1. Datos Generales de la asignatura

Nombre de la asignatura:	Ciberseguridad
Clave de la asignatura:	SVC-2102
SATCA[1]:	2-3-5
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura

La asignatura de Ciberseguridad se encuentra en el VIII semestre y forma parte de un grupo de asignaturas de la especialidad Sistemas virtualizados y cómputo en la nube. Y se relaciona con las competencias del perfil de egreso: Identificar y comprender las tecnologías de hardware para proponer, desarrollar y mantener aplicaciones eficientes y administrar bases de datos conforme a requerimientos definidos, normas organizacionales de manejo y seguridad de la información, utilizando tecnologías emergentes.

La importancia de la asignatura se relaciona con la formación profesional de los alumnos en los conceptos y técnicas básicas para proponer estrategias preventivas en materia de Ciberseguridad, para salvaguardar la seguridad integral en la red de datos personales y confidenciales, sistemas y equipos de información.
Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales la capacidad de identificar las amenazas y vulnerabilidades que existe en la infraestructura de red de una organización, de tal forma que puede hacer un análisis de riesgos.
Además, permite identificar e integrar los mecanismos de seguridad y la infraestructura tecnológica necesaria para asegurar la disponibilidad, confidencialidad e integridad de la información en las redes de computadoras.
Permite también al alumno, aplicar mecanismos de mejora continua en los servicios de tecnologías de información y comunicaciones, encaminados a satisfacer las necesidades de los usuarios.
Proporciona al estudiante la capacidad necesaria para diseñar aplicaciones Web con los mecanismos de seguridad necesarios para su funcionalidad

Intención didáctica

El temario del curso se ha organizado en cinco unidades cada una conformada por contenidos que contribuirán al buen aprendizaje de esta materia.
El enfoque sugerido para la asignatura requiere que las actividades prácticas promuevan el manejo de estándares, protocolos, métodos, reglas, herramientas y leyes que permitan minimizar los posibles riesgos a la infraestructura o a la información. Para esta asignatura se requiere de conocimientos sobre software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras

[1] Sistema de Asignación y Transferencia de Créditos Académicos

personas.
Además, se contempla el desarrollo de habilidades para el planteamiento de problemas, trabajo en equipo, asimismo, elementos que propicien procesos intelectuales como inducción-deducción y análisis-síntesis con la intención de generar una actividad intelectual compleja; las actividades teóricas se han descrito como actividades previas al tratamiento práctico de los temas. En las actividades prácticas sugeridas, es conveniente que el profesor sólo guie al estudiante en la construcción de su conocimiento.
En el primer tema se abordan aspectos de la Ciberseguridad, el valor de la información y posibles riesgos a los que está expuesto una organización.
En el segundo tema se tratan los temas sobre las normatividades de la Ciberseguridad.
En el tercer se abordan los algoritmos criptográficos desarrollados a lo largo de la historia, así como un análisis de las técnicas de cifrado de datos se programan los algoritmos utilizando un lenguaje de programación orientado a objetos.
El tema cuatro presenta la autentificación a nivel de red, que es utilizada para proteger la información adoptando medidas de seguridad, uso de protocolos de transmisión segura firewalls y redes privadas virtuales.
El tema cinco plantea la seguridad en los servicios principales de internet como DNS, Web, Correo y FTTP.
El enfoque sugerido para la asignatura requiere que las actividades prácticas promuevan el desarrollo de habilidades para la experimentación, tales como: identificación, manejo e implementación de software especializado de seguridad, desarrollo de algoritmos de cifrado de datos, uso de lenguajes de programación orientados a objetos, herramientas para seguridad en redes; planteamiento de problemas; trabajo en equipo; asimismo, propicien procesos intelectuales como inducción-deducción y análisis-síntesis con la intención de generar una actividad intelectual compleja; por esta razón varias de las actividades prácticas se han descrito como actividades previas al tratamiento teórico de los temas, de manera que no sean una mera corroboración de lo visto previamente en clase, sino una oportunidad para conceptualizar a partir de lo observado.
En las actividades prácticas sugeridas, es conveniente que el profesor busque sólo guiar a sus alumnos para que ellos hagan la elección de los elementos a programar y la manera en que los tratarán. Para que aprendan a planificar, que no planifique el profesor todo por ellos, sino involucrarlos en el proceso de planeación. La lista de actividades de aprendizaje no es exhaustiva, se sugieren sobre todo las necesarias para hacer más significativo y efectivo el aprendizaje. Algunas de las actividades sugeridas pueden hacerse como actividad extra clase y comenzar el tratamiento en clase a partir de la discusión de los resultados de las observaciones, incluyendo posibles actividades en línea, en caso de poder contar con un sistema gestor de contenidos. Se busca partir de hacer los procesos de manera manual, para que el estudiante se acostumbre a reconocer el funcionamiento de los algoritmos y de las técnicas de protección y no sólo se hable de ellos en el aula. Es importante ofrecer escenarios distintos, ya sean construidos, artificiales, virtuales o naturales.
En las actividades de aprendizaje sugeridas, generalmente se propone la formalización de los conceptos a partir de experiencias concretas; se busca que el alumno tenga el primer contacto con el concepto en forma concreta y sea a través de la observación, la reflexión y la discusión que se dé la formalización; la resolución de problemas se hará después de este proceso. Esta resolución de problemas no se especifica en la descripción de actividades, por ser más familiar en el desarrollo de cualquier curso. Pero se sugiere que se diseñen problemas con datos faltantes o sobrantes de manera que el alumno se ejercite en la identificación de datos relevantes y elaboración de supuestos.
En el transcurso de las actividades programadas es muy importante que el estudiante aprenda a valorar las actividades que lleva al cabo y entienda que está construyendo su

hacer futuro y en consecuencia actúe de una manera profesional; de igual manera, aprecie la importancia del conocimiento y los hábitos de trabajo; desarrolle la precisión y la curiosidad, la puntualidad, el entusiasmo y el interés, la tenacidad, la flexibilidad y la autonomía.
Es necesario que el profesor ponga atención y cuidado en estos aspectos en el desarrollo de las actividades de aprendizaje de esta asignatura.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
TecNM campus Comalcalco Julio de 2021	Dr. David Ramírez Peralta	Diseño y elaboración de la especialidad en virtualización y cómputo en la nube de la carrera de Ingeniería en Sistemas Computacionales.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Diseña mecanismos de Ciberseguridad para redes de computadoras, desarrolla algoritmos de cifrado de datos, e implementa esquemas lógicos de seguridad para apoyar la productividad de las organizaciones.

5. Competencias previas

Competencias específicas:

- Diseña y elabora un proyecto de cableado estructurado aplicando normas y estándares vigentes para la solución de problemas de conectividad.
- Aplica la programación orientada a objetos para resolver problemas reales y de ingeniería.

Competencias genéricas:

- Capacidad de análisis y síntesis.
- Capacidad de organizar y planificar.
- Comunicación oral y escrita.
- Habilidad para buscar y analizar información proveniente de fuentes diversas.
- Solución de problemas.
- Toma de decisiones.
- Capacidad crítica y autocrítica.
- Capacidad de trabajar en equipo.
- Capacidad de comunicar sus ideas.
- Capacidad de liderazgo.
- Capacidad de aplicar los conocimientos en la práctica.
- Habilidades de investigación.
- Capacidad de adaptarse a nuevas situaciones.

Capacidad de generar nuevas ideas (creatividad).

6. Temario

No.	Temas	Subtemas
1	Introducción a la Ciberseguridad	1.1 Ciberespacio y Ciberseguridad 1.2 Definición y niveles de seguridad 1.3 Análisis de requerimientos de seguridad 1.3.1 Amenazas 1.3.2 Vulnerabilidades 1.3.3 Riesgos 1.3.4 Tipos de ataques 1.3.4.1 Denegación del servicio 1.3.4.2 Suplantación de la identidad
2	Propuesta de estrategia en materia de Ciberseguridad	2.1. Normativas internacionales en materia de Ciberseguridad 2.2. Legislación informática de México 2.3. Derechos fundamentales en Internet relacionados con la ciberseguridad 2.4. Ejemplos de estrategias preventivas en materia de ciberseguridad 2.5. Diseño de estrategias en ciberseguridad 2.6. Acciones para evitar malas prácticas que ponen en riesgo la seguridad en la red
3	Criptografía	2.1 Definición de criptografía 2.1.1 Tipos de cifrado 2.1.1.1 Cifrado por sustitución 2.1.1.2 Cifrado por transposición 2.2 Criptosistemas de Clave Secreta. 2.2.1 Generalidades sobre sistemas de clave secreta. 2.2.2 Algoritmo DES (Data Encryption Standard). 2.2.3 Modos de cifra en bloque. 2.2.4 Algoritmo IDEA (International Data Encryption Algorithm). 2.2.5 Algoritmo AES (Advanced Encryption Standard). 2.3 Criptosistemas de Cifrado en Flujo 2.3.1 Cifradores con clave continua de un solo uso. 2.3.2 Postulados de Golomb para secuencias cifrantes. 2.3.3 Estructuras generadoras de secuencias cifrantes. 2.3.4 Cifrados en flujo con registros de desplazamiento. 2.4 Criptosistemas de Clave Pública 2.4.1 Introducción a la cifra con clave pública. 2.4.2 Protocolo de Diffie y Hellman para el intercambio de claves.

		2.4.3 Cifradores de mochila de Merkle-Hellman. 2.4.4 Cifrado RSA. 2.4.5 Cifrado ElGamal
4	Autenticación	3.1 Protocolos de Autenticación 3.1.1 Claves secretas compartidas 3.1.2 Centros de distribución de claves 3.1.3 Claves públicas 3.1.4 Ejemplos de protocolos de autenticación 3.2 Firmas Digitales 3.2.1 Firmas digitales de clave simétrica Firmas digitales de llave pública 3.3 Cortafuegos (firewalls) 3.3.1 Alcances y limitaciones 3.3.2 Componentes 3.3.3 Filtros de paquetes 3.3.4 Filtro de servicios
5	Seguridad en servicios de Internet	4.1 Seguridad en la Web 4.1.1 Asignación segura de nombres de dominio (DNS) 4.1.2 Capa de sockets seguros 4.1.3 HTTP Seguro 4.1.4 Seguridad en correo electrónico 4.1.5 MIME Seguro 4.1.6 PGP, GPG

7. Actividades de aprendizaje de los temas

1. Introducción a la Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica: • Conoce los conceptos básicos de Ciberseguridad, reconociendo la importancia de la misma en las redes de computadoras. *Genéricas*: ▪ Capacidad de análisis y síntesis ▪ Capacidad de organizar y planificar ▪ Comunicación oral y escrita ▪ Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado ▪ Solución de problemas ▪ Toma de decisiones	▪ Comunicar y presentar la asignatura: encuadre, empleo de recursos educativos abiertos (REA), entrega de productos y evidencias de aprendizaje en la plataforma drive y tiempo de acompañamiento docente. ▪ Organizar al grupo en equipos para realizar la búsqueda en internet de los siguientes subtemas: Ciberespacio y Ciberseguridad, niveles de seguridad, análisis de requerimientos de seguridad, amenazas, vulnerabilidades y riesgos. ▪ Por equipos tendrán que elaborar una presentación para exponer ante

	el grupo los temas. Deberán compartir la información con sus compañeros y subirla a una carpeta en la nube. ▪ Lista de cotejo de la presentación de temas relacionados a la Ciberseguridad, categorías: -Se identifican claramente las ideas primarias de las ideas secundarias. -La presentación está ordenada. -Las relaciones entre conceptos presentan jerarquías. -No hay errores ortográficos en la presentación -Se observa la preparación del tema, el uso de referencias empleadas y un orden de ideas. -Se observa seguridad al tratar el tema, buen uso del recurso de apoyo, fluidez de ideas, tono de voz adecuado. ▪ Por equipos, realizar una investigación sobre lo siguiente: tipos de ataques. ▪ Con la información resultante elabora un mapa conceptual que represente la información investigada. ▪ Valorar la actividad con una lista de cotejo de mapa conceptual. ▪ Retroalimentar los temas tratados durante las presentaciones, sugerencias de mejora en el mapa conceptual.
2. Propuesta de estrategia en materia de Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica: ▪ Analiza la normatividad aplicada a la Ciberseguridad y propone estrategias preventivas de Ciberseguridad. *Genéricas:* • Capacidad de análisis y síntesis • Capacidad de organizar y planificar • Comunicación oral y escrita • Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado • Solución de problemas • Toma de decisiones	▪ Organizar al grupo en equipos para elaborar un objeto de aprendizaje para ello deberán utilizar herramientas digitales para la elaboración de un vídeo relacionado con los siguientes temas: Normativas internacionales en materia de Ciberseguridad, Legislación informática de México, Derechos fundamentales en Internet relacionados con la Ciberseguridad, Ejemplos de estrategias preventivas en materia de Ciberseguridad, Diseño de estrategias en Ciberseguridad y

	Acciones para evitar malas prácticas que ponen en riesgo la seguridad en la red ▪ Proporcionar a los alumnos los siguientes indicadores de logro para el desarrollo del proyecto: ❖ El sonido es adecuado, la voz es fluida, no hay sonidos que interrumpan y se entiende cuando pasa de una idea a otra. ❖ El vídeo está bien grabado, presenta imágenes sin pixelear y hay apoyos gráficos. ❖ El recurso presenta la información de forma objetiva, no presenta errores u omisiones que pudieran confundir o equivocar la interpretación de los contenidos. ❖ Enfatiza los puntos clave y las ideas más significativas con un nivel adecuado de detalle. ❖ El recurso es útil para generar aprendizajes con respecto al tema que aborda. ❖ Presenta información de forma clara y precisa, incluyendo ejemplos o demostraciones de uso del recurso para el uso en la enseñanza. ❖ El recurso presenta al final las fuentes de información que permiten respaldar los contenidos que se presentan. ❖ El recurso se encuentra en la nube y la liga de acceso puede abrirse desde cualquier dispositivo. ▪ Organización de las presentaciones de los Objetos de Aprendizaje, retroalimentación entre compañeros y por parte del facilitador.
3. Criptografía	
Competencias	Actividades de aprendizaje
Específica: • Desarrolla técnicas de cifrado, algoritmos de criptografía para resguardar la información en las organizaciones. *Genéricas:* • Capacidad de análisis y síntesis • Capacidad de organizar y planificar • Comunicación oral y escrita	• Organizar al grupo en equipos para realizar la búsqueda en internet de los subtemas del tema 3. • Por equipos tendrán que elaborar una presentación para exponer ante el grupo los temas. Deberán compartir la información con sus compañeros y subirla a una carpeta en la nube. • Lista de cotejo de la presentación

• Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado • Solución de problemas • Toma de decisiones	de temas relacionados a la Ciberseguridad, categorías: -Se identifican claramente las ideas primarias de las ideas secundarias. -La presentación está ordenada. -Las relaciones entre conceptos presentan jerarquías. -No hay errores ortográficos en la presentación -Se observa la preparación del tema, el uso de referencias empleadas y un orden de ideas. -Se observa seguridad al tratar el tema, buen uso del recurso de apoyo, fluidez de ideas, tono de voz adecuado. • Desarrolla algoritmos de cifrado mediante un lenguaje de programación orientada a objetos. • Evaluar mediante lista de cotejo el programa: -Funcionalidad -Codificación -Documentación
4. Autenticación	
Competencias	Actividades de aprendizaje
Específica: • Crea mecanismos de filtrado de paquetes, conoce los diferentes tipos de autenticación y comprende las firmas digitales. *Genéricas* • Capacidad de análisis y síntesis • Capacidad de organizar y planificar • Comunicación oral y escrita • Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado • Solución de problemas • Toma de decisiones	▪ Elaborar una infografía del tema protocolos de autenticación, firmas digitales y cortafuegos. ▪ Evaluar la infografía respetando los siguientes indicadores de logro: ✓ El título es llamativo, está centrado en la lámina y está acompañado de una imagen principal. ✓ Formato de texto según las instrucciones dadas por la docente (tamaño de fuente, interlineado, sangría, alineación, entre otros). ✓ Utiliza imágenes relacionadas con el contenido. ✓ Hace uso de elementos llamativos que ayudad a reforzar la información (flechas, formas, figuras geométricas, entre otras) ✓ Organización coherente del contenido. (desde lo más complejo a lo más específico) ✓ Se evidencia originalidad en la

	elaboración de la infografía. ✓ Ordena la información de manera que sea comprensible representativa del tema sugerido. ▪ Organizar la exhibición de las infografías, retroalimentar a los alumnos en contenidos y sobre la infografía. ▪ Organizar a los alumnos por equipos para configura un firewall en diferentes plataformas operativas. ▪ Evaluar la configuración con una lista de cotejo, donde se considere: Diseño, Presentación, Estructura.
5. Seguridad en servicios de Internet	
Competencias	Actividades de aprendizaje
Específica: • Configurara los principales servicios de Internet e implementa políticas de seguridad informática para asegurarlos. *Genéricas:* ▪ Capacidad de análisis y síntesis ▪ Capacidad de organizar y planificar ▪ Comunicación oral y escrita ▪ Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado ▪ Solución de problemas ▪ Toma de decisiones	▪ Por equipos, realizar una investigación sobre los conceptos del tema seguridad en la web. ▪ Con la información resultante elabora un mapa conceptual que represente la información investigada. ▪ Valorar la actividad con una lista de cotejo de mapa conceptual. ▪ Retroalimentar los temas tratados durante las presentaciones, sugerencias de mejora en el mapa conceptual. ▪ Organizar a los alumnos en equipos para configurar un servicio de dns y lo asegura mediante políticas de seguridad. ▪ Evaluar la configuración con una lista de cotejo, donde se considere: Diseño, Presentación, Estructura.

8. Práctica(s)

Instalación, configuración e implementación de un sistema operativo de red en forma segura.

9. Proyecto de asignatura

Proyecto: Instalación, configuración e implementación de un sistema operativo en forma segura.

Objetivo: Desarrollar algoritmos de cifrado de datos para instalar, configurar e implementar un sistema operativo de forma segura.

Fundamentación: Los ciberataques a las empresas se han convertido en un delito en auge. Con el continuo proceso de digitalización corporativa y la popularización del teletrabajo, se ha creado una situación en la que cada vez hay más personas conetadas. En este escenario la asignatura de ciberseguridad desarrolla habilidades tecnológicas en los estudiantes que le permiten detectar, prevenir y configurar algoritmos de cifrados que brinden seguridad a los usuarios, desde los espacios educativos hasta las empresas. La ciberseguridad se convierte en un conocimiento necesario que requiere compartir inteligencia, experiencias y formación entre estudiantes para desarrollar el proyecto en equipo.

Planeación: Se requiere el desarrollo de habilidades relacionadas con actitud crítica, reconocer los conocimientos que se aplican en el desarrollo del proyecto, fomentar el trabajo en equipo y la habilidad blanda de liderazgo, optimización del tiempo y valores relacionados con el reconocimiento de las habilidades del otro y responsabilidad. Las prácticas de cada unidad permiten observar, retroalimentar y valorar los avances del proyecto para finalizar con la integración de cada una de las partes.

Ejecución: Desarrollar mediante las siguientes prácticas en cada unidad el avance del proyecto en equipos y retroalimentar en los avances:

1. La primera fase es realizar investigación documental sobre los tipos de ataques y temas relacionados con el proyecto.
2. Desarrolla algoritmos de cifrado mediante un lenguaje de programación orientada a objetos.
3. Configurar un servicio de dns y asegurarlo mediante políticas de seguridad.
4. Evaluar en el programa: Funcionalidad; Codificación; Documentación.

Evaluación: Presentación de resultados así como retroalimentar los defectos encontrados en el sistema y autoevaluación de la experiencia del proyecto desarrollado

10. Evaluación por competencias

Evaluación formativa

Producto o Evidencia de aprendizaje	Instrumento de evaluación
Lista de cotejo de mapa conceptual	Lista de cotejo de mapa conceptual: palabras clave, organización, jerarquía, enlaces.
Presentación grupal: Cómputo en la nube	Rúbrica de presentación de temas relacionados aciberseguridad, categorías:

	-Se identifican claramente las ideas primarias de las ideas secundarias. -El organizador gráfico está ordenado. -Las relaciones entre conceptos presentan jerarquías. -No hay errores ortográficos en la presentación -Se observa la preparación del tema, el uso de referencias empleadas y un orden de ideas. -Se observa seguridad al tratar el tema, buen uso del recurso de apoyo, fluidez de ideas, tono de voz adecuado.
Infografía	Evaluar la infografía respetando los siguientes indicadores de logro: – El título es llamativo, está centrado en la lámina y está acompañado de una imagen principal. – Formato de texto según las instrucciones dadas por la docente (tamaño de fuente, interlineado, sangría, alineación, entre otros). – Utiliza imágenes relacionadas con el contenido. – Hace uso de elementos llamativos que ayudad a reforzar la información (flechas, formas, figuras geométricas, entre otras) – Organización coherente del contenido. (desde lo más complejo a lo más específico) – Se evidencia originalidad en la elaboración de la infografía. – Ordena la información de manera que sea comprensible representativa del tema sugerido.
Elaboración de un objeto de aprendizaje: vídeo.	▪ Lista de cotejo, indicadores de logro para el desarrollo del proyecto: ✓ El sonido es adecuado, la voz es fluida, no hay sonidos que interrumpan y se entiende cuando pasa de una idea a otra. ✓ El vídeo está bien grabado, presenta imágenes sin pixelear y hay apoyos gráficos. ✓ El recurso presenta la información de forma objetiva, no presenta errores u omisiones que pudieran confundir o equivocar la interpretación de los contenidos. ✓ Enfatiza los puntos clave y las ideas más significativas con un nivel adecuado de detalle. ✓ El recurso es útil para generar aprendizajes con respecto al tema que aborda. ✓ Presenta información de forma clara y precisa, incluyendo ejemplos o demostraciones de uso del recurso para el uso en la enseñanza. ✓ El recurso presenta al final las fuentes de información que permiten respaldar los contenidos que se presentan. ✓ El recurso se encuentra en la nube y la liga de acceso puede abrirse desde cualquier dispositivo.

Evaluación del proyecto: Configuración, instalación y desarrollo de un Sistema operativo seguro.	Indicadores de logro que se tienen que cumplir: _Analizamos los requerimientos de desarrollo de software _Identificamos los algoritmos de cifrado mediante el lenguaje de programación orientada a objetos _Configuramos el servicio dns y aseguirarlo mediante políticas de seguridad. _Definimos la estrategia de pruebas. _Definimos los criterios de funcionalidad, codificación y documentación. _Identificamos los entornos (ambientes) requeridos. _Determinamos necesidades de personal y entrenamiento. _Establecimos procedimientos de prueba.
Autoevaluación del equipo:	Preguntas de reflexión: ¿qué problemáticas se identificaron? ¿Qué necesitamos aprender?, ¿qué temas debo estudiar de manera individual para mejorar mi desempeño en el equipo? ¿qué decisiones tuvo que tomar el equipo para resolver el problema?, ¿en qué áreas de aprendizaje relacionadas con los resultados me considero experto?.

Evaluación sumativa:

1. Participación en clases
2. Evidencias de productos y desempeños en la plataforma
3. Portafolio de aprendizaje personal
4. Autoevaluación

11. Fuentes de información

REFERENCIAS:

Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, (185), 19-64.

Chinchilla, E. J. S., & Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. Tecnología y desarrollo, 15. https://sistemas.acis.org.co/index.php/sistemas/article/download/94/78

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20), 80-93.

Gaona García, Elvis Eduardo; Rojas Martínez, Sergio Leonardo; Trujillo Rodríguez, Cesar, Leonardo; Mojica Nava, Eduardo Alirio. (2014). Authenticated encryption of pmu data. https://www.redalyc.org/articulo.oa?id=257059813006

Kamberg, M.L (2018). Ciberseguridad: protege tu identidad y tus datos. First Edition. ISBN: 978-1-4777-8998-8.

Nikki Giant. (2017). Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones. Editorial Narcea Ediciones; 1er edición, ASIN: B072B95SZN.

Sabillón, R., & Cano, J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. Revista Ibérica de Sistemas e Tecnologias de Informação, 2019,(32).

Víctor Gayoso Martínez, Luis Hernández Encinas, David Arroyo Guardeño. (2020). Ciberseguridad. Edición: Los Libros de La Catarata. ISBN: 978841352120.

RECURSOS EDUCATIVOS ABIERTOS

Instituto Nacional de Ciberseguridad. Aprende Ciberseguridad https://www.incibe.es/aprendeciberseguridad

Qué Es Ciberseguirdad. Definición, Tipos Y Objetivos De La Seguridad Informática. https://www.avansis.es/ciberseguridad/que-es-ciberseguridad/#Que_es_Ciberseguridad_Significado