Atizapán de Zaragoza a 16 de agosto 2019

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS CIUDAD DE MEXICO
ESCUELA DISEÑO, INGENIERIA Y ARQUITECTURA
DEPARTAMENTO DE COMPUTACION

Datos curso y profesor

Materia: Seguridad Informática **Clave-Gpo:** TC2027-01
Carrera: 6 ISC05, 6 ISI05, 6 ITC05, 8 ITIC08, 6 ITC08, 6 ISC08, 8 ITC09, 8 ISC09
Requisito: Haber cursado TC2002 (Redes II) y TC2008 (Sistemas Operativos)
Profesor: Dr. Roberto Gómez Cárdenas **Cubículo:** Sin Oficina, Profesor de Cátedra
e-mail: `rogomez@itesm.mx` **twitter:** `@cryptomex`
Home Page: `http://cryptomex.org`

Objetivo General

Al finalizar el curso el alumno tendrá una visión general de área de seguridad informática con los fundamentos necesarios para entender los riesgos, amenazas, vulnerabilidades a los que se ven sometidos los sistemas computacionales en la actualidad, así como los controles y métodos de protección contra posibles ataques, que son necesarios para el funcionamiento adecuado de estos sistemas en la empresa moderna. Además conocerá el estado actual de las leyes que competen a la seguridad de sistemas informáticos en el ámbito nacional e internacional.

Competencias

- Distinguir los conceptos básicos de la seguridad informática en un ambiente real.
- Evaluar una política de seguridad de una empresa.
- Aplicar recursos criptográficos para asegurar la confidencialidad y autenticidad de la información.
- Seleccionar los mecanismos adecuados para cubrir los requerimientos de seguridad informática de una organización.
- Identificar los diferentes tipos de código malicioso y sus contramedidas.
- Listar los elementos de la legislación mexicana e internacional vigente, aplicados a la seguridad informatica.
- Relatar las tendencias de investigación en el área de seguridad computacional.

Contenido Temático Oficial

Durante el curso se abordarán los siguientes temas:

1. Conceptos básicos
    - Estrategia de seguridad informática
    - Mecanismos de seguridad informática
    - Actores en el área de seguridad informática

- Certificaciones en el área de seguridad informática

2. Políticas de Seguridad
   - Conceptos básicos de políticas de seguridad
   - Análisis de riesgos
   - Elaboración de políticas de seguridad
3. Criptologia
   - Criptografia simétrica
   - Criptografia asimétrica
   - Criptografia e integridad de información
   - Criptografía y autenticidad
   - PKI
   - Redes privadas virtuales (VPNs)
4. Herramientas de Seguridad
   - Analizadores de protocolos
   - Analizadores de vulnerabilidades
   - Firewalls
   - Sistemas de detección de intrusos
5. Código malicioso
   - Ataques a nivel aplicación
   - Metodologías de mitigación
6. Legislación informática
   - Legislación mexicana
   - Legislación internacional
7. Tendencias futuras

Recursos Didácticos

- *Security in Computing*, C. Pfleeger, Prentice Hall, 1996, 2nd edition
- *IT Auditing: Using Controls to Protect Information Assets* Chris Davis,Mike Schiller,Kevin Wheeler, McGraw-Hill Osborne Media; 2006
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Bruce Schneier, 1995, 2nd Edition
- *Practical Cryptography* Niels Ferguson, Bruce Schneier; Ed. Wiley; 2003
- *Network Intrusion Detection*, Stephen Northcutt, Judy Nova Ed. Sams; 2002, 3 edition
- *Computer Security Basics*, D. Russell and G.T. Gangeni, O'Reilly & Associates; 1991
- *Network Security, Private Communication in a Public World*, C. Kaufman, R. Perlman, M. Speciner, Ed. Prentice Hall, 2002, 2da. Edición
- *Building DMZs for Enterprise Networks*, R.J. Shimonski, W. Schmied, V. Chang, T.W. Shinder, Ed. Syngress; 2003
- *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems*, S. Northcutt, L. Zeltser, S. Winters, Karen Fredrick, Ronald W. Ritchey, Ed. Sams; 2005, 2da. Edición

Otras fuentes de consulta

- *Podcasts*
  - Security Now
  - Risky Business
  - The Silver Bullet Security Podcast
  - Pauldotcom Security Weekly
  - Crimen Digital
- *Twitter*
  - teamcymru
  - Security by default
  - Help Net Security
  - Fausto Cepeda
  - Adolfo Grego
  - Roberto Martínez
- *Grupos Interés LinkedIn*
  - LFPDPPP
  - Information Security Commun
  - Computer Security Institute (CSI)
  - (ASIMX) Asociación de Seguridad Informática Mexicana
- *Revistas*
  - IEEE Security & Privacy
  - Hakin9
  - Bsecure
- *Sitios web*
  - Security Focus
  - Security by Default
  - El blog de Bruce Schneier
  - El blog de Brian Krebs

Plataforma Tecnológica

- Correo eléctronico
- Twitter
- Podcast
- Blackboard

Fechas de examenes

Las fechas de los examenes ya fueron definidas por el sistema y se encuentran especificadas en el calendario escolar. Este último puede ser consultado a través de la página del campus. Las fechas son fijas y no pueden cambiarse. En base a dicho calendario se definen las siguientes fechas de examenes parciales y final

1er. Parcial:	20 septiembre 2019
2do. Parcial:	25 octubre 2019
Final:	29 noviembre 2019

Evaluaciones

Las ponderaciones para asignar las calificiones parciales, y la calificación final, son las siguientes:

Parciales		**Final**	
Examen:	70 %	Parcial 1:	30 %
Proyecto:	30 %	Parcial 2	15 %
		Examen Final:	20 %
		Proyecto Final:	20 %
		Promedio Tareas:	10 %
		Semana i:	5 %

Los proyectos son opcionales. En caso de que durante un parcial no se haya dejado ningún proyecto, o que decida no hacerlo, la calificación parcial será la obtenida en el exámen.

Al igual que los proyectos parciales, el proyecto final es opcional. Si en la evaluación final no se deja ningún proyecto, o decide no presentarlo, la calificación final se calculará de acuerdo a los siguentes parámetros:

Parcial 1:	40 %
Parcial 2	15 %
Examen Final:	30 %
Promedio Tareas:	10 %
Semana i:	5 %

Políticas del curso

Las siguientes políticas aplican al curso de Seguridad Informática, NO están a discusión y cualquier caso no cubierto en este documento será resuelto de acuerdo al criterio del profesor.

Generales

- El estudiante contará con un lugar fijo asignado por el profesor el cual deberá ocupar durante todo el semestre. Dicho lugar se le asignará el primer día de clases.
- El curso cuenta con una página, en la cual se encuentra parte de la información aquí presentada. La dirección de la página es: `http://cryptomex.org/seguridad.html`.
- **Algunos** temas del curso serán impartidos auxiliandose de acetatos. Estos se encuentran disponibles en la sección de *Material de Apoyo* de la página del curso.

- El temario es el mismo para todos los campus del sistema, si desea obtener una copia puede bajarlo de la página de Planes de Estudio del Sistema:
(`http://serviciosva.itesm.mx/PlanesEstudio/Main.aspx?Form=Busqueda_Materias`
Es obligación del alumno revisarlo.
- Después de 5 minutos de la entrada del profesor al salón, ningún alumno podrá entrar a clase **NO HAY RETARDOS!!!**
- La calificación es sobre 100, por lo que no habra discusiones de redondeo. La calificación mínima aprobatoria es 70.
- Es obligación del alumno revisar constantemente, (al menos una vez al día) su correo electrónico (el asignado por la institución). En cualquier momento el profesor puede enviar mensajes importantes de naturaleza académica a los alumnos.
- Esta estrictamente prohibido utilizar, o tener abierta, cualquier tipo de computadora durante el tiempo que dura la clase. Si un alumno es sorprendido consultando una computadora deberá abandonar el salón de clases, y se le asignará una falta.
- En caso de contar con un teléfono celular o tableta, debe apagarlo al inicio del curso y activarlo al final de la clase.
- Se espera un comportamiento maduro y de respeto por parte del alumno. El alumno que no cumpla con dicho comportamiento deberá abandonar el salón de clases, y se le asignará una falta.
- No portar sombreros o gorras.
- Es importante cuidar el inmobiliario y equipo de computo del salón de clases. No se permite subir los pies en sillas o en otro tipo de mueble. Es necesario asegurarse que los equipos estan apagados, en caso de que estuvieran encendidos, favor de apagarlos.
- Al final de la clase se debe asegurar que los equipos a su alcance estén apagados.

Tareas o actividades

- El termino *actividades* se aplica a las tareas en los cursos rediseñados. En este documento el termino de actividades/tareas se usa indistintamente.
- La fecha de entrega de las tareas, salvo indicación contraria por parte del profesor, es una semana después de que se haya dejado.
- Cualquier evidencia de copia se sancionará de acuerdo a lo estipulado en el Reglamento Académico de Carreras Profesionales.
- Las tareas son individuales, salvo indicación contraria del profesor, y deberán entregarse en el salón de clases **dentro de los primeros cinco minutos del día especificado**. No se aceptará ninguna tarea fuera del salón de clases, ni después de la hora y día convenidos. Evitar excusas como no sirve la impresora, no tengo papel, el servidor no responde, etc.
- La presentación de las tareas debe ser digna de un alumno de nivel licenciatura y elaborada de una manera legible.
- Se manejarán tres tipos de tareas:
  - Lecturas de artículos.
  - Investigaciones/reportes.
  - Programas.

  Cada tipo de tarea cuenta con su propio formato.

- En el caso de las lecturas de artículos, se pedirá un reporte por artículo. Estos reportes deberán contener el resumen, el análisis de las referencias y los comentarios de artículo. El resumen debe ser de tipo ejecutivo,es decir no deberá de exceder el tamaño de una cuartilla. El análisis debe ser lo más consiso y preciso posible, y los comentarios deberán ocupar al menos una página. Los datos a incluir y el formato se encuentran descritos dentro del documento de *formato de lectura de artículos*. Se deben examinar al menos tres referencias del artículo y definir su relación con el artículo analizado.

Requisito	**Porcentaje**
Formato (letra,titulo)	10 %
Calidad del resumen	30 %
Calidad del análisis presentado	30 %
Calidad de las refencias examinadas	30 %

  - En caso de que se indique que no se examinen referencias, el 30 % será repartido entre los 3 otros rubros.

- Los reportes de las investigaciones que se efectuen deberán cumplir con un formato de artículo de investigación. Los datos de la tarea y su autor deben estar centrados en la parte alta de la primera página. El reporte debe estar dividido en secciones. Los datos a incluir y el formato se encuentran descritos dentro del documento de *formato de investigación*.

- Para este tipo de tareas (investigación) se solicita una busqueda bibliográfica de al menos cuatro fuentes, una de estas fuentes NO debe ser electrónica. Una de las fuentes electrónicas debe ser de la biblioteca digital (las bases de datos de la IEEE y ACM son muy buenas fuentes). La estructura de la investigación debe ser lo más lógica posible, evitar realizar copy/paste de las referencias a diestra y siniestra. Se aplicará la siguiente rúbrica para asignar la calificación a este tipo de tareas:

Requisito	**Porcentaje**
Formato (letra,titulo, margenes)	10 %
Secciones presentadas	10 %
Longitud del trabajo	10 %
Referencias	20 %
Calidad de lo investigado (no copy/paste)	50 %

- En el caso de códigos de programas, este debe incluir los datos del código y del autor a nivel comentarios. No se aceptará nada escrito a mano. Los datos a incluir y el formato se encuentran descritos dentro del documento de *formato de códigos de programas*. La sección de programas de este documento proporciona más información con respecto a la entrega de programas. Los programas no deben ser implementados en un plataforma web, NO deben ejecurse desde un navegador.

- Para evitar confusiones, los formatos de las tres tipos de tareas anteriormente mencionados los puede bajar de la página del curso (sección tareas).

- Cada formato cuenta con su propio tamaño de letra el cual se debe respetar.

- En caso de que la tarea ocupe más de una hoja, estas deben estar engrapadas (no clips, no rasgaduras por la esquina).

- No debe entregar la tarea en folders.

- En caso de que no se cumpla con cualquiera de los puntos anteriores se asignará un tercio de la calificación original.

- El lenguaje de presentación de las tareas es el español, tarea en cualquier otro idioma tendrá una calificación de cero.

- Si la tarea debe enviarse por correo electrónico esta debe cumplir con los siguientes puntos:
  - La hora límite de recepción es la hora de inicio de clase, después de esa hora no se tomará en cuenta, no hay excusa de que el servidor no sirve, o de que se tienen problemas con su equipo.
  - La hora de recepción que se toma en cuenta es la de la computadora del profesor, no la del alumno.
  - El subject debe ser: `T<num> Segu` donde `<num>` es el número de tarea. (p.e. `T4 Segu`, es la tarea 4 del curso de Seguridad Informática).
  - El nombre del archivo que contenga la tarea, debe cumplir con el formato: `T<num>-<matricula>`, donde `<num>` es el número de la tarea y `<matricula>` es la matrícula del alumno, (por ejemplo `T5-445566` es la tarea 5 del alumno con matrícula 445566.
  - El cuerpo del correo debe incluir lo siguiente:

    ```
    Envio de la tarea xxx del curso de Seguridad Informatica
    <Descripcion de la tarea>
    <Fecha y hora de envio>
    Nombre completo matricula
    ```

    Debe contar con el nombre completo y matrícula de todos los integrantes del equipo (si es que se dejo en equipo). La descripción de la tarea no debe ocupar más de una línea.

  Tarea que no cumpla con lo anterior no se tomará en cuenta.

Exámenes

- Los exámenes abarcan todo lo visto en el salón de clases, se encuentre en los slides de apoyo, o no. También incluye lo visto y tratado en las tareas.
- Los exámenes deben realizarse de la manera más clara y limpia posible. Respuesta que no se entienda, respuesta que esta mal, (se le asignarán cero puntos).
- Los exámenes se deben contestar con tinta, si el examen no se resuelve con tinta tendra una penalización de 20 puntos.
- Las aclaraciones sobre calificaciones de tareas y/o examenes se harán fuera del salón de clase. Se deberá de concertar una cita con el profesor para tal efecto. La revisión se llevará a cabo en el lugar acordado por ambas partes.
- Después de una semana de entregada la calificación, (tanto de tareas como de examenes), no se aceptará ninguna demanda de aclaración. Esto implica que el alumno esta de acuerdo con dicha calificación.
- Una tarde antes de la aplicación del exámen y el mismo día de su aplicación, no se dará ningún tipo de asesoría.
- Cualquier evidencia de copia se sancionará de acuerdo a lo estipulado en el Reglamento Académico de Carreras Pr ofesionales.

Prácticas de laboratorio

- Durante el curso se llevarán algunas prácticas de herramientas relacionadas con seguridad informática. Estas prácticas estarán basadas en un DVD-Live que contiene la mayor parte de las herramientas. Se les entregará un DVD sobre el cual se llevarán a cabo estas prácticas.

- Es responsabilidad del estudiante el hacer un buen uso de las herramientas contenidas en el DVD arriba mencionado.
- Cualquier mal uso de las herramientas se verá sanciado de acuerdo a lo establecido en el reglamento académico y, si es el caso a la legislación que proceda de acuerdo a la falta.
- En caso de que no haya podido asisitr a la clase donde se llevaron a cabo las prácticas, es la responsabilidad del estudiante (si así lo decide) el preguntar que prácticas se lllevaron a cabo y enviarlas por correo. Cuenta con tres días hablies a partir de la fecha en que se llevaon a cabo para enviarlas. Despu"es de ese tiempo ya no serán tomadas en cuenta.

Programas

Uno de los conocimientos que debe dominar una persona que labora en el área de sistemas es la programación. Durante el curso el alumno implementará diferentes programas. (ya sea como tareas o proyectos), dichas implementaciones deben tomar en cuenta lo siguiente:

- El estudiante es libre de realizar los programas en el lenguaje que desee.
- El sistema desarrollado se probará sobre un sistema operativo windows 7, de 64 bits.
- El sistema debe contar con una interfaz gráfica de fácil uso e intuitiva. No se debe teclear ningún comando por sencillo que este sea, ni debe requerir de algún ambiente de desarrollo para ser ejecutado.
- El sistema debe verificar que el equipo donde se va probar tenga lo necesario y la version requerida (Maquina Virtual Java, .NET, etc). En caso de que se requiera instalar algo el sistema desplegará que se necesita instalar y donde se puede obtener.
- El sistema debe contar con un programa que instale los diferentes componentes del sistema. Como producto final se debe generar un icono de ejecución en el escritorio del equipo donde se probará el programa.
- El sistema debe validar que los datos de entrada a este sean los correctos.
- Los programas no deben ser implementados en uan plataforma web,es decir NO deben ejecurse desde un navegador.
- Se debe enviar por correo electrónico lo siguiente:

  1. Código fuente del programa, debidamente documentado.
  2. Un instalador del programa, el cual tendra como objetivo el instalar el programa en el equipo en que se va a probar.
  3. Un manual de usuario debidamente escrito, así como la huella digital del sistema (hash).
  4. Un diagrama de flujo de como funciona el sistema, una explicación de los diferentes módulos del programa, así como una explicación de la selección del lenguaje en que se desarrollo el sistema.

- Los últimos dos puntos también se deben entregar por escrito.
- Si asi lo considera prudente puede enviar una liga de algun servicio de almacenamiento en la nube donde se deposite el sistema a probar.
- El nombre del archivo que contiene todo lo anterior debe cumplir con la sintaxis comentada en la seccíion de tareas y actividades (`T<num>-<matricula>`).

- Los programas seran evaluados de acuerdo a la siguiente tabla:

Requisito	**Porcentaje**
Documentación	20 %
Facilidad de instalación y manejo del programa	10 %
Validación datos de entrada al sistema	10 %
La ejecución hace lo especificado y sin errores	60 %

Políticas de aplicación de exámenes parciales extemporaneos

Todas las solicitudes de alumnos para presentar una evaluación o examen parcial extemporáneo en materias programadas por la Escuela de Diseño, Ingeniería y Arquitectura (EDIA) deberán ser dirigidas al Director de Carrera por escrito, exponiendo la justificación correspondiente y proporcionando cualquier comprobante relacionado. Esta solicitud deberá realizarse a más tardar 5 días hábiles contados a partir de la fecha de aplicación del examen grupal, de otra manera la solicitud no procederá. En caso de ser autorizada, el Director de Carrera comunicará su decisión inapelable por escrito al Director de Departamento para que se aplique a la brevedad posible una evaluaciń o examen extemporáneo parcial departamental (es decir, diferente al aplicado al resto del grupo y no necesariamente a cargo del profesor que imparte la materia) y será evaluado sobre 80, a menos que el Director de Carrera considere que las razones y comprobantes expuestos por el alumno califican como fuerza mayor y ameritan que sea evaluado sobre 100. En caso de que el Director de Carrera no autorice la aplicación de la evaluación o examen parcial extemporáneo, la calificación del examen parcial será "NP".

NOTA: Esta política no aplica para exámenes finales extemporáneos, los cuales están reglamentados de manera explícita en el artículo 5.13 del Reglamento Académico de Carreras Profesionales 2015: Cuando por causa justificada un alumno no se presentara al examen final, podrá solicitar un examen extemporáneo al Director de Carrera correspondiente, exponiendo las causas de esta petición y deberá hacerlo por escrito. El derecho de presentar este examen extemporáneo caduca una semana antes del primer día de clases del siguiente periodo semestral. El Director de Carrera revisará la solicitud del alumno y dictaminará en forma definitiva si procede. En caso de que proceda, la turnará al Director de Departamento Académico correspondiente. La calificación final, que incluye el resultado de la evaluación extemporánea, deberá registrarse antes del primer día de clases del siguiente periodo semestral.

Integridad académica

Se cambió el capitulo de Integridad Académica: Tratamiento de faltas a la integridad académica:

1. Profesor asigna calificación reprobatoria (inapelable) a actividad, examen, periodo parcial o final. Se suman las posibles sanciones que determine el Comité de Integridad Académica de Campus.
2. Profesor informa al Comité de Integridad Académica del Campus. Documentar la situación.
3. El comité analiza el caso y la gravedad. Si resuelve que no hay más sanción, da aviso al estudiante.
4. Si el comité resuelve que se amerita más sanción, se lo comunica al estudiante y lo cita a una audiencia para que aporte pruebas y manifieste lo que considere a su favor.
5. Sanciones adicionales:
   - Medida correctiva
   - Estatus condicionamiento por faltas a la integridad académica
   - Suspensión

Protección Civil

- Origen
- Objetivo
- Que hacer en caso de incendio
- Que hacer en caso de temblor
- Brigadas
- Video

Actividades de Aprendizaje

- Participación en clases
- Comentarios sobre noticias de seguridad informática
- Ejercicios
- Tareas
- Proyectos de programación

Breve semblanza del profesor

- Ingeniero en Sistemas Electrónicos, ITESM-CEM
- Maestría en Sistemas Computacionales, ITESM-CEM
- DEA - Informatica Fundamental, Universidad de Paris 7
- Doctorado Informatica, Universidad de Paris 8 e INRIA Rocquencourt.
- Profesor-Investigador, ITESM-CEM
- Subdirector de Seguridad de la Información de Invex Grupo Financiero.
- Miembre del Cómite de Ciberseguridad de la ABM
- Coordinador e instructor del Diplomado en Seguridad Informática impartido por el ITESM.
- Instructor en el seminario de preparación para el exámen CISSP, organizado por la ALAPSI