Curriculum Vitae

Gerardo Vega Hernández

March 27, 2025

Contents

1 Formación y trayectoria académica **1**
1.1 Datos Generales . . . 1
1.2 Trayectoria Académica . . . 1
1.3 Experiencia académico-administrativa . . . 1

2 Labor docente **2**
2.1 Cursos semestrales a nivel posgrado . . . 2
2.1.1 Cursos semestrales en el Posgrado en Ciencia e Ingeniería de la Computación de la UNAM (sede IIMAS) . . . 2
2.1.2 Cursos semestrales en el posgrado de Matemáticas de la UNAM . . . 2
2.1.3 Cursos semestrales en el posgrado en Ingeniería Eléctrica de la UNAM . . . 2
2.2 Cursos semestrales o trimestrales a nivel licenciatura . . . 2
2.2.1 Cursos semestrales en la H. Facultad de Ciencias de la UNAM . . . 2
2.2.2 Cursos trimestrales en la Universidad Autónoma Metropolitana, Unidad Iztapalapa (durante un año sabático en esa Universidad) . . . 2
2.2.3 Cursos semestrales como ayudante de profesor en la H. Facultad de Ciencias de la UNAM 2
2.2.4 Cursos trimestrales como ayudante de posgrado en la Universidad Autónoma Metropolitana, Unidad Iztapalapa . . . 3
2.3 Otros cursos dentro de la UNAM . . . 3
2.4 Dirección de tesis . . . 3
2.4.1 Dirección de tesis a nivel Doctoral . . . 3
2.4.2 Dirección de tesis a nivel Maestría . . . 4
2.5 Participación como jurado en exámenes profesionales o de grado . . . 5
2.6 Labor docente en la evaluación y en la aplicación de exámenes . . . 9
2.6.1 Participación en Evaluaciones Semestrales de Estudiantes Doctorales . . . 9
2.6.2 Participación como Evaluador para los Coloquios de Investigación I y II . . . 10
2.6.3 Participación como entrevistador para aspirantes a estudiantes de doctorado . . . 10
2.6.4 Participación como jurado en exámenes generales de conocimientos . . . 10
2.6.5 Elaboración y aplicación de exámenes extraordinarios . . . 10
2.7 Generación de contenidos audiovisuales . . . 10
2.8 Elaboración de material docente . . . 10

3 Productividad académica **10**
3.1 Distinciones como miembro del SNI . . . 10
3.2 Publicaciones . . . 11
3.2.1 Publicaciones en revistas internacionales INDIZADAS CON ARBITRAJE y con reporte de FACTOR DE IMPACTO . . . 11
3.2.2 Memorias en extenso en congresos internacionales CON ARBITRAJE . . . 14
3.2.3 Publicaciones en revistas internacionales CON ARBITRAJE, sin reporte FACTOR DE IMPACTO, pero INDIZADAS según la clasificación del Instituto de Matemáticas de la UNAM . . . 15
3.2.4 Publicaciones en revistas CON ARBITRAJE . . . 15
3.2.5 Memorias en extenso en congresos nacionales . . . 16
3.2.6 Reportes técnicos . . . 16
3.3 Asesorías especializadas . . . 16
3.4 Administración de proyectos PAPIIT-UNAM . . . 17
3.5 Evaluación de proyectos para el CONAHCyT . . . 18
3.6 Evaluación de proyectos PAPIIT . . . 19
3.7 Evaluación de proyectos para la UACM . . . 19
3.8 Colaboración con dependencias internas a la UNAM . . . 19
3.9 Colaboración con investigadores de universidades extranjeras . . . 20
3.10 Trabajos de investigación en congresos internacionales . . . 20
3.11 Reconocimientos o premios . . . 21
3.12 Artículos arbitrados para revistas internacionales . . . 22

4 Labores de difusión **25**
4.1 Organización de congresos y coloquios 25
4.2 Pláticas de divulgación en universidades 25
4.3 Participación como invitado a congresos, talleres o seminarios 26
4.4 Participación en congresos, talleres y seminarios nacionales 27
4.5 Entrevistas a medios de difusión académica 29

5 Participación institucional **29**
5.1 Participación en cuerpos académicos colegiados 29
5.2 Participación en Comisiones Evaluadoras 29

1 Formación y trayectoria académica

1.1 Datos Generales

Nombre: **Gerardo Vega Hernández**
Nombramiento: **Investigador Titular "C" de tiempo completo**
Labora en:

Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM y **Posgrado en Ciencias e Ingeniería de la Computación del IIMAS**.

Email: **gerardov@unam.mx**
Telefono: **56226780**
Página Personal: **paginaspersonales.unam.mx/app/webroot/index.php/academicos/datosContacto/alias:gerardovega**

1.2 Trayectoria Académica

- **Licenciatura**: Matemáticas, Facultad de Ciencias UNAM, 1991.
- **Maestría**: Ciencias de la Computación, UACPyP del CCH, 1994.
- **Doctorado**: Doctorado en Ciencias (Matemáticas) en la Universidad Autónoma Metropolitana, 2001.

1.3 Experiencia académico-administrativa

- Ayudante de profesor "B", Facultad de Ciencias UNAM, Mayo de 1986-1990.
- Técnico Académico Auxiliar "C", Dirección Gral. de Serv. de Cómputo Académico UNAM, Feb. de 1989-1990.
- Técnico Académico Asociado "A", Dirección Gral. de Serv. de Cómputo Académico UNAM, Feb. de 1990-1991.
- Técnico Académico Asociado "C", Dirección Gral. de Serv. de Cómputo Académico UNAM, Feb. de 1991-1995.
- Ayudante de Posgrado, Departamento de Matemáticas, UAM-I, Jul. de 1995-1996.
- Ayudante de Posgrado, Departamento de Matemáticas, UAM-I, Ago. de 1996-1997.
- Ayudante de Posgrado, Departamento de Matemáticas, UAM-I, Sep. de 1997-1998.
- Investigador Asociado "C", Dirección Gral. de Serv. de Cómputo Académico UNAM, Ene. de 1995-2000.
- Profesor de Asignatura "A", Facultad de Ciencias y Posgrado en Ciencias e Ingeniería de la Computación del IIMAS, UNAM, Desde oct. de 1996.
- Investigador Titular "A" Definitivo, Dirección Gral. de Serv. de Cómputo Académico UNAM, Ene. de 2001-2007.
- Investigador Visitante (Profesor Titular B, durante un sabático), Departamento de Matemáticas, UAM-I, May. de 2002-2003.
- Investigador Titular "B" Definitivo, Dirección Gral. de Serv. de Cómputo Académico UNAM, Abril de 2007-2015.
- Investigador Titular "C" Definitivo, Dirección Gral. de Serv. de Cómputo Académico UNAM, Agosto de 2015.

2 Labor docente

2.1 Cursos semestrales a nivel posgrado

2.1.1 Cursos semestrales en el Posgrado en Ciencia e Ingeniería de la Computación de la UNAM (sede IIMAS)

- **Campos Finitos y sus Aplicaciones**, Año-Semestre: 15-1 y 15-2.
- **Teoría de la información y la codificación**, Año-Semestre: 00-2, 01-2, 04-1, 04-2, 05-2, 07-2, 08-2, 09-2, 10-2, 11-2, 12-2, 13-2, 16-2, 17-2, 19-1, 20-1, 21-1, 22-1, 23-1.
- **Teoría de la información y la codificación II**, Año-Semestre: 18-1.
- **Criptografía**, Año-Semestre: 06-1, 07-1, 08-1, 09-1, 10-1, 11-1, 12-1, 13-1, 14-1, 16-1, 17-1, 18-2, 19-2, 20-2, 21-2, 22-2, 23-2, 24-2.
- **Administración de Redes (Criptografía)**, Año-Semestre: 05-1
- **Redes de Computadoras**, Año-Semestre: 99-2, 02-1.
- **Seminario de Investigación I**, Año-Semestre: 99-2, 03-1, 04-2, 05-2, 07-2, 09-1, 13-2, 16-2, 17-2, 18-2, 20-2, 22-2.
- **Seminario de Investigación II**, Año-Semestre: 00-1, 02-1, 03-1, 05-1. 05-2, 06-2, 08-2, 11-1, 14-1, 17-1, 18-1, 19-1, 21-1.
- **Seminario de Investigación III**, Año-Semestre: 00-2, 02-2, 03-2, 04-1, 05-2, 06-1, 06-2, 11-2, 14-2.

2.1.2 Cursos semestrales en el posgrado de Matemáticas de la UNAM

- **Campos Finitos y sus Aplicaciones**, Año-Semestre: 15-1.

2.1.3 Cursos semestrales en el posgrado en Ingeniería Eléctrica de la UNAM

- **Teoría de la información y la codificación**, Año-Semestre: 14-2, 20-1.
- **Criptografía**, Año-Semestre: 20-2, 22-2.

2.2 Cursos semestrales o trimestrales a nivel licenciatura

2.2.1 Cursos semestrales en la H. Facultad de Ciencias de la UNAM

- **Teoría de Códigos**, Año-Semestre: 97-1, 97-2, 98-1.
- **Redes de Computadoras**, Año-Semestre: 99-1, 99-2.
- **Sem. De Computación B**, Año-Semestre: 97-1, 99-2

2.2.2 Cursos trimestrales en la Universidad Autónoma Metropolitana, Unidad Iztapalapa (durante un año sabático en esa Universidad)

- **álgebra Lineal**, trimestres 02P y 02O.
- **Matemáticas aplicadas a la Administración**, trimestre 02O.
- **Matemáticas V**, trimestre 03I.

2.2.3 Cursos semestrales como ayudante de profesor en la H. Facultad de Ciencias de la UNAM

- **Computación I**, Mayo de 1986.
- **Análisis de Fourier I**, **II** y **III** (5 veces Análisis de Fourier I, 3 Análisis de Fourier II y Análisis de Fourier III una vez). Estos cursos se impartierón entre 1987 y 1989.

2.2.4 Cursos trimestrales como ayudante de posgrado en la Universidad Autónoma Metropolitana, Unidad Iztapalapa

Se realizó labor docente dentro de la Universidad Autónoma Metropolitana, unidad Iztapalapa, como ayudante de posgrado, para cursos básicos en matemáticas, en Ingeniería y en Ciencias Sociales. Esta labor docente se realizo durante tres años, en los periodos:

- del 21/07/1995 al 20/07/1996,
- del 09/08/1996 al 08/08/1997 y
- del 24/10/1997 al 23/10/1998

2.3 Otros cursos dentro de la UNAM

- Con la colaboración del Maestro Alejandro Talavera Rosales y basándonos en mis notas de clase para mis cursos semestrales de Criptografía, se diseñó y se elaboró para la DGTIC un nuevo curso sobre conceptos básicos y fundamentales de la criptografía moderna comercial. Este nuevo curso se diseñó pensando especialmente en los becarios de la DGTIC que se interesan en los temas de seguridad informática. El curso finalmente se ofreció bajo el nombre de "**Introducción a la Criptografía Moderna Comercial**" durante los días del **7 al 9 de junio del 2021** (6 horas). Como un apoyo muy importante para el curso, se elaboró material didáctico muy completo el cual se puso a disposición de los alumnos y de la DGTIC en general. El objetivo fundamental del curso ha sido el corregir y aclarar muchas de las concepciones equivocadas que comúnmente se tienen alrededor de la seguridad informática y muy particularmente sobre criptografía moderna comercial. Se espera que el curso se convierta en un apoyo para los becarios de DGTIC.
- Nombramiento: Profesor. Curso: Curso sobre **Criptografía** para el plan de becarios del Departamento de Seguridad en Cómputo de la DGSCA. Lugar: Dir. Gral. de Serv. de Cómputo Académico. Duración: 20 horas. Fecha: Mayo 2004.
- Nombramiento : Profesor. Cursos: 31 cursos diversos sobre computación, 5 cursos del **Módulo Introductorio**, 8 de **Introducción a la Computación**, 3 del **Sistema Operativo MS-DOS**, 3 de **Técnicas de programación**, 7 de **Programación Pascal**, 2 de **Programación C**, 2 de **Introducción a VM** y 1 de **Optimización II**. Lugar: Dir. Gral. de Serv. de Cómputo Académico. Duración: 30 horas cada curso (en promedio). Fecha: Entre 1987 y 1993.

2.4 Dirección de tesis

2.4.1 Dirección de tesis a nivel Doctoral

- En el 2020 se inició con el trabajo de tutoría del estudiante **Félix Alejandro Hernández Fuentes** inscrito en el programa Doctoral del posgrado de Ciencia e Ingeniería de la Computación de la UNAM. Estatus: en proceso. El pasado 29 de junio se nos notificó que nuestro trabajo conjunto "The complete weight distribution of a subclass of optimal three-weight cyclic codes" fue aceptado para su publicación en la revista internacional Cryptography and Communications. Como se puede entender, lo anterior es un avance sustancial del trabajo doctoral de Félix.
- Se a iniciado los trabajos de dirección del trabajo tesis doctoral del estudiante **José Luis Juan Herrera García**, inscrito recientemente (2016) en el programa doctoral del posgrado Ciencias e Ingeniería de la Computación de la UNAM. Estatus: en proceso. **De hecho el 28 de febrero de 2018, José Luis presentó con éxito su examen de candidatura al Grado de Doctor en Ciencias e Ingeniería de la Computación**.
- Se continua con los trabajos de dirección del trabajo tesis doctoral del estudiante **Jesús Elisandro Cuén Ramos**, inscrito (2015) en el programa doctoral del posgrado de matemáticas de la UNAM. Estatus: en proceso. De hecho el 27 de julio de 2017, Jesús presentó con éxito su examen de candidatura al Grado de Doctor en Ciencias Matemáticas. Más aún, a la fecha el estudiante cuenta ya con 2 artículos investigación

publicados en revistas internacionales arbitradas y ha presentado dos trabajos de investigación en 2 congresos internacionales arbitrados. **Actualmente se está haciendo la revisión de su tesis doctoral y se considera que muy pronto Jesús estará presentando su examen de grado**.

- Dirección del trabajo de tesis a nivel Doctorado sobre el tema"**Distribución de Pesos de Códigos Reducibles Construidos como la Suma Directa de Dos Códigos de un solo Peso**", del estudiante **Carlos Alberto Vázquez Fernández**. Doctorado en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: terminada, fecha de examen: 8 de mayo 2015**.

2.4.2 Dirección de tesis a nivel Maestría

- El 18 de septiembre de 2019, mi ex-extudiante de maestría Daniel Becerra Pedraza presentó con éxito su examen de grado para obtener el grado de Maestro en Ciencias e Ingeniería de la Computación, con el trabajo"**Esquema de Compartición de Secretos con Detección Eficiente de Trampas**".

- El 18 de octubre de 2018, mi ex-extudiante de maestría Félix Alejandro Hernández Fuentes presentó con éxito su examen de grado para obtener el grado de Maestro en Ciencias e Ingeniería de la Computación, con el trabajo"**Algoritmo eficiente para el cálculo de las distribuciones de pesos de todos los códigos cíclicos irreducibles sobre campos finitos pequeños**". **Cabe mencionar que dicho trabajo le valió a mi estudiante una Mención honorifica**.

- A principios del 2018 se inicio la dirección del trabajo a nivel maestría del estudiante Daniel Becerra Pedraza. Mi estudiante de maestría Daniel Becerra Pedraza y yo presentamos el trabajo de investigación conjunto "**Secret Sharing Scheme with Efficient Cheating Detection** en el "**2nd International Conference on Networking, Information Systems & Security (NISS2019)**, que tuvo lugar en la Faculty of Sciences de la Universidad Mohammed V, de la ciudad de Rabat en Marruecos, durante los días del 27 al 29 de marzo del presente año. Cabe destacar que el artículo que presentamos Daniel y yo, obtuvo el 2 lugar al mejor artículo presentado al mencionado congreso internacional arbitrado. De hecho a dicho congreso se presentaron más de medio centenar (63) de artículos. **El trabajo que hemos presentamos en Rabat es básicamente la tesis con la que se graduará próximamente Daniel**.

- Se continuó con la dirección del trabajo a nivel maestría del estudiante Sanchez Neri Jesús Tonatihu, inscrito en el programa maestría del Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. **De hecho en el contexto de los Coloquios de Investigación II del Posgrado de Ciencia e Ingeniería de la Computación de la UNAM, mi estudiante presentó un avance significativo de su trabajo Tesis**. Sin embargo, al la fecha dicho estudiante ha dejado de reportarse y por tanto no se tiene una seguridad sobre la culminación de su Tesis.

- Durante 2015, se continuó con la dirección del trabajo a nivel maestría del Carlos Adrián Rodríguez Oliva, estudiante del Posgrado en Ciencias e Ingeniería de la Computación de la UNAM. El trabajo de tesis es sobre una implementación de software para la obtención de la distribución de pesos de códigos cíclicos irreducibles sobre campos finitos. **Estatus: Inconclusa**.

- Dirección del trabajo de tesis a nivel maestría de título "**Implementación del Algoritmo de Berlekamp para Factorización de Polinomios Sobre Campos Finitos**", del estudiante Carlos Alberto Vázquez Fernández. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: terminada, fecha de examen: Febrero de 2009**.

- Dirección del trabajo de tesis a nivel maestría de título "**UNAMCA Autoridad Certificadora para la UNAM**", del estudiante Enrique Reyes Castillo. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: terminada, fecha de examen: Marzo de 2006**.

- Dirección del trabajo de tesis a nivel maestría de título "**Implementación de un Sistema de Votaciones en Internet Utilizando un Protocolo Basado en Criptografía de Curvas Elípticas**", del estudiante Otoniel Manuel Ortiz Ruiz. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: terminada, fecha de examen: Octubre de 2005**.

- Dirección del trabajo de tesis a nivel maestría de título "**Implementación de un sistema de cifrado de llave pública basado en el problema del logaritmo discreto para curvas elípticas**", del estudiante Moisés Bautista Osorno. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: terminada, fecha de examen: 3 de Diciembre de 2002**.

- Dirección del trabajo de tesis a nivel maestría de título "**IMPLEMENTACIóN DEL ALGORITMO DE NIEDERREITER PARA LA FACTORIZACIóN DE POLINOMIOS SOBRE CAMPOS FINITOS PRIMOS**", del estudiante Jonathan Ponciano Vera. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: el estudiante graduó a través de un examen General de Conocimientos**.

- Dirección del trabajo de tesis a nivel Maestría sobre el tema "**Implementación de un sistema de recuperación de archivos usando técnicas de File Carving**", del estudiante Francisco Javier Ramírez Paredes. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: Inconclusa**.

- Dirección del trabajo de tesis a nivel maestría de título "**Esquema de Seguridad para el Manejo y Consulta de Expedientes Clínicos Electrónicos**", del estudiante Gibrán Granados Paredes. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: Inconclusa**.

- Dirección del trabajo de tesis a nivel maestría de título "**Desarrollo de un sistema de consulta de correo electrónico que permita el uso de sobres y firmas digitales**", del estudiante Javier Bolaños Molina. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: Inconclusa**.

- Dirección del trabajo de tesis a nivel maestría de título "**Implementación de un servidor de certificación para correo electrónico**", del estudiante Rodolfo Méndez García. Maestría en Ciencias e Ingeniería de la Computación de la UNAM. **Estatus: Inconclusa**.

- Dirección del trabajo de tesis a nivel licenciatura de título "**Desarrollo de un proveedor de seguridad para JAVA usando criptografía de curvas elípticas**", de la estudiante Elsa Lizette Arroyo Caravaca. Facultad de Ciencias de la UNAM. **Estatus: Inconclusa**.

- Dirección del trabajo de tesis a nivel licenciatura de título "**Implementación de una rutina de búsqueda exacta de subcadenas de caracteres en un sistema de recuperación de información**", de la estudiante Gabriela Barbosa García. Facultad de Ciencias de la UNAM. **Estatus: Inconclusa**.

2.5 Participación como jurado en exámenes profesionales o de grado

- Se evaluó el trabajo de maestría "**INFORME DE PASANTÍA EN ORACLE COMO DESARROLLADOR DE PRUEBAS DE SOFTWARE EN EL ÁREA DE DB TESTING**", del estudiante ARMANDO CAMILO FLORES HUELGAS, quien presentó su examen de grado. El examen se aplicó bajo el Programa de Maestría y Doctorado en Ingeniería UNAM, el día 30 de enero del 2024.

- Se evaluó el trabajo de doctorado "**Design and Analysis of Some Symmetric-Key Cryptographic Schemes for Encryption and Authentication**", del estudiante Samir Kundu inscrito al PhD degree in Computer Science del Indian Statistical Institute. 10 de enero 2024.

- Se evaluó el trabajo de maestría "**CODIFICACIÓN PARA COMUNICACIONES EN EL ESPACIO PROFUNDO UTILIZANDO CÓDIGOS TURBO CON MODIFICACIONES EN EL ENTRELAZADOR Y EN LA MATRIZ DE PERFORADO**", del estudiante MIGUEL DARIO MOCTEZUMA MONROY, quien presentó su examen de grado. El examen se aplicó bajo el Programa de Maestría y Doctorado en Ingeniería UNAM, el día 20 de junio del 2022.

- Se evaluó el trabajo de maestría "**Diseño de una interfaz gráfica para el usuario de la codificación de canal en las Comunicaciones de Espacio Profundo con Códigos LDPC**", del estudiante Marco Yael Chavarría Ávila, quien presentó su examen de grado. El examen se aplicó bajo el Programa de Maestría y Doctorado en Ingeniería UNAM, el día 16 de diciembre de 2021.

- Se evaluó el trabajo de maestría "**Esquema de Compartición de Secretos con Detección Eficiente de Trampas**", del estudiante Daniel Becerra Pedraza, quien presentó su examen de grado. El examen tuvo lugar en las instalaciones del Posgrado de Ciencia e Ingeniería de la Computación en el IIMAS de la UNAM, el día 18 de septiembre de 2019.
- Se evaluó el trabajo doctoral "**Nuevo Esquema de Cifrado Totalmente Homomórfico**", del estudiante José Luis Juan Herrera García, quien presentó su examen de candidatura a nivel Doctorado. El examen tuvo lugar en las instalaciones del Posgrado de Ciencia e Ingeniería de la Computación en el IIMAS de la UNAM, el día 28 de febrero de 2018.
- Se evaluó el trabajo doctoral "**Generador de números pseudo-aleatorios basado en caminante pseudo-aleatorio determinista**" del estudiante Carlos Enrique Quijano Tapia, quien presentó su examen de candidatura a nivel Doctorado. El examen tuvo lugar en las instalaciones del Posgrado de Ciencia e Ingeniería de la Computación en el IIMAS de la UNAM, el día 28 de noviembre de 2018.
- Se evaluó el trabajo de maestría "**Algoritmo eficiente para el cálculo de las distribuciones de pesos de todos los códigos cíclicos irreducibles sobre campos finitos pequeños**", del estudiante Félix Alejandro Hernández Fuentes, quien presentó su examen de grado. El examen tuvo lugar en las instalaciones del Posgrado de Ciencia e Ingeniería de la Computación en el IIMAS de la UNAM, el día 18 de octubre de 2018.
- Examen de grado a nivel Maestría con la tesis de título "**Codificación para el control de errores en radios definidos por software**", del estudiante Saldaña Rosas Raymundo. Programa de Maestría y Doctorado en Ingeniería-UNAM, 22 de enero de 2016.
- Participación como jurado en el Examen de Grado de Doctora en Ciencias (Computación), de la estudiante M. en C. Mayra Lorena Díaz Sosa, quien presentó el trabajo "**Códigos sobre grupos cuánticos finitos y sus rangos combinatorios**". 24 de abril de 2015. Doctorado en Ciencias e Ingeniería de la Computación de la UNAM.
- Participación como jurado en el Examen de Grado de Doctor en Ciencias (Computación), del estudiante M. en C. Carlos Alberto Vázquez Fernández, quien presentó el trabajo "**Distribución de pesos de códigos cíclicos reducibles sobre campos finitos**". 8 de mayo de 2015. Doctorado en Ciencias e Ingeniería de la Computación de la UNAM.
- Examen General de Conocimientos a nivel Maestría del estudiante Roberto Blanco Galicia. Posgrado en Ciencias e Ingeniería de la computación-UNAM. 17 de junio de 2015.
- Examen de grado a nivel Maestría con la tesis de título "**Estudio del comportamiento dinámico entre protocolos de señalización (SIP y H.323) para el soporte del VOIP**", de la estudiante Sandra Nayeli Delgado Vieyra. Posgrado en Ciencias e Ingeniería de la computación-UNAM, 30 de julio de 2015.
- Examen de grado a nivel Maestría con la tesis de título "**Implementación y análisis de una red GPRS basada en OPENBTS y equipo USRP**", del estudiante Marco Antonio Juárez Aguirre. Posgrado en Ciencias e Ingeniería de la computación-UNAM, 6 de agosto de 2015.
- Participación como jurado para la segunda etapa del Examen de Candidatura al Grado de Doctor en Matemáticas, del estudiante M. en C. Rolando Gómez Macedo. 24 de septiembre de 2014. Doctorado en Ciencias Matemáticas de la UNAM.
- Examen de grado a nivel Maestría con la tesis de título "**Análisis y propuesta de Seguridad para Sistemas de Banca Móvil Mediante árboles de Ataque**", del estudiante Luis Hugo Flores Román. Posgrado en Ciencias e Ingeniería de la computación-UNAM, 10 de abril de 2014.
- Examen de grado a nivel Maestría con la tesis de título "**Estudio Instrumental de Propagación y Comportamiento Dinámico Basado en el Estándar IEEE 802.16**", del estudiante Andrade Baruch Iván. Posgrado en Ciencias e Ingeniería de la computación-UNAM, 14 de enero de 2014.

- Examen de grado a nivel Maestría con la tesis de título "**Propuesta de Metodología Forense Digital para Recolección de Datos No Volátiles en Dispositivos Móviles con Sistemas Operativos de Código Abierto**", del estudiante Ángel Hernández Seguro. Posgrado en Ciencias e Ingeniería de la computación-UNAM, 21 de octubre de 2013.
- Participación como jurado en el Examen de Candidatura al Grado de Doctor en Ciencias (Computación), de la estudiante M. en C. Mayra Lorena Díaz Sosa. 31 de enero de 2013. Doctorado en Ciencias e Ingeniería de la Computación de la UNAM.
- Participación como jurado en el Examen de Candidatura al Grado de Doctor en Ciencias (Computación), del estudiante M. en C. Carlos Alberto Vázquez Fernández. 26 de febrero de 2013. Doctorado en Ciencias e Ingeniería de la Computación de la UNAM.
- Examen de grado a nivel Maestría con la tesis de título "**SISTEMA PARA DETECCIÓN DE INTRUSOS EN LÍNEA BASADO EN ANOMALÍAS DE RED, USANDO REDES DE MEMORIA TEMPORAL JERÁRQUICA**", de la estudiante Naim de Luna Mendoza. Posgrado en Ciencias e Ingeniería de la computación-UNAM, marzo 2012.
- Examen de grado a nivel Maestría con la tesis de título "**IDENTIFICADOR INTELIGENTE DE INCIDENTES POR MEDIO DE UN IDS BASADO EN ANOMALIAS UTILIZANDO LA PLATAFORMA NUMENTA**", de la estudiante Rosa Xochitl Sarabia Bautista. Posgrado en Ciencias e Ingeniería de la computación-UNAM, agosto 2012.
- Examen de grado a nivel Doctoral con la tesis de título "**Códigos Lagrangianos-Grassmannianos**", de el estudiante Jesús Carrillo Pacheco. UAM-I, noviembre de 2011. Doctorado en Ciencias Matemáticas de la UAM-I.
- Examen predoctoral con la tesis de título "**Studies on Disk Encryption**", de el estudiante Cuauhtemoc Mancillas López. CINVESTAV-IPN, mayo de 2011.
- Examen predoctoral con la tesis de título "**DISAGREE: Disagreement-based Querying in Gíreles Sensor Networks**", de la estudiante Martha Montes de Oca. Posgrado en Ciencias e Ingeniería de la computación-UNAM, marzo de 2011.
- Tesis a nivel maestría de título "**Estudio de las oportunidades de codificación en redes inalámbricas tipo AD HOC**", de el estudiante Carlos G. Guadarrama González. Posgrado en Ciencias e Ingeniería de la computación-UNAM, Marzo 2011.
- Tesis a nivel maestría de título "**Estudio y Desarrollo de un Sistema de Estimación de Dirección de Nodos Móviles en Sistemas Inalámbricas Basados en Wlan**", de el estudiante Rafael Iván Peralta Rios. Posgrado en Ciencias e Ingeniería de la computación-UNAM, 14 febrero 2011.
- Tesis a nivel maestría de título "**Análisis de Estrategias de Codificación y Decodificación para Códigos BCH Utilizando un Simulador de Canal de Ruido**", de el estudiante Mario Octavio Carrazco Delgado. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Febrero 2010.
- Tesis a nivel maestría de título "**Sistema de Detección de Intrusos Basados en Anomalias de Red Usando la Plataforma Numenta para Cómputo Inteligente**", de el estudiante José Roberto Sánchez Soledad. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Junio 2010.
- Tesis a nivel maestría de título "**Estudio de Sistemas Multicore para Cómputo de Alto Rendimiento**", de la estudiante Clara Vicente Hernández. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Marzo 2009.
- Sinodal del Examen Doctoral de la estudiante Lic. María Guadalupe Cota Ortiz, de la Universidad Autónoma del Estado de Hidalgo, adscrita al Instituto de Ciencias Básicas e Ingeniería. Titulo "**Elementos básicos para diseño y desarrollo de sistemas multiagente orientados a seguridad en redes de equipos de cómputo con ambiente Windows-Tecnología NT**" El examen se efectuó en el Centro de Investigación en Tecnologías de Información y Sistemas, de dicha Universidad, el día 25 de Septiembre de 2009.

- Tesis a nivel maestría de título "**Minimización del Ataque DDoS sobre Servidores de Comercio Electrónico, Utilizando la Predicción Lineal**", de el estudiante Cuauhtémoc Carlon Carlon. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Marzo 2009.
- Tesis a nivel maestría de título "**Análisis del Desempeño de la Capa Física Basada en OFDM para las Redes Inalámbricas de Banda Ancha, Basadas en el Estandar IEEE 802.16-2004**", de la estudiante Gabriela Henriquez Campos. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Abril 2009.
- Tesis a nivel maestría de título "**Análisis y Diseño de Mecanismos de Handoff en Redes Inalámbricas de Banda Ancha IEEE 802.16e**", de el estudiante Víctor Toledo Pérez. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Septiembre 2009.
- Tesis a nivel maestría de título "**Análisis de Estrategias de Codificaci[on y Decodificación para Códigos BCH Utilizando un Simulador de Canal de Ruido**", de el estudiante Mario Octavio Carrazco Delgado. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Agosto 2009.
- Tesis a nivel maestría de título "**Análisis de Tecnicas de Control de Potencia para Redes Móviles IEEE 802.16e**", de la estudiante Margarita Muñoz Goncen. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Septiembre 2009.
- Presentación del Examen Predoctoral de la estudiante Lic. María Guadalupe Cota Ortiz, de la Universidad Autónoma del Estado de Hidalgo, adscrita al Instituto de Ciencias Básicas e Ingeniería. El examen se efectuó en el Centro de Investigación en Tecnologías de Información y Sistemas, de dicha Universidad, el día jueves 27 de Noviembre de 2008.
- Tesis a nivel maestría de título "**Análisis del comportamiento Dinámico de Redes Inalámbricas de Banda Ancha con Arquitectura MESH**", de la estudiante Yasmine Macedo Reza. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Noviembre de 2008.
- Tesis a nivel maestría de título "**Codificación de Redes y Sistemas Distribuidos**", de la estudiante Carlos Iván Guerrero Román. Posgrado en Ciencias e Ingeniería de la computación-UNAM. 2008.
- Tesis a nivel maestría de título "**Protocolo Seguro para Redes AD HOC**", de la estudiante Paola Díaz Flores. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Julio de 2007.
- Tesis a nivel maestría de título "**Revisión técnica de los estándares de televisión digital terrestre para su evaluación en un proceso de adopción**", del estudiante Rafael Marcos Montante López. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Junio de 2006.
- Tesis a nivel maestría de título "**Autenticación de usuarios en redes inalámbricas mediante el uso de un protocolo robusto para el manejo de contraseñas débiles**", del estudiante Juan Fco. García Navarro. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Noviembre de 2005.
- Tesis a nivel maestría de título "**UNAMCA Autoridad Certificadora para la UNAM**", del estudiante Enrique Reyes Castillo. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Marzo de 2006.
- Tesis a nivel maestría de título "**Implementación de un Sistema de Votaciones en Internet Utilizando un Protocolo Basado en Criptografía de Curvas Elípticas**", del estudiante Otoniel Manuel Ortiz Ruiz. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Octubre de 2005.
- Tesis a nivel maestría de título "**Comparación Entre Esquemas de Seguridad: Programa PREP y Propuesta de Recopilación de Datos Electorales de Urna Electrónicas del IEDF**", del estudiante Jesús Hernández Cabrera. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Se revisó la tesis, pero se reprobó el trabajo, 2005.
- Tesis a nivel maestría de título "**Metodología para la Aplicación de la Norma ISO/IEC 17799**", de la estudiante Cintia Quezada Reyes. Posgrado en Ciencias e Ingeniería de la computación-UNAM. 2005.

- Tesis a nivel maestría de título "**Diseño e Implementación de Mecanismos de Control de la Concurrencia para un Sistema de Edición Colaborativa en Internet e Intranet**", de la estudiante Silvia Ramírez García. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Octubre 2003.
- Tesis a nivel maestría de título "**Implementación de un Sistema de Cifrado de Llave Pública Basado en el Problema del Logaritmo Discreto para Curvas Elípticas**", del estudiante Moisés Bautista Osorno. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Diciembre de 2002.
- Tesis a nivel maestría de título "**Estudio del Estándar H.323 para Transmisión en Tiempo Real en Videoconferencias**", de la estudiante Patricia Chinos Ramírez. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Junio de 2002.
- Tesis a nivel maestría de título "**Un espacio de trabajo compartido como apoyo a la edición colaborativa en internet**", del estudiante Henry Afranio Perez Luna. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Octubre de 2001.
- Tesis a nivel maestría de título "**Un espacio de tuplas tolerante a fallas**", del estudiante Jorge A. López Velarde. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Agosto de 2001.
- Tesis a nivel maestría de título "**Protocolos criptográficos de autenticación e intercambio de llaves basados en password**", del estudiante Leobardo Hernández Audelo. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Septiembre de 1999.
- Tesis a nivel licenciatura de título "**El problema de falsificación de firmas digitales intrínsecamente protegidas**", del estudiante Jose Abel Gonzalez Silva. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Noviembre de 1999.
- Tesis a nivel licenciatura de título "**Análisis y desarrollo de un algoritmo de cifrado de llave privada tipo RC5**", del estudiante Raúl Cristóbal Hernández. Posgrado en Ciencias e Ingeniería de la computación-UNAM. Junio de 1998.

2.6 Labor docente en la evaluación y en la aplicación de exámenes

2.6.1 Participación en Evaluaciones Semestrales de Estudiantes Doctorales

- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2024-1, Fecha 08/12/2023.
- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2023-2, Fecha 12/06/2023.
- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2023-1, Fecha 9/12/2022.
- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2022-2, Fecha 13/06/2022.
- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2022-1, Fecha 15/12/2021.
- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2021-2, Fecha 18/06/2021.
- Evaluación semestral del estudiante doctoral Félix Alejandro Hernández Fuentes. Año-Semestre 2021-1, Fecha 05/02/2021.
- Evaluación semestral del estudiante doctoral Carlos E. Quijano Tapia. Año-Semestre 2020-2, Fecha 06/08/2020.
- Evaluación semestral del estudiante doctoral Carlos E. Quijano Tapia. Año-Semestre 2020-1, Fecha 9/dic/2019.

2.6.2 Participación como Evaluador para los Coloquios de Investigación I y II

- Se evaluaron los avances académicos de 5 estudiantes de Maestría de la área de Redes y Seguridad en Cómputo del Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. Junio 21 de 2018.
- Se evaluaron los avances académicos de 6 estudiantes de Maestría de la área de Redes y Seguridad en Cómputo del Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. Diciembre 6 de 2017.

2.6.3 Participación como entrevistador para aspirantes a estudiantes de doctorado

- Entrevista realizada al aspirante a estudiante doctoral Mariano Larios G., el día miércoles 21 de junio de 2017, en las instalaciones del Posgrado de Ciencia e Ingeniería de la Computación de la UNAM.

2.6.4 Participación como jurado en exámenes generales de conocimientos

- Examen General de Conocimientos a nivel Maestría del alumna JOSÉ LUIS VÁZQUEZ LÁZARO. Programa de Maestría y Doctorado en Ingeniería-UNAM, 1 de abril 2024.
- Examen General de Conocimientos a nivel Maestría del alumna VALADEZ GOMEZ SUSANA. Programa de Maestría y Doctorado en Ingeniería-UNAM, 30 de abril 2021.
- Examen General de Conocimientos a nivel Maestría del alumno JONATHAN PONCIANO VERA. Programa de Maestría y Doctorado en Ingeniería-UNAM, 29 de agosto de 2016 y 9 de marzo de 2017.

2.6.5 Elaboración y aplicación de exámenes extraordinarios

- Examen para el Laboratorio de Teleproceso, Facultad de Ciencias de la UNAM, junio del 2000.
- Examen para el curso de álgebra Lineal, área de Ciencias Básicas e Ingeniería de la UAM-I, enero de 2002 (durante estancia sabática en la UAM-I).

2.7 Generación de contenidos audiovisuales

- Clases varias sobre Teoría de Códigos, Criptografía y Campos Finitos (2019-2022):
  https://www.youtube.com/channel/UCkk4m4sggK01zo0l8G16BBw
  https://drive.google.com/drive/folders/1kdkqkBw7GL2VsuVr7oRpxhc3OlGVG-Bb?usp=sharing
  https://drive.google.com/drive/folders/1l_qzzyWjX6guhAqLIm7n5CuNbW1gtJvb?usp=sharing
  https://drive.google.com/drive/folders/1KN8k7Bfk2hJps2IXlirXX6luq0hmMcIs?usp=sharing
- Conferencia para congreso internacional (WAIFI-2020):
  https://www.youtube.com/watch?v=W5Vhn-vB3ZI&t=15s

2.8 Elaboración de material docente

- Durante los dos últimos años (2017 y 2018), y con la importante ayuda del M. en I. Alejandro Talavera Rosales, se ha continuado la transcripción de mis notas de clase del curso de criptografía, con la idea de elaborar unas notas de apoyo para un curso sobre Criptografía Moderna Comercial.
- Gerardo Vega, se elaboró el material didáctico donde se presenta"**Una nueva manera de explicar la decodificación, para los códigos de Reed-Muller, que sólo requiere conocimientos de teoría de conjuntos**", Miscelánea Matemática Vol. 42, Enero 2006, pp. 27-50. ISSN-1665-5478.

3 Productividad académica

3.1 Distinciones como miembro del SNI

- Miembro del Sistema Nacional de Investigadores, como Investigador Nacional Nivel II durante el período del 1 de enero de 2023 al 31 de diciembre de 2027.

- Miembro del Sistema Nacional de Investigadores, como Investigador Nacional Nivel II durante el período del 1 de enero de 2018 al 31 de diciembre de 2022.
- Miembro del Sistema Nacional de Investigadores, como Investigador Nacional Nivel II durante el período del 1 de enero de 2013 al 31 de diciembre de 2017.
- Miembro del Sistema Nacional de Investigadores, como Investigador Nacional Nivel II durante el período del 1 de enero de 2009 al 31 de diciembre de 2012.
- Miembro del Sistema Nacional de Investigadores, como Investigador Nacional Nivel I durante el período del 1 de enero de 2005 al 31 de diciembre de 2008.
- Miembro del Sistema Nacional de Investigadores, como Investigador Nacional Nivel I durante el período del 10 de octubre del 2001 al 30 de junio del 2004.
- Miembro del Sistema Nacional de Investigadores, como Candidato a Investigador durante el período del 1 de julio de 1997 al 30 de junio del 2000.

3.2 Publicaciones

3.2.1 Publicaciones en revistas internacionales INDIZADAS CON ARBITRAJE y con reporte de FACTOR DE IMPACTO

En la siguiente lista se incluye, para cada artículo, el número de Citas Tipo A (no autocitas) y el número de autocitas. Para una descripción detallada de tales citas, consultar:
http://www.paginaspersonales.unam.mx/app/webroot/files/6335/Citas.pdf.

- Félix Hernández & Gerardo Vega, "**Obtaining new classes of optimal linear codes by puncturing and shortening optimal cyclic codes**", Por publicarse en Applicable Algebra in Engineering, Communication and Computing (Springer), 2024. DOI: https://doi.org/10.1007/s00200-024-00653-7.
- Félix Hernández & Gerardo Vega, "**The Subfield and Extended Codes of a Subclass of Optimal Three-Weight Cyclic Codes**", Algorithmica (Springer), vol. 85, pp. 3973-3995, 2023. Citas Tipo A=0 y autocitas=0. p-ISSN:0178-4617, e-ISSN:1432-0541, Impact Factor: 1.1.
DOI: https://doi.org/10.1007/s00453-023-01173-5.
- Gerardo Vega, "**The b-symbol weight distributions of all semiprimitive irreducible cyclic codes**", Designs, Codes and Cryptography (Springer), vol. 91(6), pp. 2213-2221, 2023. Citas Tipo A=0 y autocitas=0. p-ISSN:0925-1022, e-ISSN:1573-7586. Impact Factor: 1.640. DOI: https://doi.org/10.1007/s10623-023-01193-w.
- Gerardo Vega, "**Lee weight distributions of trace codes over $\mathbb{F}_q + u\mathbb{F}_q$ from irreducible cyclic codes**", Journal of Algebra Combinatorics Discrete Structures and Applications (Jacodesmath Institute), vol. 10(2), pp. 87-96, 2023. Citas Tipo A=0 y autocitas=0. p-ISSN: 2148-838X. Impact Factor: 1.03. DOI https://doi.org/10.13069/jacodesmath.v10i2.197.
- Gerardo Vega & Félix Hernández, "**The complete weight distribution of a subclass of optimal three-weight cyclic codes**", Cryptography and Communications (Springer), vol. 15, pp. 317-330, 2023. Citas Tipo A=0 y autocitas=0. p-ISSN:1936-2447, e-ISSN:1936-2455, Impact Factor: 1.376. DOI: https://doi.org/10.1007/s12095-022-00601-7.
- Gerardo Vega & Jesús E. Cuén-Ramos, "**The weight distribution of families of reducible cyclic codes through the weight distribution of some irreducible cyclic codes**", Advances in Mathematics of Communications (American Institute of Mathematical Sciences), vol. 14(3), pp. 525-533, 2020. Citas Tipo A=0 y autocitas=0. p-ISSN:1930-5346, e-ISSN:1930-5338. Impact Factor: 0.92. DOI: 10.3934/amc.2020059.
- Gerardo Vega, "**A characterization of all semiprimitive irreducible cyclic codes in terms of their lengths**", Applicable Algebra in Engineering, Communication and Computing (Springer), vol. 30(5), pp. 441-452, 2019. Citas Tipo A=**1** y autocitas=1. p-ISSN:0938-1279, e-ISSN:1432-0622. Impact Factor: 1.085. DOI: doi.org/10.1007/s00200-019-00385-z.

- Gerardo Vega, "**A correction on the determination of the weight enumerator polynomial of some irreducible cyclic codes**", Designs, Codes and Cryptography (Springer), vol. 86(4), pp. 835-840, 2018. Citas Tipo A=0 y autocitas=0. p-ISSN:0925-1022, e-ISSN:1573-7586. Impact Factor: 1.640. DOI: doi.org/10.1007/s10623-017-0364-2.
- Gerardo Vega, "**The weight distribution for any irreducible cyclic codes of length p^m**", Applicable Algebra in Engineering, Communication and Computing (Springer), vol. 29(4), pp. 363-370, 2018. Citas Tipo A=**5** y autocitas=1. p-ISSN:0938-1279, e-ISSN:1432-0622. Impact Factor: 1.085. DOI: doi.org/10.1007/s00200-017-0347-6.
- Gerardo Vega, "**An extended characterization of a class of optimal three-weight cyclic codes over any finite field**", Finite Fields and Their Applications (Elsevier), vol. 48, pp. 160-174, 2017. Citas Tipo A=0 y autocitas=0. p-ISSN: 1071-5797. Impact Factor: 1.310. DOI: doi.org/10.1016/j.ffa.2017.07.010.
- Gerardo Vega, "**An improved method for determining the weight distribution of a family of q-ary cyclic codes**", Applicable Algebra in Engineering, Communication and Computing (Springer), vol. 28(6), pp. 527-533, 2017. Citas Tipo A=0 y autocitas=1. p-ISSN:0938-1279, e-ISSN:1432-0622. Impact Factor: 1.085. DOI: doi.org/10.1007/s00200-017-0318-y.
- Jesús E. Cuén-Ramos & Gerardo Vega, "**A class of cyclic codes constructed via semiprimitive two-weight irreducible cyclic codes**", Journal of Algebra Combinatorics Discrete Structures and Applications (Jacodesmath Institute), vol. 4(3), pp. 281-290, 2017. Citas Tipo A=0 y autocitas=0. p-ISSN: 2148-838X. Impact Factor: 1.03. DOI: 10.13069/jacodesmath.327385.
- Gerardo Vega, "**A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field**", Finite Fields and Their Applications (Elsevier), vol. 42, pp. 23-38, 2016. Citas Tipo A=**7** y autocitas=1. p-ISSN: 1071-5797. Impact Factor: 1.310. DOI: doi.org/10.1016/j.ffa.2016.07.001.
- Gerardo Vega, "**A critical review and some remarks about one- and two-weight irreducible cyclic codes**", Finite Fields and Their Applications (Elsevier), vol. 33, pp. 1-13, 2015. Citas Tipo A=**7** y autocitas=1. p-ISSN: 1071-5797. Impact Factor: 1.310. DOI: doi.org/10.1016/j.ffa.2014.11.001.
- Luis B. Morales & Gerardo Vega, "**On the enumeration of $E(s^2)$-optimal and minimax-optimal k-circulant supersaturated designs**", Journal of Combinatorial Designs (Wiley), vol. 22(4), pp. 149-160, 2014. Citas Tipo A=0 y autocitas=2. p-ISSN:1063-8539, e-ISSN:1520-6610. Impact Factor: 0.657. DOI: 10.1002/jcd.21341.
- Gerardo Vega & Luis B. Morales, "**A General Description for the Weight Distribution of Some Reducible Cyclic Codes**", IEEE Transactions on Information Theory (IEEE Information Theory Society), vol. 59(9), pp. 5994-6001, 2013. Citas Tipo A=**3** y autocitas=0. p-ISSN:0018-9448, e-ISSN:1557-9654. Impact Factor: 2.65. DOI: 10.1109/TIT.2013.2263195.
- Gerardo Vega, "**The Weight Distribution of an Extended Class of Reducible Cyclic Codes**", IEEE Transactions on Information Theory (IEEE Information Theory Society), vol. 58(7), pp. 4862-4869, 2012. Citas Tipo A=**45** y autocitas=0. p-ISSN:0018-9448, e-ISSN:1557-9654. Impact Factor: 2.65. DOI: 10.1109/TIT.2012.2193376.
- Gerardo Vega, "**A Note About Two-Weight Non-Irreducible Cyclic Codes**", IEEE Transactions on Information Theory (IEEE Information Theory Society), vol. 58(4), pp. 2263-2264, 2012. Citas Tipo A=**2** y autocitas=0. p-ISSN:0018-9448, e-ISSN:1557-9654. Impact Factor: 2.65. DOI: 10.1109/TIT.2011.2178113.
- Carlos A. Vázquez & Gerardo Vega, "**On the Weight Distribution of the Dual of some Cyclic Codes with Two Non Conjugated Zeros**", Journal of Applied Research and Technology (SciELO), vol. 9(1), pp. 36-48, 2011. Citas Tipo A=**1** y autocitas=0. p-ISSN:1665-6423, e-ISSN:2448-6736. Impact per Paper (SNIP): 1.216. DOI: http://www.scielo.org.mx/pdf/jart/v9n1/v9n1a3.pdf.
- Gerardo Vega, "**Some Precisions On PS Bent Functions**", International Mathematical Forum (Hikari Ltd), vol. 5(11), pp. 537-544, 2010. Citas Tipo A=**3** y autocitas=0. p-ISSN:1312-7594, e-ISSN:1314-7536. Impact Factor: 0.5. DOI: http://www.m-hikari.com/imf-2010/9-12-2010/index.html.

- Gerardo Vega, "**Two-weight Cyclic Codes Constructed as the Direct Sum of Two One-weight Cyclic Codes**", Finite Fields and Their Applications (Elsevier), vol. 14(3), pp. 785-797, 2008. Citas Tipo A=**16** y autocitas=0. p-ISSN:1071-5797. Impact Factor: 1.310. DOI: doi.org/10.1016/j.ffa.2008.01.002.
- Omran Ahmadi & Gerardo Vega, "**On the Parity of the Number of Irreducible Factors of Self-reciprocal Polynomials over Finite Fields**", Finite Fields and Their Applications (Elsevier), vol. 14(1), pp. 124-131, 2008. Citas Tipo A=**11** y autocitas=1. p-ISSN:1071-5797. Impact Factor: 1.310. DOI: doi.org/10.1016/j.ffa.2006.09.004.
- G. Vega & Jacques Wolfmann, "**New Classes of 2-weight Cyclic Codes**", Designs, Codes and Cryptography (Springer), vol. 42(3), pp. 327-334, 2007. Citas Tipo A=**27** y autocitas=1. p-ISSN:0925-1022, e-ISSN:1573-7586. Impact Factor: 1.640. DOI: doi.org/10.1007/s10623-007-9038-9.
- Gerardo Vega, "**A Characterization for the Reducibility of some Self-reciprocal Binary Pentanomials**", International Mathematical Forum (Hikari Ltd), vol. 2(29-32), pp. 1507-1524, 2007. Citas Tipo A=0 y autocitas=0. p-ISSN:1312-7594, e-ISSN:1314-7536. Impact Factor: 0.5. DOI: dx.doi.org/10.12988/imf.2007.07137.
- Gerardo Vega, "**Nonlinear Cyclic Codes over Z_4 whose Nechaev-Gray Images are Binary Linear Cyclic Codes**", International Mathematical Forum (Hikari Ltd), vol. 1(17-20), pp. 809-821, 2006. Citas Tipo A=0 y autocitas=0. p-ISSN:1312-7594, e-ISSN:1314-7536. Impact Factor: 0.5. DOI: dx.doi.org/10.12988/imf.2006.06068.
- Gerardo Vega & Jacques Wolfmann, "**Some Families of Z_4-Cyclic Codes**", Finite Fields and Their Applications (Elsevier), vol. 10, pp. 530-539, 2004. Citas Tipo A=**7** y autocitas=1. p-ISSN:1071-5797. Impact Factor: 1.310. DOI: doi.org/10.1016/j.ffa.2003.11.003.
- A. Huertas-Vázquez, G. Vega-Hernández, et al, "**Contribution of Chromosome 1q21-q23 to Familial Combined Hyperlipidemia in Mexican Families**", Annals of Human Genetics, University College London 2004. Citas Tipo A=**7** y autocitas=0. e-ISSN:1469-1809. Impact Factor: 2.211. DOI: https://doi.org/10.1046/j.1529-8817.2003.00116.x.
- H. Tapia-Recillas & G. Vega, "**On Z_{2^k}-Linear and Quaternary Codes**", Journal on Discrete Mathematics (Society for Industrial and Applied Mathematics), vol. 17(1), pp. 103-113, 2003. Citas Tipo A=**17** y autocitas=7. p-ISSN:0895-4801, e-ISSN:10957146. Impact Factor: 0.967. DOI: doi.org/10.1137/S0895480101397219.
- H. Tapia-Recillas & G. Vega, "**Some Constacyclic Codes over Z_{2^k} and Binary Quasicyclic Codes**", Discrete Applied Mathematics (Elsevier), vol. 128, pp. 305-316, 2003. Citas Tipo A=**23** y autocitas=3. p-ISSN:0166-218X. Impact Factor: 1.31. DOI: doi.org/10.1016/S0166-218X(02)00453-5.
- Samuel Canizales-Quinteros, Gerardo Vega-Hernández, et al, "**Locus on Chromosome 6p Linked to Elevated HDL Cholesterol Serum Levels and to Protection Against Premature Atherosclerosis in a Kindred With Familial Hypercholesterolemia**", Circulation Research, American Heart Association Journals, vol. 92, pp. 569-576, 2003. Citas Tipo A=**17** y autocitas=0. e-ISSN:0009-7330. Impact factor: 11.019. DOI: https://doi.org/10.1161/01.RES.0000064174.69165.66.
- H. Tapia-Recillas & G. Vega, "**A Generalization of Negacyclic Codes**", Electronic Notes in Discrete Mathematics (Elsevier), vol. 6, pp. 251-261, 2001. Citas Tipo A=**6** y autocitas=1. p-ISSN:15710653. DOI: https://doi.org/10.1016/S1571-0653(04)00176-3.
- H. Tapia-Recillas & G. Vega, "**An upper bound on the number of iterations for transforming a Boolean function of degree greater or equal than 4 to a function of degree 3**", Designs, Codes and Cryptography (Kluwer Academic Publishers), vol. 24(3), pp. 305-312, 2001. Citas Tipo A=**1** y autocitas=0. p-ISSN:0925-1022, e-ISSN:1573-7586. Impact Factor: 1.640. DOI: doi.org/10.1023/A:1011279406162.
- Laura del Bosque-Plata, Gerardo Vega-Hernández, et al., "**Analysis of the Glucokinase Gene in Mexican Families Displaying Early-Onset Non-Insulin-Dependent Diabetes Mellitus Including MODY Families**", American Journal of Medical Genetics, vol. 72(2), pp. 387-393, 1997. Citas Tipo A=7 y autocitas=0. e-ISSN:1552-4833. Impact Factor: 2.159. DOI: 10.1002/(sici)1096-8628(19971112)72:4¡387::aid-ajmg3¿3.0.co;2-o.

- Luis Guillermo Cota, Gerardo Vega, Rodrigo Correa y Luis Javier Alvarez, "**Determination of structural Features in Simulated Amorphous Materials by Straightforward Methods**", Molecular Simulation (Taylor & Francis), vol. 20, pp. 315-330, 1998. Citas Tipo A=0 y autocitas=1. p-ISSN:0892-7022, e-ISSN:10290435. Impact Factor 1.133. DOI: https://doi.org/10.1080/08927029808022040.

3.2.2 Memorias en extenso en congresos internacionales CON ARBITRAJE

En la siguiente lista se incluye, para cada artículo, el número de Citas Tipo A (no autocitas) y el número de autocitas. Para una descripción detallada de tales citas, consultar:
http://paginaspersonales.unam.mx/app/webroot/files/6335/Citas.pdf.

- Félix Hernández & Gerardo Vega, "**On the Subfield Codes of a Subclass of Optimal Cyclic Codes and Their Covering Structures**", in "Latin American Symposium on Theoretical Informatic, LATIN 2022 (Eds. A. Castañeda, et al.)", Lecture Notes in Computer Science (Springer), vol. 13568, pp. 255–270, 2022. Citas Tipo A=0 y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: https://doi.org/10.1007/978-3-031-20624-5_16.

- Gerardo Vega, "**Explicit factorization of some period polynomials**", in "Proceedings of International Workshop on the Arithmetic of Finite Fields WAIFI 2020 (Eds. Jean Claude Bajard, et al.)", Lecture Notes in Computer Science (Springer), vol. 12542, pp. 222–233, 2021. Citas Tipo A=0 y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/978-3-030-68869-1_13.

- Daniel Becerra & Gerardo Vega, "**Secret Sharing Scheme with Efficient Cheating Detection**", in "Proceedings of the 2nd International Conference on Networking, Information Systems & Security (Eds. Badr Abouelmajd, et al.)", Article No. 5, pp. 1–7, 2019. Citas Tipo A=1 y autocitas=0. ISBN 978-1-4503-6645-8/19/03. DOI: doi.org/10.1145/3320326.3320331. Cabe destacar que este artículo obtuvo el 2 lugar al mejor artículo presentado al mencionado congreso internacional arbitrado, en el cual se presentaron más de medio centenar (63) de artículos.

- Jesús E. Cuén-Ramos & Gerardo Vega, "**The weight distribution of families of reducible cyclic codes through the weight distribution of some irreducible cyclic codes**", in "Latin American Week on Coding and Information LAWCI 2018 (Eds. Marcelo Firer, et al.), UNICAMP-Campinas, Brazil, 2018, july 22-27". Citas Tipo A=0 y autocitas=0.

- Gerardo Vega & Jesús E. Cuén-Ramos, "**The Weight Distribution for an Extended Family of Reducible Cyclic Codes**", in "Second International Conference in Codes, Cryptology and Information Security, C2SI 2017 (Eds. Said El Hajji, et al.)", Lecture Notes in Computer Science (Springer), vol. 10194, pp. 213-229, 2017. Citas Tipo A=0 y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/978-3-319-55589-8_14.

- Gerardo Vega, "**A Family of Six-Weight Reducible Cyclic Codes and their Weight Distribution**", in "First International Conference in Codes, Cryptology and Information Security, C2SI 2015 (Eds. Abderrahmane Nitaj, et al.)", Lecture Notes in Computer Science (Springer), vol. 9084, pp. 184-196, 2015. Citas Tipo A=0 y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/978-3-319-18681-8_15.

- Jesús Carrillo-Pacheco, Gerardo Vega & Felipe Zaldívar, "**The Weight Distribution of a Family of Lagrangian-Grassmannian Codes**", in "First International Conference in Codes, Cryptology and Information Security, C2SI 2015 (Eds. Abderrahmane Nitaj, et al.)", Lecture Notes in Computer Science (Springer), vol. 9084, pp. 240-246, 2015. Citas Tipo A=0 y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/978-3-319-18681-8_19.

- Gerardo Vega & Carlos A. Vázquez, "**The Weight Distribution of a Family of Reducible Cyclic Codes**", in "Proceedings of International Workshop on the Arithmetic of Finite Fields WAIFI 2012 (Eds. Ferruh Özbudak, et al.)", Lecture Notes in Computer Science (Springer), vol. 7369, pp. 16-28, 2012. Citas Tipo A=**3** y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/978-3-642-31662-3_2.

- Gerardo Vega, "**On the Number of Two-weight Cyclic Codes with Composite Parity-check Polynomials**", in "Proceedings of International Workshop on the Arithmetic of Finite Fields WAIFI 2008 (Eds. Joachim Gathen, et al.)", Lecture Notes in Computer Science (Springer), vol. 5130, pp. 144-156, 2008. Citas Tipo A=0 y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/978-3-540-69499-1_13.

- Gerardo Vega, "**Determining the Number of One-weight Cyclic Codes when Length and Dimension are Given**", in "Proceedings of International Workshop on the Arithmetic of Finite Fields WAIFI 2007 (Eds. Claude Carlet, et al.)", Lecture Notes in Computer Science (Springer), vol. 4547, pp. 284-293, 2007. Citas Tipo A=**16** y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: 10.1007/978-3-540-73074-3_22.

- H. Tapia-Recillas & G. Vega, "**On the F_p-Linearity of the Generalized Gray Map image of a $Z_{p^{k+1}}$-Linear Code**", in "Proceedings of Finite Fields with Applications to Coding Theory Cryptography and Related Areas, Fq6 (Eds. Gary L. Mullen, et al.)", Springer Verlag, May 2001, pp. 306-312. ISBN 978-3-642-59435-9. Citas Tipo A=0 y autocitas=2.

- H. Tapia-Recillas & G. Vega, "**A Generalization of Negacyclic Codes**", in "Proceedings of International Workshop on Coding and Cryptography, WCC 2001 (Eds. Claude Carlet, et al.)", Junuary 2001, París Francia, pp. 519-529.

- N. Gutiérrez-Herrera, H. Tapia-Recillas & G. Vega, "**A Parseval type of relation on Z_n**", in "Proceedings of World Multiconference on Systems, Cybernetics and Informatics, SCI 2000", Orlando Florida julio del 2000, pp. 672-674. Citas Tipo A=0 y autocitas=0.

- H. Tapia-Recillas, G. Vega & E. Daltabuit, "**Some Results on Regular Mappings**", in "Proceedings of Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, AAECC-12, (Eds. Teo Mora, et al.)", Lecture Notes in Computer Science (Springer), vol. 1255, pp. 321-328, 1997. Citas Tipo A=**5** y autocitas=0. p-ISSN:0302-9743, e-ISSN:1611-3349. Impact Factor 1.363. DOI: doi.org/10.1007/3-540-63163-1_25.

- L. Hernández & G. Vega, "**Protocolo para Autenticación, Intercambio de llaves e Información Seguros en Comunicaciones remotas**", en las "Memorias de la Conferencia Internacional Ciencia y Tecnología para el Desarrollo, I Simposio de Telemática CIMAF'97 (Eds. Luis Pastor Sánchez Fernández)", pp. 6-16. 1998. Citas Tipo A=0 y autocitas=0.

3.2.3 Publicaciones en revistas internacionales CON ARBITRAJE, sin reporte FACTOR DE IMPACTO, pero INDIZADAS según la clasificación del Instituto de Matemáticas de la UNAM

- Gerardo Vega, "**Una nueva manera de explicar la decodificación, para los códigos de Reed-Muller, que sólo requiere conocimientos de teoría de conjuntos**", Miscelánea Matemática Vol. 42, Enero 2006, pp. 27-50. ISSN-1665-5478.

3.2.4 Publicaciones en revistas CON ARBITRAJE

- Gerardo Vega, "**Firmas Digitales**", Suplemento ENTERATE de la gaceta de la UNAM, 26 de septiembre 2002, pp. 2-5.

- Gerardo Vega, "**Los Sistemas de Recuperación de Información por indexación de triadas, una experiencia**", Revista Internacional de Centro Universitario de Investigaciones Bibliotecológicas UNAM, vol. 8 Número 17 (1994), pp. 10-17. ISSN: 0187-358X.

- Gerardo Vega, "**Técnicas de Búsqueda**", Soluciones Avanzadas, abril 1995, pp. 55-57.

3.2.5 Memorias en extenso en congresos nacionales

- Daniel Becerra & Gerardo Vega, "**Esquema de compartición de secretos con detección eficiente de trampas**", XIII Coloquio Nacional Teoría de Códigos, Criptografía y áreas Relacionadas, Palacio de Minería de la UNAM. Del 24 al 26 de abril de 2019.
- José Luis Juan Herrera García & Gerardo Vega, "**Sumando en Cifrado Homomórfico sin Arranque**", 12o Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas. Casa de la Primera Imprenta en América, Ciudad de México. Universidad Autónoma Metropolitana, 27 de junio de 2017.
- Elisandro Cuén & Gerardo Vega, "**Una Familia de Códigos Cíclicos Reducibles de Seis Pesos y su Distribución Pesos**", Decimoprimero Coloquio Nacional Teoría de Códigos, Criptografía y áreas Relacionadas, Facultad de Ciencias Físico Matemáticas BUAP. Del 16 al 19 de junio de 2015.
- Tapia-Recillas & G. Vega, "**Los principales sistemas de cifrado simétrico en la actualidad**", Memorias del Congreso General de Cómputo "cómputo.99mx".
- Tapia-Recillas & G. Vega, "**Una Generalización de los Códigos Negacíclicos**", Memorias del Congreso de Seguridad en Cómputo 2000.
- Tapia-Recillas & G. Vega, "**A cyclic approach to bent functions**", en las "Memorias del XXXI Congreso Nacional de la Sociedad Matemática Mexicana, Aportaciones Matemáticas, Serie Comunicaciones", vol. 25, pp. 109-114, 1999. Citas Tipo A=0 y autocitas=0.
- A. Santillan, G. Vega, R. Gómez, A. Villareal, G. Cisneros, "**Niveles de Optimización de Programas en la Supercomputadora CRAY**", Memorias de la Octava conferencia internacional: Las Computadoras en las Instituciones de Educación y de Investigación. 12 de noviembre de 1992.

3.2.6 Reportes técnicos

- Gerardo Vega Hernández, "**Nueva Definición ASN.1 para la NOM-151**", Secretaría de Economía, Noviembre de 2007.

3.3 Asesorías especializadas

- Desde finales del 2006, se tuvieron reuniones de trabajo con el personal de Normatividad de la Secretaría de Economía, con el objeto de concretar y realizar un nuevo proyecto de investigación y desarrollo alrededor de la Norma Oficial Mexicana número 151 (NOM-151). La idea, para este caso, fue la de investigar y evaluar los protocolos para el estampado de sellos de tiempo, con el objeto de que a la NOM-151 se le incorpore un servicio de este tipo. Este proyecto finalmente se concretó formalmente bajo un convenio de colaboración entre la UNAM y la Secretaría de Economía, el cual tuvo vigencia durante los últimos cuatro meses del año 2007. Bajo este proyecto se logró una nueva definición para los estándares nacionales sobre conservación de mensajes digitales. Más aún se desarrolló, para la Secretaría de Economía, una aplicación computacional la cual será usada como patrón de comparación y evaluación de las futuras aplicaciones alrededor de la NOM-151. También se elaboró una serie de documentos los cuales serán una guía para los desarrolladores de estas futuras aplicaciones. La realización de este proyecto requirió la colaboración de personal altamente especializado el cual siempre estuvo bajo mi coordinación y dirección. La culminación de este proyecto ha dejado, además de una experiencia académica enriquecedora, beneficios económicos para la UNAM.
- Durante el mes de marzo de 2007, **se realizó trabajo de evaluación y de sitio para la Entidad Mexicana de Acreditación**, correspondientes a la solicitud de ampliación del Organismo de Certificación denominado Normalización y Certificación Electrónica, A.C. (NYCE), en la NOM-151-SCFI-2002 "Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos". La realización de esta evaluación trajo una aportación económica a la UNAM.
- En marzo de 2006, se entregó a la Secretaría de Economía una propuesta técnica y económica para la realización de un proyecto cuyo objetivo fue la **investigación y posterior desarrollo de una aplicación computacional que permitiera generar y verificar mensajes conservados según la NOM-151**.

Este trabajo de investigación y desarrollo consistió en determinar los mejores algoritmos criptográficos y de codificación para implementar una herramienta para la conservación de mensajes electrónicos. Finalmente durante el 2005 se formalizó el convenio de colaboración para el desarrollo del sistema que establece la norma oficial mexicana "NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos", que celebraron, por una parte la Universidad Nacional Autónoma de México a través de la Dirección General de Servicios de Cómputo Académico (DGSCA) y por otra parte, el ejecutivo federal a través de la Secretaría de Economía. Como resultado se obtuvo el Sistema de Conservación de Mensajes el cual es una sofisticada aplicación computacional (ideada y diseñada íntegramente en la UNAM) que ha servido de base para determinar la correcta observancia de las aplicaciones de los comerciantes que decidan apegarse a la NOM-151. Tal aplicación se entregó a la Secretaría de Economía junto con un buen número de documentos inherentes a dicho sistema (manual de usuario, manual de instalación, manual de referencia, diagramas UML, etc.). La realización de este proyecto requirió de la participación de un pequeño grupo de colaboradores los cuales fueron dirigidos por el Dr. Gerardo Vega. Es de mencionarse que la exitosa culminación de este proyecto trajo consigo una aportación económica para la UNAM.

- A través de un convenio de colaboración entre la UNAM y la Secretaría de Comercio, suscrito en 2004, se realizó la **revisión y análisis del documento "NOM-151-SCFI-2002 Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos"**. El objetivo de la colaboración fue la detección de errores y ambigüedades en dicho estándar. De igual forma, se sugirieron las correcciones pertinentes a tal documento. Se entregó a la Secretaría de Economía un reporte detallando los resultados de este trabajo de evaluación, el cual fue aceptado de conformidad por la Secretaría. La realización de este proyecto trajo una aportación económica a la UNAM.

- Con el apoyo económico del Consejo Nacional de Ciencias y Tecnología (CONACyT) y con la importante colaboración de un grupo de expertos en criptografía y en seguridad informática, los cuales estuvieron bajo la coordinación del Dr. Gerardo Vega, se realizó la **Evaluación de Componentes Criptográficos del Sistema Compranet**, durante el año de 2003 (9 meses). Este sistema electrónico fue desarrollado por la Secretaría de la Función Pública (ex Contraloría), con el fin de transparentar, agilizar y automatizar las licitaciones gubernamentales. Como resultado de esta asesoría, se entregó un grupo de recomendaciones (tres reportes) a la Secretaría de la Función Pública, las cuales permitirán mejorar la seguridad y equidad para todos los participantes en una licitación electrónica gubernamental. Cabe mencionar que un impulsor determinante para estos trabajos de evaluación fue el Banco Mundial, quien está estudiando la posibilidad de promover a Compranet como una importante opción para las licitaciones gubernamentales en otros países de Latinoamérica. La realización de este proyecto trajo una aportación económica a la UNAM.

- Arbitro para el "**7th World Multi-Conference on Systems, Cybernetics and Informatics, SCI 2003**", Orlando Florida, E.U.A.

- Colaboración con la Subprocuraduría Especial para el Caso Colosio, en el análisis de documentos cifrados (1998-1999). Cabe destacar que por esta colaboración la UNAM recibió una aportación económica.

3.4 Administración de proyectos PAPIIT-UNAM

- Se concluyó con éxito la coordinación y administración del proyecto PAPIIT IN109818 "**La riqueza algebraica de los códigos cíclicos y su uso en el cálculo de sus distribuciones de pesos**". Durante los tres años de vigencia (2018-2020) de tal proyecto se exploraron diversas líneas de investigación en Teoría de Códigos y Criptografía, las cuales se realizaron con la estrecha colaboración de mis estudiantes de posgrado (Maestría y Doctorado). Cinco de estas líneas de investigación se tradujeron en trabajos formales de investigación que a su vez se tradujeron en cinco publicaciones en publicaciones internacionales arbitradas. Más aún, tres de estos cinco trabajos de investigación fueron también presentados con éxito en congresos internacionales arbitrados, todos ellos especializados en el área de Teoría de Códigos y/o Criptografía. Cabe destacar que en uno de estos congresos internacionales se logro obtener, en colaboración con uno de mis estudiantes de maestría, el 2 lugar al mejor artículo presentado (de entre más de medio centenar (63) de artículos). El **19 de marzo del 2021** elaboré mi informe final sobre el proyecto PAPIIT IN109818, el cual coordiné y administré durante los años del 2018 al 2020. Como resultado de mi informe se calificó mi proyecto PAPIIT IN109818 como "***Muy bueno***".

- Se concluyó con éxito la coordinación y administración del proyecto PAPIIT IN107515 "**Estudio de la distribución de pesos para los códigos cíclicos reducibles e irreducibles**", el cual tuvo una vigencia de tres años (2015-2017). Como se puede leer en la notificación enviada por el PAPIIT como respuesta a mi informe final (**6 de marzo del 2018**), el Comité Evaluador del área de las Ciencias Físico Matemáticas y de las Ingenierías, tuvo a bien en calificar el desarrollo de mi proyecto como "***Muy bueno***". Considero que lo anterior fue así debido a que durante este proyecto se logró la publicación de 8 trabajos de investigación en revistas o series arbitradas de reconocido prestigio internacional. Cabe destacar que TODOS estos artículos fueron publicados con un agradecimiento explícito al proyecto PAPIIT-UNAM IN107515. Es de destacar que algunas de estas publicaciones han empezado a tener un impacto en el ámbito académico a nivel internacional. Por ejemplo, recientemente se publicó un artículo en la IEEE (Ziling Heng and Qin Yue, "**Several classes of cyclic codes with either optimal three weights or a few weights**", IEEE Transactions on Information Theory, vol. 62, no. 8, Aug 2016, pp 4501-4513) en el cual se puede leer textualmente al final del Abstract la frase "**In particular, we obtain a class of three-weight optimal cyclic codes achieving the Griesmer bound, which generalizes a Vega's result, and several classes of cyclic codes with a few weights, which solve an open problem proposed by Vega.**" Y bueno la razón de lo anterior se debe a que en el mencionado artículo se generalizó parcialmente una caracterización matemática que yo presenté en uno de mis más recientes trabajos (Gerardo Vega, "**A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field**", Finite Fields and Their Applications, Elsevier Science, Vol 42, Nov 2016, pp 23-38). De hecho este trabajo, a pesar de tener poco más de dos años de haber sido publicado, cuenta ya con por lo menos 3 Citas Tipo A (no auto citas).

- Se concluyó con éxito la coordinación y administración del proyecto PAPIIT IN105611 "**Estudio de códigos cíclicos en estructuras fuertes y débiles**", el cual tuvo una vigencia de dos años (2011-2012). Como se puede leer en la notificación enviada por el PAPIIT como respuesta a mi informe final (**23 mayo del 2013**), el Comité Evaluador del área de las Ciencias Físico Matemáticas y de las Ingenierías, determinó que el proyecto "***cumplió con los objetivos propuestos***".

3.5 Evaluación de proyectos para el CONAHCyT

- Evaluación del proyecto: "**Nuevos algoritmos y métodos de cifrado homomórfico post-cuántico para seguridad y privacidad de próxima generación en ciencia de datos**", correspondiente a la Convocatoria de Investigación en Fronteras de la Ciencia. El trabajo de evaluación se realizó en febrero de 2024.

- Evaluación del proyecto: "**Desarrollo de algoritmos de cifrado post-cuántico para el Internet de las Cosas**", correspondiente a la Convocatoria de Investigación en Fronteras de la Ciencia. El trabajo de evaluación se realizó en febrero de 2024.

- Evaluación del proyecto: "**PROTECCIÓN DE DATOS CLÍNICOS DE PACIENTES USANDO TÉCNICAS DE OCULTAMIENTO DE DATOS EN IMÁGENES MÉDICAS, INTELIGENCIA ARTIFICIAL Y PROCESAMIENTO DE IMÁGENES**", correspondiente a la Convocatoria de Investigación en Fronteras de la Ciencia. El trabajo de evaluación se realizó en febrero de 2024.

- Evaluación del proyecto: "**Desarrollo de nuevos algoritmos y arquitecturas de cómputo para criptograía ligera**", correspondiente a la Convocatoria de Investigación en el marco del proyecto CB-2016-281565. Se realizó la evaluación del candidato propuesto por el DR. MIGUEL MORALES SANDOVAL, para realizar una Estancia Posdoctoral en el contexto de dicho proyecto. El trabajo de evaluación se realizó el 12/09/2019.

- Evaluación del proyecto: "**NUEVOS ALGORITMOS CON COMPLEJIDAD (QUASI) POLINOMIAL PARA EL PROBLEMA DEL LOGARITMO DISCRETO**", correspondiente a la Convocatoria de Investigación en Fronteras de la Ciencia 2016-01. El trabajo de evaluación se realizó en mayo de 2017.

- Evaluación del proyecto: "**GESTION DE LA CONFIDENCIALIDAD DE DATOS EN REDES DE SENSORES A GRAN ESCALA**", correspondiente Fondo Institucional del CONACYT (FOINS). Agosto 2016.

- Evaluación del proyecto número 000000000254238 con título: "**PROPUESTA Y ESTUDIO TEORICO-EXPERIMENTAL DE UN PROTOCOLO PARA CRIPTOGRAFIA CUANTICA CON BASE EN LA TEORIA DE LA INFORMACION Y EL TEOREMA DE LA NO CLONACION UTILIZANDO EL LIMITE DE HELSTROM-HOLEVO-YUEN.**", correspondiente a la convocatoria de Investigación Científica Básica 2015. Septiembre 2015.
- Evaluación del proyecto: "**159803 Holistic Approach of Quantum Based Security (HoliQuantum)**". Junio de 2011.
- Evaluación del proyecto: "**Análisis y desarrollo de algoritmos y protocolos criptográficos basados en los atributos y su aplicación en la seguridad del expediente clínico electrónico de la norma oficial mexicana PROY-NOM-024-SSA3-2007**". Noviembre de 2011.
- Evaluación del proyecto: "**Detección de intrusos en redes ad hoc - aplicación de la teoría de la coordinación**", que fuera sometido al comité de Ingeniería Eléctrica, Ciencias de la Computación y Matemáticas Aplicadas a la Ingeniería, dentro de la convocatoria CONACYT 2005.
- Evaluación del proyecto: "**Combinación de Compresión y Criptografía de Datos: Estudio de Factibilidad**", que fuera sometido al comité de Ingeniería Eléctrica, Ciencias de la Computación y Matemáticas Aplicadas a la Ingeniería, dentro de la convocatoria CONACYT 2004.
- Se realizó, para el CONACYT, el trabajo de Evaluador para el proceso de selección de candidatos a cursar estudios de Posgrado en el extranjero en el marco de la **Convocatoria de Demanda libre 2004**. 30 de junio de 2004.
- Evaluación del proyecto: "**Development of Risk Assessment Models and Methods for Networked Information Systems**", que fuera sometido al comité de Ingeniería Eléctrica, Ciencias de la Computación y Matemáticas Aplicadas a la Ingeniería, dentro de la convocatoria CONACYT 2003.
- Evaluación del proyecto: "**Diseño y desarrollo de un sistema de seguridad computacional inspirado en un sistema inmunológico natural**", que fuera sometido al comité de Ingeniería Eléctrica, Ciencias de la Computación y Matemáticas Aplicadas a la Ingeniería, dentro de la convocatoria CONACYT 2001.
- Evaluación del proyecto: "**Cifrado y Descifrado de Información mediante el Uso de Sistemas Caoticos**", que fuera sometido al comité de Ingeniería Eléctrica, Ciencias de la Computación y Matemáticas Aplicadas a la Ingeniería, dentro de la convocatoria CONACYT 2001.

3.6 Evaluación de proyectos PAPIIT

- Evaluación del proyecto: "**Condiciones de Consistencia y Progreso en Sistemas Distribuidos**", correspondiente a la Convocatoria 2020 del Programa de Apoyo a Proyectos de Investigación e Innovación Tecnológica (PAPIIT) UNAM. El trabajo de evaluación se realizó el 22/08/2019.

3.7 Evaluación de proyectos para la UACM

- Evaluación del proyecto: "**On Lagrangian-Grassmannian variety and Plücker Matrices**", correspondiente a la Convocatoria Proyectos de Investigación del Colegio de Ciencia y Tecnología (CCyT)-2024 de la UACM. El trabajo de evaluación se realizó el 2/04/2024.

3.8 Colaboración con dependencias internas a la UNAM

- La DGIA-UNAM, con el desarrollo de un sistema automático de consulta para el banco de información de **ARIES**, tal sistema fue diseñado y es mantenido y administrado por el Mto. Vega desde 1995.
- Colaboración en con el Instituto de Investigaciones Biomédicas en el proyecto "**Búsqueda del gen responsable de la hiperalfalipoproteinemia que confiere un efecto protector contra el desarrollo de ateroesclerosis producido por hipercolesterolemia**".

- Colaboración con el Instituto de Investigaciones Filológicas en la edición del disco compacto "**La Babilonia de Hierro J.J. Tablada Crónicas Neoyorkinas**", septiembre de 1997.
- Colaboración en con el Instituto de Investigaciones Antropológicas en los proyectos "**Análisis espacial del uso de recursos naturales en túneles postteothihuacanos**" y "**Población prehispánica y recursos naturales después de la caída de Teotihuacan: análisis espacial de distribuciones arqueológicas**". Tales proyectos están bajo la responsabilidad de la Doctora Emily McClung Heumann, el primer proyecto cuenta con el apoyo del CONACyt (25074-H) y el segundo con el apoyo del PAPIIT (IN405997) de la Dirección General de Asuntos del Personal Académico de la UNAM.

3.9 Colaboración con investigadores de universidades extranjeras

- Con los recursos economicos del proyecto PAPIIT IN107515, se invito al Profesor Robert Henry Morelos-Zaragoza, del Department of Electrical Engineering, San Jose State University. El profesor Robert estuvo de visita en nuestra universidad durante la tercera semana de agosto del 2016. En el marco de su visita se organizó un simposio sobre codificación para los estudiantes de posgrado de la UNAM.
- Se consiguió el apoyo económico que permitió organizar la visita del profesor Jacques Wolfmann de la universidad francesa de Toulon-Var. Durante esta visita se pudo tener la oportunidad de intercambiar experiencias en el ámbito de la investigación en Teoría de Códigos, con este prestigiado investigador. Además el profesor Wolfmann impartió la conferencia "**A Cyclic Classification of Bent Functions**", dirigida en general a la comunidad académica de nuestra Universidad y en particular a los estudiantes del Posgrado en Ciencia e Ingeniería de la Computación de la UNAM. La conferencia se realizó el día lunes 10 de noviembre de 2008 a las 11:30 horas en el Auditorio del Instituto de Investigaciones en Matemáticas Aplicadas y Sistemas (IIMAS) de la UNAM.
- Gracias a apoyo económico de la DGSCA y del Posgrado del IIMAS de la UNAM, se invitó al profesor Jacques Wolfmann, de la Universidad de Toulon et du Var en Francia, a pasar una estancia de una semana durante el mes de noviembre de 2005. El Profesor J. Wolfmann presentó un mini curso introductorio sobre Codificación Algebraica ("Introduction to Algebraic Coding Theory"), así como también una conferencia sobre su línea de investigación actual ("**New results on 2-weight projective cyclic codes**"). Además se concluyó un artículo conjunto el cual se sometió para su publicación en una revista internacional (Designs, Codes and Cryptography).
- Gracias a apoyo económico de la UAM-I y de la DGSCA de la UNAM, se invitó al profesor Jacques Wolfmann, de la Universidad de Toulon et du Var en Francia, a pasar una estancia de una semana durante el mes de agosto de 2002. En esta ocasión, se tuvo la oportunidad de intercambiar experiencias con este prestigiado investigador. Como resultado de este acercamiento se logró una colaboración conjunta para la presentación de un trabajo en un congreso internacional (Seventh International Conference on Finite Fields and Applications), además se concluyó un artículo conjunto el cual se sometió para su publicación en una revista internacional (Finite Fields and Their Applications).
- Se invitó a la DGSCA al profesor Claude Carlet, de la Universidad de Caen en Francia, durante el intervalo del 10 al 17 de abril del 2000. Durante esta visita se pudo tener la oportunidad de intercambiar experiencias con este prestigiado investigador. Además, se organizaron dos pláticas sobre Teoría de Códigos y Criptografía, las cuales estuvieron a cargo del profesor Carlet.

3.10 Trabajos de investigación en congresos internacionales

- Gerardo Vega, "**Explicit factorization of some period polynomials**", International Workshop on the Arithmetic of Finite Fields (WAIFI 2020), Rennes, France. July 6-8, 2020.
- Daniel Becerra & Gerardo Vega, "**Secret Sharing Scheme with Efficient Cheating Detection**", in "2nd International Conference on Networking, Information Systems & Security (NISS2019)", que tuvo lugar en la Faculty of Sciences de la Universidad Mohammed V, de la ciudad de Rabat en Marruecos, durante los días del 27 al 29 de marzo del 2019. Cabe destacar que este artículo obtuvo el 2 lugar al mejor artículo presentado al mencionado congreso internacional arbitrado, en el cual se presentaron más de medio centenar (63) de artículos.

- Jesús E. Cuén-Ramos & Gerardo Vega, "**The weight distribution of families of reducible cyclic codes through the weight distribution of some irreducible cyclic codes**", in "Latin American Week on Coding and Information (LAWCI 2018), UNICAMP-CAMPINAS, BRAZIL, 2018, july 22-27".
- Gerardo Vega, Jesús E. Cuén-Ramos, "**The weight distribution for an extended family of reducible cyclic codes**", in "Second International Conference in Codes, Cryptology and Information Security, C2SI 2017, Rabat, Morocco, April 10-12, 2017", Lecture Notes in Computer Science, Springer Verlag, vol. 10194, pp. 213-229, April 10-12, 2017. ISSN: 0302-9743.
- Gerardo Vega, "**A Family of Six-Weight Reducible Cyclic Codes and their Weight Distribution**", First International Conference in Codes, Cryptology and Information Security, C2SI 2015, Rabat, Morocco. May 26-28, 2015.
- Jesús Carrillo-Pacheco, Gerardo Vega & Felipe Zaldívar, "**The Weight Distribution of a Family of Lagrangian-Grassmannian Codes**", First International Conference in Codes, Cryptology and Information Security, C2SI 2015, Rabat, Morocco. May 26-28, 2015.
- Gerardo Vega & Carlos A. Vázquez, "**The Weight Distribution of a Family of Reducible Cyclic Codes**", International Workshop on the Arithmetic of Finite Fields (WAIFI 2012), Bochum, Germany. July 16-19, 2012.
- Gerardo Vega, "**On the Number of Two-weight Cyclic Codes with Composite Parity-check Polynomials**", in "**Proceedings of International Workshop on the Arithmetic of Finite Fields WAIFI 2008 (Joachim von zur Gathen (Eds.))**", Lecture Notes in Computer Science, Springer Verlag, vol. 5130, pp. 144-156, 2008. Siena, Italy July 6-9, 2008.
- Gerardo Vega, "**Determining the Number of One-weight Cyclic Codes when Length and Dimension are Given**", in "**Proceedings of International Workshop on the Arithmetic of Finite Fields WAIFI 2007 (C. Carlet and B. Sunar (Eds.))**", Lecture Notes in Computer Science, Springer Verlag, vol. 4547, pp. 284-293, 2007. Madrid, Spain, June 21-22, 2007.
- Jacques Wolfmann & Gerardo Vega, "**Some Classes of Cyclic Codes over Z_4**", in "**Seventh International Conference on Finite Fields (Fq7)**", Toulouse France. Mayo de 2003.
- Horacio Tapia & Gerardo Vega, "**On Z_{2^k}-Linear and Quaternary Codes**", in "**Sixth International Conference on Finite Fields (Fq6)**", Cd. de Oaxaca, México. Mayo de 2002.
- Horacio Tapia & Gerardo Vega, "**A Generalization of Negacyclic Codes**", in "**International Workshop on Coding and Cryptography (WCC-2001)**", París Francia. Enero de 2001.
- Horacio Tapia & Gerardo Vega & Noé Gutiérrez, "**A Parseval type of relation on Z_n**", in "**Proceedings of the World Multiconference on Systemics, Cybernetics and Informatics (2000)**", Estados Unidos. Julio 23 a 26 de 2000.
- H. Tapia-Recillas, G. Vega and E. Daltabuit, "**Some Results on Regular Mappings**", in "**Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC-12)**", Lecture Notes in Computer Science 1255, Springer Verlag, 1997, pp. 321-328. Toulouse, France, June 23-27, 1997.
- Leobardo Hernández & Gerardo Vega, "**Protocolo para autenticación, intercambio de llaves e información seguras en comunicaciones remotas**", in "**International Conference CIMAF'97**", Ciudad de la Habana, Cuba. Marzo de 1997.

3.11 Reconocimientos o premios

- Daniel Becerra & Gerardo Vega, ganadores del 2 lugar al mejor artículo presentado en el "**2nd International Conference on Networking, Information Systems & Security (NISS2019)**", que tuvo lugar en la Faculty of Sciences de la Universidad Mohammed V, de la ciudad de Rabat en Marruecos, durante los días del 27 al 29 de marzo del 2019, presentando el trabajo "**Secret Sharing Scheme with Efficient Cheating Detection**".

- Ganador conjuntamente con varios investigadores del 1er. Lugar del "**Premio Lilly de Investigación en Diabetes Mellitus**", otorgado por Eli Lilly y Compañía de México, S.A. de C.V. en noviembre de 1996.
- Reconocimiento por facilitar una implementación de un algoritmo rápido para el cálculo de la trasformada de Fourier discreta. Reconocimiento entregado por el Dr. Gianfranco Bisiacchi, Director del Programa Universitario de Investigación y Desarrollo Espacial, enero de 1994.
- Mención Honorífica a la mejor tesis de Licenciatura en Matemáticas en 1990. Otorgada por la Sociedad Matemática Mexicana en Noviembre de 1991.

3.12 Artículos arbitrados para revistas internacionales

- Arbitraje del artículo: "**One-Sided Repeated-Root Two-Dimensional Cyclic and Constacyclic Codes**", para la revista Applicable Algebra in Engineering, Communication and Computing (Springer). Junio de 2022.
- Arbitraje del artículo: "**The linearity of Carlet's Gray image of linear codes over $\mathbb{Z}_8$**" (3era. versión corregida), para la revista Designs, Codes and Cryptography (Springer). Mayo de 2022.
- Arbitraje del artículo: "**The linearity of Carlet's Gray image of linear codes over $\mathbb{Z}_8$**" (2da. versión corregida), para la revista Designs, Codes and Cryptography (Springer). Marzo de 2022.
- Arbitraje del artículo: "**New good quasi-cyclic codes and codes with improved minimum distance**", para la revista Journal of Algebra Combinatorics Discrete Structures and Applications (Jacodesmath Institute). Enero de 2022.
- Arbitraje del artículo: "**Weight distributions of all $3p^k$-dimensional irreducible cyclic codes of length p^m**" (este artículo fue rechazado por mi con anterioridad), para la revista Applicable Algebra in Engineering, Communication and Computing (Springer). Diciembre de 2021.
- Arbitraje del artículo: "**Weight distributions of all $3p^k$-dimensional irreducible cyclic codes of length p^m**", para la revista Journal of Applied Mathematics and Computing (Springer). Noviembre de 2021.
- Arbitraje del artículo: "**Weight enumerator polynomials of $3p^d$-dimensional irreducible cyclic codes of length p^m**", para la revista Journal of Applied Mathematics and Computing (Springer). Octubre de 2021.
- Arbitraje del artículo: "**The linearity of Carlet's Gray image of linear codes over $\mathbb{Z}_8$**" (1era. versión corregida), para la revista Designs, Codes and Cryptography (Springer). Octubre de 2021.
- Arbitraje del artículo: "**REMARK ON A FAMILY OF CODES OVER $\mathbb{Z}_4$**", para la revista Designs, Codes and Cryptography (Springer). Septiembre de 2021.
- Arbitraje del artículo: "**Weight distributions of some irreducible cyclic codes of length p^m; p odd prime**" (este artículo fue rechazado por mi con anterioridad), para la revista Advances in Mathematics of Communications (American Institute of Mathematical Sciences). Septiembre de 2021.
- Arbitraje del artículo: "**The linearity of Carlet's Gray image of a cyclic code of odd length over $\mathbb{Z}_8$**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). Agosto de 2021.
- Arbitraje del artículo: "**Weight distribution of some irreducible cyclic codes and their duals**" (este artículo fue rechazado por mi con anterioridad), para la revista Designs, Codes and Cryptography (Springer). Julio de 2021.
- Arbitraje del artículo: "**Weight distributions of some irreducible cyclic codes of length n**", para la revista Designs, Codes and Cryptography (Springer). Mayo de 2021.

- Arbitraje del artículo: "**The linearity of the Gray image of a $\mathbb{Z}_8$-additive code using its generator matrix**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). Abril de 2021.
- Arbitraje del artículo: "**Weight distribution of some irreducible cyclic codes and their duals**", para la revista Finite Fields and their Applications (Elsevier). Marzo de 2021.
- Arbitraje del artículo: "**Generalized Hamming weights of codes derived from the incidence matrices of some graphs**", para la revista Pacific Journal of Mathematics (Mathematical Sciences Publishers). Enero de 2021.
- Arbitraje del artículo: "**Weight distributions of some irreducible cyclic codes of length p^m; p odd prime**", para la revista Advances in Mathematics of Communications (American Institute of Mathematical Sciences). Octubre de 2020.
- Arbitraje del artículo: "**Weight distributions of six families of 3-weight binary linear codes**", para la revista Discrete Mathematics (Elsevier). Mayo de 2020.
- Arbitraje del artículo: "**Three-weight codes from semiprimitive irreducible cyclic codes**", para la revista Discrete Mathematics (Elsevier). Septiembre de 2019.
- Arbitraje del artículo: "**The weight distribution of a class of p-ary cyclic codes with few weights**", para la revista Discrete Mathematics (Elsevier). Octubre de 2018.
- Arbitraje del artículo: "**A class of three-weight cyclic codes and their duals**", para la revista Finite Fields and their Applications (Elsevier). Diciembre de 2018.
- Arbitraje del artículo: "**New Classes of p-ary Few Weights Codes**", para la revista Cryptography and Communications (Springer). Marzo de 2017.
- Arbitraje del artículo: "**The Weight Enumerator of a Class of Reducible Cyclic Codes**", para la revista Applicable Algebra in Engineering, Communication and Computing (Springer). Mayo de 2017.
- Arbitraje del artículo: "**Several Classes of Trace Codes With Either Optimal Two Weights or a Few Weights over $F_q + uF_q$**", para la revista Finite Fields and their Applications (Elsevier). Julio de 2017.
- Arbitraje del artículo: "**Two-weight codes and second order recurrences**", para la revista IEEE Communications Letters (IEEE Information Theory Society). Octubre de 2017. Se incluye reporte.
- Arbitraje del artículo: "**On Generalized MacDonald Codes**", para la revista IEEE Involve, a Journal of Mathematics (IEEE Information Theory Society). Diciembre de 2017.
- Arbitraje del artículo: "**Pisano period codes**", para la revista Finite Fields and their Applications (Elsevier). Diciembre de 2017.
- Arbitraje del artículo: "**Some results on two-weight and three-weight linear codes**", para la revista Finite Fields and Their Applications (Elsevier). Febrero de 2016.
- Arbitraje del artículo: "**Three-Weight Cyclic Codes and Their Weight Distributions**", para la revista Discrete Mathematics (Elsevier). Primera versión 2014. Versión corregida y aumentada. Agosto de 2015.
- Arbitraje del artículo: "**Weight Distribution of a class of Reducible Cyclic Codes**", para la revista Finite Fields and Their Applications (Elsevier). Agosto de 2015.
- Arbitraje del artículo: "**A Class of p-ary Cyclic Codes and Their Weight Enumerators**", para la revista Advances in Mathematics of Communications (American Institute of Mathematical Sciences). Mayo de 2015.
- Arbitraje del artículo: "**Several classes of optimal cyclic codes with Melas code type**", para la revista Designs, Codes and Cryptography (Springer). Febrero de 2015.

- Arbitraje del artículo: "**Weight distributions of a class of cyclic codes from F_l-conjugates**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). Agosto de 2014.
- Arbitraje del artículo: "**Three-Weight Cyclic Codes and Their Weight Distributions**", para la revista Discrete Mathematics (Elsevier). Octubre de 2014.
- Arbitraje del artículo: "**The minimum Hamming distances of irreducible cyclic codes**", para la revista Finite Fields and Their Applications (Elsevier). Abril de 2014.
- Arbitraje del artículo: "**Irreducible cyclic codes of length 2^n over finite fields and their weight distribution**", para la revista Finite Fields and Their Applications (Elsevier). Junio de 2014.
- Arbitraje del artículo: "**Two-weight and three-weight cyclic codes**", para la revista Designs, Codes and Cryptography (Springer). Diciembre de 2013.
- Arbitraje del artículo: "**Five Families of Three-Weight Ternary Cyclic Codes and Their Duals**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). agosto de 2013.
- Arbitraje del artículo: "**Weight Distribution of a Class of Cyclic Codes with Arbitrary Number of Zeros**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). mayo de 2013.
- Arbitraje del artículo: "**$(t+p)$-constacyclic codes over Z_{p^m}**", para la revista Discrete Mathematics (Elsevier). Enero de 2012.
- Arbitraje del artículo: "**Cyclic Codes from the Two-Prime Sequences**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). Febrero de 2012.
- Arbitraje del artículo: "**The weight distributions of irreducible cyclic codes**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). Junio de 2012.
- Arbitraje del artículo: "**A characterization of two-weight projective cyclic codes**", para la revista IEEE Transactions on Information Theory (IEEE Information Theory Society). Septiembre de 2012.
- Arbitrage del articulo: "**One-Lee weight codes and two-Lee weight projective codes over Z_4**", para la revista Applicable Algebra in Engineering, Communication and Computing (Springer). Junio de 2011.
- Arbitrage del articulo: "**Some constacyclic self-dual codes over the integers modulo 2^m**", para la revista Finite Fields and their Applications (Elsevier). Agosto de 2011.
- Arbitrage del articulo: "**New families of two-weight cyclic projective codes constructed as a direct product of two one-weight irreducible cyclic codes**", para la revista Designs, Codes and Cryptography (Springer). Marzo de 2010.
- Revisión del articulo: "**The parity of the number of irreducible factors of polynomial $x^{l-ef}(x^f+1)^e+1$ over F_2**", la revista Finite Fields and their Applications (Elsevier). Marzo de 2010.
- Arbitraje del artículo: "**A Generalized Counting and Factoring Technique for Polynomials over Finite Fields**", para la revista Discrete Mathematics (Elsevier). Enero de 2009.
- Revisión del artículo: "**One and two-Lee weight codes over Z_4**", la revista Discrete Mathematics (Elsevier). Octubre de 2009.
- Arbitraje del artículo: "**The parity of the number of irreducible factors of $x^{l-ef}(x^f+1)^e+1$ over F_2 from $\sigma-$LFSR**", para Finite Fields and Their Applications (Elsevier). Agosto de 2007.
- Revisión del artículo: "**Enumeration results on the joint linear complexity of multisequences**", para la Mathematical Reviews de la American Mathematical Society (AMS). Marzo de 2007.

- Arbitraje de 6 artículos para el congreso: International Workshop on Coding and Cryptography, WCC 2001, París, Francia. Del 8 al 12 de enero del 2001.
- Arbitraje del artículo: "**Quantum Cryptoanalysis of Elliptic Curve Systems**", para la revista: Computación y Sistemas (IPN). Septiembre del 2000.
- Arbitraje del artículo: "**Modelo de comportamiento de las bibliotecas públicas cubanas**", para la revista: Revista Internacional del Centro Universitario de Investigaciones bibliotecológicas UNAM. Marzo de 1995.

4 Labores de difusión

4.1 Organización de congresos y coloquios

- Co-organizador del Simposio sobre teoría de la codificación para el control de errores, algoritmos y arquitecturas. Auditorio del IIMAS, Ciudad Universitaria, 17 de agosto de 2016.
- Se consiguió el apoyo económico que permitió organizar la visita del profesor Jacques Wolfmann de la universidad francesa de Toulon-Var. Durante esta visita se pudo tener la oportunidad de intercambiar experiencias en el ámbito de la investigación en Teoría de Códigos, con este prestigiado investigador. Además el profesor Wolfmann impartió la conferencia "**A Cyclic Classification of Bent Functions**", dirigida en general a la comunidad académica de nuestra Universidad y en particular a los estudiantes del Posgrado en Ciencia e Ingeniería de la Computación de la UNAM. La conferencia se realizó el día lunes 10 de noviembre de 2008 a las 11:30 horas en el Auditorio del Instituto de Investigaciones en Matemáticas Aplicadas y Sistemas (IIMAS) de la UNAM.
- Participación como parte del comité organizador del "**Primer, Segundo, Tercer, Cuarto y Quinto Coloquio Nacional de Teoría de Códigos, Criptografía y áreas Relacionadas**" Realizándose el primero en las instalaciones del Departamento de Matemáticas de la Universidad Autónoma Metropolitana Unidad Iztapalapa, en mayo de 1997. El segundo, en la Dirección General de Servicios de Cómputo Académico de la UNAM, en junio de 1998. El tercero en la Casa de la primera imprenta de América, en julio del 1999. El cuarto y quinto en el Palacio de Minería de la UNAM, en junio del 2000 y julio del 2002 respectivamente.
- Organizador de la Sesión de Seguridad en Cómputo del Congreso Virtual Cómputo 2000, que tuvo lugar en las instalaciones de la DGSCA-UNAM, del 16 al 20 de octubre del 2000.

4.2 Pláticas de divulgación en universidades

- Gerardo Vega, "**Aplicaciones de la Firma Digital**". Universidad de la Ciudad de México. Septiembre 2006.
- Gerardo Vega, "**Introducción a la Criptografía**". Depto. De Seguridad en Cómputo, DGSCA-UNAM. Mayo y Junio de 2004.
- Gerardo Vega, "**Introducción a la Teoría de Códigos**". Universidad Juárez del Estado de Durango. Abril 2004.
- Gerardo Vega, "**Algunas clases de códigos cíclicos sobre** Z_4". Universidad Autónoma de Yucatán. Septiembre 2003.
- Gerardo Vega, "**Curso sobre Funciones Booleanas**". Universidad Autónoma de Yucatán. Septiembre 2003.
- Gerardo Vega, "**Pláticas de divulgación sobre Criptografía para el Instituto Tecnológico de Oaxaca**". Instituto Tecnológico de Oaxaca. Mayo 2002.
- Gerardo Vega, "**Aspectos generales sobre seguridad en informática y el proyecto de correo SEguro en la UNAM (SEUNAM)**". Sede del Servicio de Administración Tributaria de la Secretaria de Hacienda y Crédito Publico. Noviembre 2001.

- Gerardo Vega, "**Teoría de Códigos. Septiembre 2003**". Instituto Tecnológico de Oaxaca. Mayo 2001.
- Gerardo Vega, "**Los principales sistemas de cifrado simétrico en la actualidad**". Sede del programa de Maestría en Ciencias con Opción en Computación del Departamento de Ingeniería Eléctrica del CINVESTAV-IPN. Septiembre 1999.
- Gerardo Vega, "**El Algoritmo DES**". ENEP Aragón - UNAM. Mayo de 1997.
- Gerardo Vega, "**Introducción a los Códigos Lineales**". Universidad Autónoma de San Luis Potosí. Abril de 1997.
- Gerardo Vega, "**Aritmética Modular**". ENEP Aragón - UNAM. Marzo de 1997.
- Gerardo Vega, "**Seguridad en Computo Y Criptografía**". Facultad de Contaduría y Administración - UNAM. Febrero de 1997.

4.3 Participación como invitado a congresos, talleres o seminarios

- Gerardo Vega, "**Esquemas de codificación para la protección de la información**", Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. 19 de Noviembre de 2021.
- Gerardo Vega, "**Esquemas de codificación para la protección de la información**", Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. 30 de octubre de 2020.
- Gerardo Vega, "**Redes y Seguridad en Cómputo**", Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. 4 de octubre de 2019.
- Gerardo Vega, "**Experiencias de los Representantes Académicos del COLACAD**", Colegio de Académicos de la DGTIC. Primero de marzo de 2018.
- Gerardo Vega, "**Redes y Seguridad en Cómputo**", Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. 16 de noviembre de 2018.
- Gerardo Vega, "**Seminario de Orientación 2018-1**", Posgrado de Ciencia e Ingeniería de la Computación de la UNAM. 24 de noviembre de 2017.
- Gerardo Vega, "**Los campos finitos en la teoría de códigos correctores**", Simposio sobre teoría de la codificación para el control de errores, algoritmos y arquitecturas. Auditorio del IIMAS, Ciudad Universitaria, 17 de agosto de 2016.
- Gerardo Vega, "**La criptografía Moderna Comersial**", Seminario semanal del laboratorio de cómputo científico. Organizado por el Departamento de Matemáticas de la H. Facultad de Ciencias de la UNAM. 27 Agosto de 2015.
- Gerardo Vega, "**Teoría de Códigos y Criptografía**", Taller de Investigación; Ingeniería de Sistemas y Redes Computacionales. Organizado por el Posgrado de Ciencias e Ingeniería de UNAM. Noviembre de 2014.
- Gerardo Vega, "**Teoría de Códigos y Criptografía**", Taller de Investigación; Ingeniería de Sistemas y Redes Computacionales. Organizado por el Posgrado de Ciencias e Ingeniería de UNAM. Noviembre de 2013.
- Gerardo Vega, "**Teoría de Códigos y Criptografía**", Taller de Investigación; Ingeniería de Sistemas y Redes Computacionales. Organizado por el Posgrado de Ciencias e Ingeniería de UNAM. Diciembre de 2012.
- Gerardo Vega, "**Las matemáticas en las firmas digitales**", "Curso Matemáticas... un viaje al infinito", Dirección General de Divulgación de la Ciencia de la UNAM, Casita de las Ciencias de Universum, Zona Cultural de Ciudad Universitaria. 29 de noviembre del 2008.

- Gerardo Vega, "**Algunas Clases de Códigos Ciclícos sobre** Z_4", Platicas de Investigación y Dibulgación para la Facultad de Matemáticas de la Universidad Autonoma de Yucatán. 11 al 15 de Julio del 2005.
- Gerardo Vega, "**Aritmética Modular**", Seminario para alumnos de Ingenieria en Computación de la ENEP Aragón, UNAM, 2 de septiembre del 2003.
- Gerardo Vega, "**El algoritmo DES**", Seminario para alumnos de Ingenieria en Computación de la ENEP Aragón, UNAM, 5 de agosto del 2003.
- Gerardo Vega, "**Aspectos generales sobre seguridad en informática**", Sede del Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público (SAT-SHCP). 15 de mayo del 2003.
- Gerardo Vega, "**Los principales sistemas de cifrado en la actualidad**", Seminario códigos y criptografía del programa de maestría en ciencias del depto. de Ingeniería Electrica del CINVESTAV IPN, 5 de junio del 2002.
- Gerardo Vega, "**Los principales sistemas de cifrado en la actualidad**", Platicas sobre criptografía organizadas por la Facultad de Contaduría de la UNAM, 2 de sepiembre del 1998.

4.4 Participación en congresos, talleres y seminarios nacionales

- Daniel Becerra & Gerardo Vega, "**Esquema de compartición de secretos con detección eficiente de trampas**", 13o Coloquio Nacional Teoría de Códigos, Criptografía y áreas Relacionadas, Palacio de Minería de la UNAM. Del 24 al 26 de abril de 2019.
- José Luis Juan Herrera García & Gerardo Vega, "**Sumando en Cifrado Homomórfico sin Arranque**", 12o Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas. Casa de la Primera Imprenta en América, Ciudad de México. Universidad Autónoma Metropolitana, 27 de junio de 2017.
- Cuen Ramos Jesus & Gerardo Vega, "**Una Familia de Códigos Cíclicos Reducibles de Seis Pesos y su Distribución Pesos**", XI Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas. Facultad de Ciencias Físico Matemáticas, de la Benemérita Universidad Autónoma de Puebla, del 16 al 19 de junio de 2015.
- Carlos A. Fernández & Gerardo Vega, "**Códigos constancíclicos sobre** Z_{p^m}", Noveno Coloquio Nacional de Teoría de Códigos, Criptografia y Áreas Relacionadas. Centro Histórico, Ciudad de México, Septiembre 28, 29 y 30 de 2011.
- Gerardo Vega, "**Firma Digital**". XVIII Escuela de Análisis Numérico y Optimización, Universidad Autónoma de Coahuila, México. Abril de 2008.
- Gerardo Vega, "**Los sistemas modernos de cifrado de datos**". XVII Escuela de Análisis Numérico y Optimización, Universidad Juárez del Estado de Durango, México. mayo de 2007.
- Gerardo Vega, "**Introducción a la Teoría de Códigos**". XIV Escuela de Análisis Numérico y Optimización, Universidad Juárez del Estado de Durango, México. Enero de 2004.
- Gerardo Vega, "**Teoría de Códigos y Criptografía**". Talleres y Escuelas de Computación, Posgrado de Ciencias e Ingeniería de UNAM, Ciudad Universitaria, México D.F. Diciembre 2004.
- Moisés Bautista & Gerardo Vega, "**Implementación de un criptosistema basado en curvas elípticas**". Quinto Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas, Cd. de México. Junio de 2002.
- Gerardo Vega, "**El sistema de cifrado DES y los mapeos regulares**". Jornadas del Doctorado en Ciencias de la UAM-I, México D.F. Mayo 2001.
- Participación en el Primer Taller Internacional de Criptografía, celebrado del 8 al 12 de mayo del 2000, en el Instituto Tecnológico de la Costa Grande en la Cd. Zihuatanejo, Gro., México. Cabe destacar que este primer taller estuvo a cargo del profesor Neal Koblitz de la Universidad de Washington, E.U.A.

- Gerardo Vega, "**Una Generalización de los Códigos Negacíclicos**". Congreso de Seguridad en Cómputo 2000, Palacio de Minería, Ciudad de México. Noviembre de 2000.
- Gerardo Vega & Horacio Tapia, "**Un método de factorización de funciones Booleanas de grado mayor o igual a 4 a funciones de grado 3**". XXXIII Congreso Nacional de Matemáticas, Cd. de Saltillo, Coahuila, México. Octubre de 2000.
- Gerardo Vega, "**Introducción a la Teoría de Códigos**". Cuarto Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas, Palacio de Minería, Centro Histórico de la Ciudad de México. Junio de 2000.
- Gerardo Vega, "**El DES y la Criptografía simétrica**". Seminario de Criptografía del Dpto. de Matemáticas de la UAM-I. Abril 2000.
- Gerardo Vega, "**Los principales sistemas de cifrado simétrico en la actualidad**". Congreso General de Cómputo "cómputo.99mx", Palacio de Minería, Centro Histórico de la Ciudad de México. Octubre de 1999.
- Gerardo Vega, "**Un método de factorización de funciones booleanas de grado mayor o igual a 4 a funciones de grado 3**". Tercer Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas, Casa de la primera imprenta en América, Ciudad de México. Julio de 1999.
- Gerardo Vega, "**Los principales sistemas criptográficos de clave privada y sus características**". Ciclo Criptografía'99, organizado por la UAM-I, SECOFI Y SEGURIDATA, Aditorio del edificio principal de la Secretaría de Comercio y Fomento Industrial, Ciudad de México. Junio de 1999.
- Gerardo Vega, "**Una caracterización de los mapeos regulares**". Seminario de Computación 1999, Auditorio de Videoconferencias de la DGSCA-UNAM, Ciudad de México. mayo de 1999.
- Gerardo Vega, "**El Sistema de llave secreta DES**". Pláticas de Seguridad en Cómputo, ENEP, ARAGON-UNAM, México D.F. Febrero de 1999.
- Gerardo Vega, "**Una Caracterización de los Mapeos Regulares**". Segundo Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas, DGSCA-UNAM, México D.F. Junio de 1998.
- Gerardo Vega, "**Un sistema de cifrado de datos basado en polinomios sobre campos finitos**". Primer Coloquio Nacional de Códigos, Criptografía y áreas Relacionadas, Universidad Autónoma Metropolitana-Izt, México D.F. Mayo de 1997.
- Gerardo Vega, "**Los sistemas Modernos de cifrado de Datos**". VII Escuela de Análisis Numérico y Optimización, Ciudad de Aguascalientes, Ags., México. Marzo de 1997.
- Gerardo Vega, "**Códigos y Criptografía**". VII Semana de las Matemáticas, Universidad Autónoma Metropolitana-Izt., Noviembre de 1997.
- Horacio Tapia & Gerardo Vega, "**A Characterization of Regular Mappings**". "Aspectos Combinatorios y Computacionales de Optimización, Topología y Algebra" ACCOTA'96, Ciudad de Taxco Gro., México. Noviembre de 1996.
- Gerardo Vega, "**Taller de Criptografía**". VI Semana de las Matemáticas, Universidad Autónoma Metropolitana-Izt. Noviembre de 1996.
- Gerardo Vega & Horacio Tapia, "**Criptoanálisis diferencial y lineal en el DES**". XXIX Congreso Nacional de Matemáticas, Ciudad de San Luis Potosí, San Luis Potosí, México. Octubre de 1996.
- Antonio Velázquez, Alejandro García Carrancá & Gerardo Vega, "**El proyecto de Genoma Humano en México**". Coloquios de Investigación, Museo Universum UNAM, México D.F. Mayo de 1996.
- Luis Javier Alvarez & Gerardo Vega, "**Análisis de la Efemérides del Volcán de Colima (1906) arreglada por el Presbítero Severo Díaz**". V Reunión Internacional: Volcán de Colima, Universidad de Colima, México. Enero de 1996.

- Gerardo Vega, "**Programa DGSCA para la captura en CD'Room de crónicas de José Juan Tablada**". Jornadas Filológicas, Instituto de Investigaciones Filológicas UNAM. Noviembre de 1995.
- Gerardo Vega, "**Sofía, un sistema de recuperación de información por indexación de triadas**". Jornadas Filológicas, Instituto de Investigaciones Filológicas UNAM. Julio de 1995.
- Gerardo Vega, "**Los sistemas de recuperación de información por indexación de triadas**". Serie de platicas organizadas por el Centro Universitario de Investigaciones Bibliotecológicas de la UNAM. Noviembre de 1994.
- Gerardo Vega, "**Algoritmos para la FFT**". III Escuela de Análisis Numérico y Optimización, Saltillo, Coah. México. Noviembre de 1993.
- Gerardo Vega & Max A. García, "**Un sistema para aprender a orientarse en la ciudad**". Congreso Nacional sobre Informática. 25 Octubre de 1991.
- Javier Aurrecoechea & Gerardo Vega, "**Una implementación del algoritmo de Good para el cálculo de la TFD**". XXIII Congreso Nacional de Matemáticas, Ciudad de Guanajuato, Gto. México. Noviembre de 1990.

4.5 Entrevistas a medios de difusión académica

- Entrevista concedida a la Gaceta UNAM, en el marco del Cuarto Coloquio Nacional de Teoría de Códigos, Criptografía y áreas Relacionadas. Dicha entrevista fue publicada en el número 3,376 del 19 de junio del 2000.
- Entrevista concedida al diario REFORMA, en el marco del Quinto Coloquio Nacional de Teoría de Códigos, Criptografía y áreas Relacionadas. Dicha entrevista fue publicada el 18 de julio del 2002.
- Entrevista concedida al diario MILENIO, el tema fundamental de esta entrevista fue los aspectos generales de la seguridad informática, sobre todo aquellos relacionados con la transmisión y/o almacenamiento de información electrónica. Dicha entrevista fue publicada el 9 de agosto del 2002.
- Entrevista concedida a la revista Seguridad y Justicia el tema fundamental de esta entrevista fue los aspectos generales de la seguridad informática, sobre todo aquellos relacionados con la transmisión y/o almacenamiento de información electrónica. Dicha entrevista fue publicada en el núm. 5 (año 2), septiembre del 2002.

5 Participación institucional

5.1 Participación en cuerpos académicos colegiados

- Del 18 de noviembre del 2015 al 17 de noviembre del 2021 (**6 años**) se participó como miembro de la **Comisión Dictaminadora** de la **Dirección General de Cómputo y de Tecnologías de Información y Comunicación** de la UNAM. Durante esos 6 años se participó puntualmente, sin excepción, en todas las reuniones y en todas las tareas que dicha comisión realizó o me asignó.

5.2 Participación en Comisiones Evaluadoras

- Participación como **Jurado Calificador** para el Premio MIXBAAL a la Mejor Tesis de Matemáticas Aplicadas. Premio otorgado por la Escuela Nacional de Análisis Numérico y Optimización (Facultad de Ciencias UNAM). Durante los años 2011, 2012, 2013 y 2014.
- Participación como **Par Académico** en el proceso de evaluación de los programas de posgrado presentados en el marco de la Convocatoria extraordinaria 2012 del Programa Nacional de Posgrado de Calidad (PNPC) de la Dirección Adjunta de Posgrados y Becas del CONACyT. 30 de enero de 2013.
- Se realizó, para el CONACYT, el trabajo de **Evaluador** para el proceso de selección de candidatos a cursar estudios de Posgrado en el marco de la Convocatoria de Demanda libre 2004.