DR. VÍCTOR MANUEL SILVA GARCÍA

FORMACIÓN ACADÉMICA

- Sistema Nacional de Investigadores Nivel I, Enero-2011 a Diciembre-2013
  Mención Honorífica.

- Doctor en Ciencias de la Computación.
  CIC - IPN.

- Maestría en Estadística
  Colegio de Postgraduados, Universidad Autónoma de Chapingo.

- Licenciatura en Físico y Matemática
  ESFM – IPN.

Distinciones

- Primer lugar en el Certamen: "Premio de Ingeniería de la Cuidad de México 2011", en la categoría "Profesionales de la Ingeniería en Sistemas Computacionales"

- Mención Honorífica del Doctorado en Ciencias de la Computación
  Abril – 2007.

- Presidente Ejecutivo
  9°, "Simposium Internacional "Aportaciones de las Universidades a la Docencia, la Investigación, la Tecnología y el Desarrollo Sept-2007 a 2011.

- Presea "Juan de Dios Bátiz"
  30 años de servicio en el IPN – 2003.

EXPERIENCIA LABORAL:

- Director del Centro de Innovación y Desarrollo Tecnológico en Cómputo.
  Junio de 2005 a la fecha.

- Subdirector de Apoyo y Transferencia de Tecnología del CIDETEC.
  Julio de 2003 a mayo de 2005.

- Asesor de la Dirección de la Escuela Superior de Cómputo del IPN.
  Febrero a Marzo del 2001.

- Coordinador General del Programa de Estímulo al Desempeño Docente y COTEPABE-IPN.
  Julio de 1997 a enero del 2001.

- Coordinador General del Programa de Estímulo al Desempeño Docente-IPN.
  Abril de 1994 a junio de 1997.

- Coordinador General de Becas al Desempeño Académico-IPN.
  Noviembre de 1992 a marzo de 1994.

- Jefe de la División Técnica-IPN.
  Abril de 1989 a junio de 1991.

- Jefe de la División de Procesos Editoriales-IPN.
  Agosto de 1985 a marzo de 1989.

- Jefe de la División de Coordinación de Bibliotecas-IPN.
  Junio de 1984 a agosto de 1985.

- Asesor de la Dirección de UPIICSA-IPN.
  Noviembre de 1980 a octubre de 1983

- Jefe del Departamento de Matemáticas de la UPIICSA.
  Julio de 1977 a febrero de 1979.

GRUPOS DE INVESTIGACIÓN

- Coordinador y miembro de la Red de Computación del Instituto Politécnico Nacional.

- **Líneas trabajadas en la Red**: Transporte, Seguridad, Educación y Cómputo Científico.
  Octubre de 2009 a la fecha.

PUBLICACIONES:

REVISTAS NACIONALES:

- Computación y Sistemas, Una Evidencia Robusta de que el Algoritmo DES fortalecido con una Permutación Inicial Variable es Eficiente, 2011.

- Revistas de Divulgación, CONVERSUS-IPN, Criptografía, crucial para México, 31 de enero de 2007.

- Revistas de Divulgación, Economía y Democracia, Centro de Estudios sobre Economiá, Finanzas y Desarrollo Agropecuario, El Desarrollo Tecnológico en Ingeniería de Cómputo: Retos y Oportunidades, 31 de agosto de 2006.

- Algoritmo para aproximar el área bajo la curva de la Función Normal Estándar, Artículo publicado en "Polibits", Vol. 1, Número. 26, junio 2002.

- Simposium, Regresión de un Modelo no Lineal, Aplicado a la Curva de Lorenz, ESIQIE-IPN, 24 de septiembre de 1998.

REVISTAS INTERNACIONALES:

- Reducing Computational Complexity for 192 Bits SPN Encryption Algorithms with Variable Permutation; Artículo publicado en JP Journal of Algebra, Number Theory and Applications; Vol. 4, Pag. 967-976, 2010, India.

- Construction of a Cryptosystem Using the AES Box and a Bijective Function from the Natural Numbers to the Set of Permutations, Artículo publicado en Ciencia e Ingeniería Neogranadina, Vol. 19-1, julio de 2009, Colombia.

- Modelado y Control de un Robot Móvil sin Uso de Mediciones de Variables Mecánicas en el Control de los Activadores. Se publicará IEEE Latín American.

- Bijective Funtion with Domain in N and Im age in the Set of Permutation: An application to Cryptography. Artículo públicado en International Journal of Computer Science an Network Security, Vol. 7 No. 4, 2007.

- Algotithm for Strengthening Some Cryptographic Systems, Artículo publicado en International Journal of Computer Science an Network Security, Vol. 7, No. 20, 2010

- Reducing Computational Complexity for 192 Bits SPN Encryption Algorithms with variable Permutation, Artículo Publicado en Vol. 16, No. 2, 2010 Journal of Algebra, Number Theory and Applications.

DESARROLLOS TECNOLÓGICOS Y ASESORÍAS

- "Estudio y análisis respecto de la opción más Segura, Eficaz y Funcional, para apoyar la Identificación, Control y Registro Vehicular Vía Radiofrecuencia". Este trabajo se entregó a la Secretaría de Seguridad Pública, septiembre 2007.

- Adaptación del Hardware y/o Software del Pilotaje Automático SACEM para la Conversión de Trenes de 6 a 9 carros en la Línea A. Este trabajo se entregó al "Sistema de Transporte Colectivo Metro", 30 de diciembre de 2009.

- Desarrollo de un Prototipo de control de Peaje en el Sistema de Transporte Colectivo a través de la Tecnología de Tarjeta sin Contacto. Este trabajo se entregó al "Sistema de Transporte Colectivo Metro", 21 de diciembre de 2009.

- Diseño, construcción e implementación de un Criptosistema en un FPGA utilizando el algoritmo de encriptación de Doble Ronda como una solución al Teorema LR. Este trabajo se entregó al "Instituto Politécnico Nacional", 24 de noviembre de 2008.

PARTICIPACIÓN EN CONGRESOS

- Conferencias, Criptosistema DES, Instituto Tecnológico Superior de los Rios (Tabasco), Conferencia Magistral, 20 de octubre de 2005.

- 1er. Simposium Internacional en Ingeniería de Sistemas Computacionales. Criptosistemas DES. Instituto Tecnológico Superior de los Ríos Tabasco. 20 de octubre de 2005.

- A cryptanalysis procedure of the data encryption standard, SPIE, 2005.

- VIII Simposium Internacional "Aportaciones de las universidades a la docencia, la investigación, la tecnología y el desarrollo", Diseño de un dispositivo para encriptación de datos en tiempo real, 2006.

- Reduciendo el requerimiento de información para el criptoanálisis de Triple – DES, utilizando el Teorema LR, VII Coloquio nacional de Códigos, Criptografía y Áreas Relacionadas, 2006.

- 9th. Conference on Computing CORE 2008. Using Decision Diagrams to Efficient y Represent Morphological Associative Memories. Centro de Investigación en Computación. 29 de mayo de 2008.

- 9th. Conference on Computing CORE 2008. Secure Comunication. An application to the Electronic Money Transfer. Centro de Investigación en Computación. 30 de mayo de 2008.

CAPÍTULOS DE LIBRO

- Capítulo 3 – "Modelos Alfa – Beta Aplicados", Amadeo José Argüelles Cruz, Cornelio Yánez Márquez, Víctor Manuel Silva García (2007), Tópicos Selectos en Ciencias de la Computación. Colección CIDETEC, Instituto Politécnico Nacional. México. ISBN 978-970-94-6965-3

- Capítulo 4 – “Un nuevo Criptosistema Basado en Permutaciones”, Víctor Manuel Silva García, Cornelio Yáñez Márquez, Juan Luis Díaz de León (2007). Tópicos Selectos en Ciencias de la Computación. Colección CIDETEC, Instituto Politécnico Nacional. México. ISBN 978-970-94-6965-3.

FORMACIÓN DE RECURSOS HUMANOS

Licenciatura

- Director de Tesis de Licenciatura, Tema “La Inversa Generalizada” en la ESFM – IPN.

- Director de Tesis de Licenciatura, Tema “Análisis de algunos modelos utilizados para toma de Decisiones” en la UPIICSA – IPN.

- Director de Tesis de Licenciatura, Tema “Tres Alternativas para el Tamaño de la Muestra para Proporciones” en la ESFM – IPN.

Maestría

- Director de Tesis de Maestría, Tema: “Criptoanálisis para triple- DES utilizando el teorema LR”.

- Director de Tesis de Maestría, Tema: “Implementación de un FPGA del Algoritmo de Encriptación Doble Ronda como una solución al Teorema LR”.

- Asesor de Tesis de Maestría, Tema: “Propuesta de Implementación de un Tablero de Control Gerencial para GGM Gasolineras” en la UPIIICSA – IPN.

- Asesor de Tesis de Maestría, Tema: “Decisiones Agencia y Gobernabilidad Corporativa: Un estudio del Caso ENRON”.

- Director de Tesis de Maestría, Tema: “Diseño de un Esquema de Comunicación Segura utilizando como Sistema Simétrico Triple – DES y Asimétrico RSA”.

- Director de Tesis de Maestría, Tema: “Herramientas case con el Enfoque de Entidades e Interrelaciones”.

- Director de Tesis de Maestría, Tema: “Simulación de Escenarios Naturales Tridimensionales”.

- Director de Tesis de Maestría, Tema: “Algoritmo de encriptación simétrico que procesa bloques de 192 bits con llaves descifrado de 192 bits, empleando los teoremas Factorial y JV”.

- Director de Tesis de Maestría, Tema: “Esquema de encriptación de imágenes usando 3 - DES de permutación variable”.

Doctorado

- Director de Tesis de Doctorado, Tema: “Capos Finitos JV en el Conjutno de las Permutaciones: Una aplicación a la Criptografía. Examen Doctoral, Enero 2011.

- Director de Tesis de Doctorado, Tema: “Teoría y Aplicaciones del Clasificador Gamma”. Examen Doctoral, Agosto 2011.

PROPIEDAD INTELECTUAL

- Título. AES – 128 con Permutación Variable, No. De Registro: 03-2009-052110565900-01 Fecha: 29 de mayo de 2009