acciones de auditoría.	Puede planificar acciones de auditoría, evaluar los resultados y expresarlos en un informe.	Puede profundizar en análisis de casos más complejas, elaborando informes detallados.
RA5 Peritaje U 5	No reconoce los conceptos necesarios para gestionar una pericia y/o comprender el rol del perito.	Reconoce los fundamentos, pero no alcanza a poder planificar una pericia.	Puede planificar y ejecutar una pericia, evaluar los resultados y expresarlos en un informe.	Puede profundizar en análisis de situaciones más complejas, elaborando informes detallados.
RA6	No interviene o es	Baja participación en	Aceptable participación	Destacada participación en

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Participación y proactividad Todas	casi nula su participación en clase ni cumplimenta las lecturas previas a clase, no demuestra interés por el trabajo en equipo ni en alcanzar los resultados de aprendizaje.	clase y ocasional cumplimiento de las lecturas previas a clase. Bajo interés por el trabajo en equipo.	en clase y demuestra seguir la asignatura al día. Buen desempeño en equipo.	clase, demuestra seguir la asignatura al día, realizando aportes o preguntas valiosas en sus intervenciones. Buen desempeño en equipo.
Dominios que se evalúan	Expresión oral y escrita Dominio de conceptos	-Expresión oral y escrita. -Dominio de conceptos -Participación en clase -Trabajo en equipo -Calidad de presentaciones y exposiciones -Originalidad y proactividad	-Expresión oral y escrita -Dominio de conceptos -Participación en clase -Trabajo en equipo -Oportunidad de entregas -Calidad de presentaciones y exposiciones -Originalidad y proactividad	--Expresión oral y escrita Dominio de conceptos -Participación en clase -Trabajo en equipo -Oportunidad de entregas -Calidad de presentaciones y exposiciones -Originalidad y proactividad
Calificación rúbrica	No califica. Debe recursar.	Aprueba cursada. Debe rendir final.	Aprobación directa. Aprueba con promoción.	
Calificación numérica	Menos de 4	4-5	6-7-8	9-10
Acreditación	Para aprobar la cursada el estudiante debe "Alcanzar mínimamente los saberes" de **todos** los Resultados de Aprendizaje (RA), completar el 75% de asistencia a clases y completar 100% de los trabajos prácticos/evaluaciones/coevaluaciones y monografías.			
Aprobación directa	Para aprobar la asignatura por promoción el estudiante debe "Alcanzar satisfactoriamente los saberes" como mínimo en **todos** los Resultados de Aprendizaje (RA).			
Aprobación no directa	En el caso de no alcanzar la aprobación directa, habiendo aprobado la cursada, el estudiante deberá rendir examen final para aprobar la asignatura.			

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

EVALUACIÓN. ACREDITACIÓN DE SABERES
La acreditación resulta de la combinación entre parciales, TP, autoevaluaciones, coevaluaciones, monografías y exposiciones. Cada actividad puede contribuir en distinta proporción a la validación de los Resultados de Aprendizaje.

Referencias:

ESx	Evaluación sumativa/ Coevaluación x	P.x	Parcial x
Mx	Monografía	RP.x	Recuperatorio Parcial x
U.x	Unidad x	TP.x	trabajo Práctico x
RA	Resultado de aprendizaje	Ev.In.	Evaluación Integradora

(las siguientes actividades figuran en el CRONOGRAMA y servirán para la acreditación)

Id.	Actividad de evaluación	Requisito	Contribución a los RA (c/u 20%)				
			RA 1	RA 2	RA 3	RA 4	RA 5
ES1 Evaluación sumativa/ Coevaluación	Autoevaluación 1 : Conceptos de seguridad	Completo	15%				
ES2 Evaluación sumativa/ Coevaluación	Autoevaluación 2 : Normas aplicables.	Completo	15%				
TP1.1 Trabajo en equipo	Análisis de riesgo.	Completo expuesto	30%				
ES3 Evaluación sumativa o Coevaluación	Autoevaluación 3 : BCP	Completo		15%			
P1 Evaluación sumativa	1er Parcial o integradora	Rendido	40%	40%	20%		
M1 Evaluación formativa	Monografía (individual)	Completo			20%		
TP1.2	BCP. Desarrollo y	Completo		45%			

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Trabajo en equipo	exposición plan de contingencia	expuesto					
ES4 Evaluación sumativa o Coevaluación	Autoevaluación 4: Firma digital	Completo			15%		
TP2 Trabajo en equipo	Práctico herramientas de seguridad ofensiva	Completo			15%		
TP3.1 Trabajo en equipo	TP 3.1 Caso de Estudio Auditoría	Completo				30%	
TP3.2 Trabajo en equipo	TP 3.2 Informe auditoría	Completo Expuesto				30%	
ES5 Evaluación sumativa/ Coevaluación	Autoevaluación 5 Práctica Pericial	Completo					40%
P2 Evaluación sumativa	2do Parcial o integradora	Rendido			30%	40%	60%
			RA 1	**RA 2**	**RA 3**	**RA 4**	**RA 5**

Recuperación: El estudiante que no alcance los mínimos de los resultados de aprendizaje en alguna de las evaluaciones parciales tendrá dos instancias de recuperación por cada evaluación según la planificación definida; existiendo también la posibilidad de un recuperatorio flotante (integradora) al final de la cursada que le acreditará la totalidad de los saberes en el nivel requerido.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

PROGRAMA ANALITICO. Unidades temáticas
Nota: las Unidades se relacionan 1 a 1 con los resultados de aprendizaje (RA).

UNIDAD Nº 1: MARCO CONCEPTUAL Y GENERALIDADES. NORMAS APLICABLES.

Definición de información, procesos y sistemas de información.
Activos informáticos. Amenazas. Clasificación. Confidencialidad, disponibilidad, integridad.
Legalidad. Concepto del marco normativo y del control interno.
Propósito y objetivos de los Sistemas de Gestión de Seguridad de la Información (SGSI).
Organismos y certificaciones internacionales relacionadas.
Aspectos normativos y marco referencial: ISO/IEC 27001-2 y familia, Protección de Datos Personales, Delitos Informáticos, Firma Digital, Comunicación BCRA A-4609/5374, COBIT, PCI y SOX.

Tiempo asignado: 12 hs cátedra – 9 hs.reloj Tiempo estimado fuera del aula: 6hs.reloj

UNIDAD Nº 2: RIESGOS Y CONTINUIDAD DEL NEGOCIO

Evolución y convergencia tecnológica.
Amenazas y vulnerabilidades asociadas a las TICs.
Tipos de ataques y amenazas: malware, virus informático, denegación de servicios (DoS), phishing, robo de información, robo de identidad, fraude informático, ransomware.
Estándares y mejores prácticas de la gestión de riesgos. Métricas.
ISO/IEC 27005: recomendaciones y directrices generales para la gestión de riesgo en el SGSI.
Riesgo, decisión e incertidumbre. Evaluación, tratamiento, aceptación, seguimiento y revisión del riesgo de seguridad de la información.
Continuidad del negocio. Aspectos fundamentales para la confección del Business Continuity Plan (BCP) y Disaster Recovery Plan (DRP).

Tiempo asignado: 15hs cátedra / 12 hs.reloj. Tiempo estimado fuera del aula: 15hs.reloj.

UNIDAD Nº 3: GESTION DE LA SEGURIDAD DE LA INFORMACION

Marco de referencia ISO/IEC 27001 y su relación con la normativa ISO/IEC 27002.
Objetivos de seguridad y controles.
Metodología para la implementación y mantenimiento de un SGSI.
Manual de políticas y normas de seguridad de la información.
Organización interna, funciones y responsabilidades de seguridad.
Control de accesos, criptografía y mecanismos de autenticación.
Firma digital. Características y configuraciones de claves seguras.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL
MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Gestión de usuarios, perfiles y accesos. Segregación de funciones.
Seguridad física y medioambiental: áreas seguras y equipamientos.
Seguridad lógica: sistemas operativos, bases de datos, herramientas de trabajo, redes de comunicación, ataques en redes, sistemas aplicativos, accesos a Internet, protección contra el malware, logs. Hacking ético, seguridad ofensiva.
Requisitos de seguridad en la adquisición de los sistemas de información, desarrollo y mantenimiento.
Separación de los entornos de trabajo. Procedimientos de resguardo y verificación de copias de seguridad. Gestión de incidentes de seguridad de la información.
Integridad referencial y transaccional.

Tiempo asignado: 21hs cátedra / 15.75hs.reloj

UNIDAD Nº 4: AUDITORIA INFORMATICA

Normativa internacional ISO 19011: Directrices para la auditoría de los Sistemas de Gestión. Características y principios básicos de auditoría y la profesión del auditor. Definición de auditoría informática, principales desafíos y áreas de responsabilidades.
Clasificación de tipos de auditoría informática, fases y técnicas. Código de ética del auditor. Metodologías para la Gestión de la Auditoría Informática. Clasificación y evaluación de controles. Planes y programas de auditoría. Asignación de recursos e integración de equipos de trabajo. Definición de criterios, técnicas y herramientas de auditoría.
Auditorías a instalaciones físicas, seguridad lógica en bases de datos, redes, aplicaciones y ofimática, ciclo de vida en el desarrollo de software, outsourcing de TI.
Ejecución del proceso de auditoría, entrevistas, pruebas, evidencias y documentación de respaldo. Evaluación de hallazgos, redacción de comentarios y reunión preliminar.
Confección y presentación del informe de auditoría.

Tiempo asignado: 21hs.cátedra / 15.75 hs reloj

UNIDAD Nº 5: PERITAJE INFORMATICO

El rol del perito informático y las pruebas. El proceso judicial.
La designación y aceptación. Requisitos para ser perito, deberes y obligaciones.
Las etapas de una pericia. Análisis de Tipos de casos y de incidentes.
Adquisición, registro y análisis de las evidencias.
Requisitos y validez de las pruebas.
Herramientas para la copia y el registro de evidencias.
El Informe pericial.

Tiempo asignado: 10hs.cátedra / 7.5hs.reloj

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL
MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

RECURSOS NECESARIOS

- Aula acorde a la cantidad de inscriptos
- CVG
- Zoom para clases virtuales o revisión de TP's
- En el aula: Cañón y pizarra. Acceso a Internet
- Disponibilidad en biblioteca de material obligatorio

*Posible necesidad de afrontar gastos de viaje de expositor invitado en caso de visita presencial.

BIBLIOGRAFÍA

OBLIGATORIA

Martínez, J.G. (2010). *El plan de continuidad del negocio. Guía práctica para su elaboración,* Editorial Díaz de Santos
ISBN: 978-84-7978-793-6 (Versión electrónica) 978-84-7978-793-3 (Versión impresa)

Esta obra proporciona los elementos prácticos necesarios para la elaboración de un BCP y deja claro que aún en una misma organización, en momentos diferentes o con equipos diferentes, los planes no tienen porque coincidir.

Gómez Vieites, A. (2014). *Enciclopedia de la seguridad informática,* Editorial Ra-Ma
ISBN 978-84-9964-394-6

Aborda globalmente la problemática de la Seguridad Informática y la Protección de Datos, contemplando tanto los aspectos técnicos, como los factores humanos y organizativos.

Piattini Velthuis, M. y al. (2008). *Auditoria de tecnologías y sistemas de información*, Alfa-Omega Grupo Editor o Editorial Ra-Ma
ISBN 978-84-7897-849-6 (Edición impresa)

Presenta los conceptos fundamentales sobre control interno y auditoría de TSI, ofrece un tratamiento sistemático de las técnicas y métodos del auditor informático.

Luis Enrique Arellano González, L.E. y Darahuge, M.E., *Manual de informática forense*, ERREPAR
ISBN 978-987-01-1681-3

Provee elementos para realizar la gestión de la prueba documental informática, y proponiendo ejercicios prácticos resueltos.

International Organization for Standardization (2005). *Código de Práctica para la Gestión de la Seguridad de la Información (*ISO/IEC 17799). Digital uso académico

International Organization for Standardization (2013). *Information Technology. Security Techniques. Information Security Management* (ISO/IEC 27001.) ISO-IRAM, 2013

International Organization for Standardization (2013). *Information Technology. Security Techniques. Code of Practice for Information Security Management* (ISO/IEC 27002).

ES COPIA FIEL DEL ORIGINAL
DIRECCIÓN ACADÉMICA
MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

ISO-IRAM, 2013

COMPLEMENTARIA

BCRA. (2017) Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades Financieras (COMUNICACIÓN "A" 6354 y "A" 6375)

Fanjul, A. (2016). Ethical hacking (ebook). Ed.Autores de Argentina
ISBN: 978-987-711-551-2
Metodología y herramientas para realizar un Penetration Test exitoso, así como diversas técnicas de ataque y de explotación de vulnerabilidades.

Sosa, T.E. (2006). Peritos judiciales: teoría y práctica para la actuación procesal. Librería Editora Platense
ISBN 9505361823, 9789505361823
Presenta de teoría y práctica de la actuación procesal.

Erickson, J. (2008). Hacking: the art of exploitation, 2nd edition. Ed. No Starch Press, Inc. 2008
ISBN: 978-1-59327-144-2
The goal of this book is to share the art of hacking with everyone.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL
MARÍA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP