ReCIBE, Año 4 No. 1, Febrero 2015

Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT)

Heltton Emmanuel Ramírez Luna
Centro de Investigación en Matemáticas (CIMAT) Unidad Zacatecas
heltton.ramirez@cimat.mx

Jezreel Mejia Miranda
Centro de Investigación en Matemáticas (CIMAT) Unidad Zacatecas
jmejia@cimat.mx

Resumen: En este artículo se describe una propuesta creada para proteger la información y la infraestructura de un equipo de respuestas ante incidentes de seguridad (CSIRT), el cual es una organización dedicada a dar respuesta a incidencias de seguridad en tecnologías de la información. Un CSIRT está conformado por un grupo de expertos en seguridad de la información la cual provee de servicios como alertas y advertencias, tratamiento de incidentes, observatorio de tecnología, auditorías de seguridad, cómputo forense, entre otros. Por lo tanto, se hace uso de información sensible como datos de usuarios y de empresas que deberá tener fuertes métodos de seguridad. En este artículo se aborda una propuesta de los aspectos de seguridad que debe tener un CSIRT abarcando las áreas de Telecomunicaciones, Equipo hardware y Sistemas SIEM (Security Information and Event Management). Esta propuesta no toma en consideración la tipología en la que un CSIRT puede establecerse.

Palabras clave: Seguridad, CSIRT, infraestructura, seguridad en redes.

Proposal of security technical infraestructura for a Computer Security Incident Response Team (CSIRT)

Abstract: This paper presents a proposal created to protect the information and the infraestructure to a Computer Security Incident Response Team which is an organization entity that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. A CSIRT is formed by a group of experts in information security which provides services such as alerts and warnings, incident handling, observatory technology, security audits, forensic computing, among others. Therefore, sensitive information that must have strong security methods physical and logical is used. This paper is addressed on a proposal for security aspects which must have a CSIRT covering the areas of Telecommunications, Computer hardware and systems SIEM (Security Information and Event Management). This proposal does not take into consideration the type in which a CSIRT can be established.

Keywords: Security, vulnerabilities, web application, attacks, techniques, tools, vulnerability detection.

1. Introducción

Los sistemas informáticos se han convertido en parte esencial de la vida cotidiana. Según resultados del estudio realizado en abril del 2013, el 43.4% de la población en México, de seis años en adelante, se declaró usuaria de internet y el 30% de los hogares del país tienen una conexión a internet. Esto muestra una taza de crecimiento de 13.9% en el periodo del 2006 al 2013 (INEGI, 2014). Este crecimiento no sólo es por parte de México, un estudio realizado por la UIT (Unión Internacional de Telecomunicaciones) estima que a finales del 2014 habrá cerca de tres mil millones de usuarios en Internet (Unión Internacional de

Telecomunicaciones, 2014). Un informe en 2013 de la compañía de seguridad informática Kaspersky®, los usuarios mexicanos reciben un promedio de 3.56 ataques con malware financiero. (también a nivel internacional). Debido a las necesidades de seguridad que hasta la fecha son confirmadas, se creó el concepto de un equipo de respuesta ante incidentes de seguridad (CSIRT, del inglés Computer Security Incident Response Team con la finalidad de atender incidencias de seguridad relacionadas con la información (Roldán, 2011). Como toda empresa el activo más importante es su información, un estudio de la firma de antivirus ESET arrojó que las compañías latinoamericanas pierden 93,000 millones de dólares al año por ataques relacionados con tecnologías de la información (Escamilla, 2012). El robo o fuga de información a través del correo electrónico es el rubro más vulnerable para las empresas, con 19.2%, de acuerdo con un estudio de la consultora Deloitte México (Deloitte, 2014). En segundo lugar está el robo de información vía dispositivos de memoria portátil y/o móviles, con 13.6%, seguido del robo o pérdida de laptops, tabletas y celulares con 12.8%. La información que maneja un CSIRT es de carácter sensible, ya que en ella se encuentran datos de usuarios, empresas y entidades gubernamentales debido a que son utilizadas cuando una incidencia es generada. Este artículo presenta los aspectos que debe tener un CSIRT tomando en consideración las áreas de Telecomunicaciones, Equipo hardware y Sistema SIEM (Security Information and Event Management). El método de investigación fue la revisión sistemática, el cual contempla tres pasos los cuales son planificación, revisión y el ultimo publicación. Por lo tanto, este artículo está estructurado de la siguiente manera: sección 2 presenta una síntesis de lo que es un CSIRT y sus distintos nombramientos así como servicios que puede ofrecer, sección 3 se aborda las Telecomunicaciones; en la sección 4 se presenta el Equipo Hardware y buenas prácticas; en la sección 5 se habla de sistemas SIEM (Security information and event management); en la sección 6 se presenta la propuesta, y en la sección 7 se presentan las Conclusiones y trabajos futuros posibles.

2. ¿Qué es un CSIRT?

Un CSIRT (Computer Security Incident Response Team) es un equipo especialista en seguridad de la información dedicado a responder incidentes de seguridad informática (ENISA, 2006). El término CSIRT es el que se suele usar en lugar del término protegido CERT, registrado en EE.UU por el CERT Coordination Center (Centro Criptológico Nacional, 2013). Se usan diferentes abreviaturas para el mismo tipo de equipos:

- **CERT o CERT/CC:** (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación).
- **CSIRT:** (Computer Security Incident Response Team, equipo de respuesta a incidentes de seguridad informática).
- **IRT:** (Incident Response Team, equipo de respuesta a incidentes).
- **CIRT:** (Computer Incident Response Team, equipo de respuesta a incidentes informáticos).
- **SERT:** (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad).

2.1 Servicios de un CSIRT

Los servicios de un CSIRT están alineados a las necesidades de la población sobre seguridad informática (Penedo, 2006). Son muchos los servicios que un CSIRT puede prestar, pero hasta ahora ningún CSIRT los ofrece todos. A continuación en la Tabla 1 se presenta una breve visión general de todos los servicios conocidos de CSIRT.

Tabla 1. **Servicios de un CSIRT (CERT/CC, 2009).**

Servicios reactivos	**Servicios proactivos**	**Manejo de instancias**
Alerta y advertencias	Comunicados	Análisis de instancias
Tratamiento de incidentes	Observatorio de tecnología	Respuesta a las instancias
Análisis de incidentes	Evaluaciones o auditoría de la seguridad	Coordinación de la respuesta a las instancias
Apoyo a la respuesta a incidentes	Configuración y mantenimiento de la seguridad	Gestión de la calidad de la seguridad
Coordinación de la respuesta a incidentes	Desarrollo de herramientas de seguridad	Análisis de riesgos
Respuesta a incidentes	Servicios de detección de intrusos	Continuidad de negocio y recuperación tras un desastre
Respuesta a incidentes en el sitio	Difusión de información relacionada con la seguridad	Consultoría de seguridad
Tratamiento de la vulnerabilidad		Sensibilización
Análisis de la vulnerabilidad		Educación/Formación
Respuesta a la vulnerabilidad		Evaluación o certificación de productos

Independientemente de los servicios que ofrezca un CSIRT, como cualquier empresa responsable con su información, es necesario contar con métodos de

llevar una adecuada gestión de acceso, seguridad en el puesto de trabajo, seguridad en aplicaciones y datos, seguridad en los sistemas y seguridad en las redes de cómputo.

3. Telecomunicaciones

Uno de los activos principales de un CSIRT son las telecomunicaciones debido a que siempre debe estar en constante comunicación con otros CSIRTs para el intercambio de información como investigaciones, nuevas tendencias de malware, entre otros temas de interés y con sus clientes para llevar a cabo el seguimiento de incidentes (Roldán, 2011), por lo tanto es esencial contar con mecanismos de seguridad para las telecomunicaciones. Las características para que una comunicación sea segura, son los siguientes:

- **Confidencialidad:** Nadie ajeno a las partes interesadas puede acceder al contenido de la comunicación.
- **Integridad:** Nadie puede manipular el contenido de la comunicación, así se garantiza que llegue intacta.
- **Autenticidad:** La persona que se encuentra al otro extremo de la comunicación será la que esté autorizada a recibir dicha información.

3.1 Acceso a internet

El acceso a internet deberá estar adaptado a las políticas de la gestión de la seguridad del CSIRT (ENISA, 2006). Dichas políticas, descritas por el propio CSIRT, describen qué sitios no puede el personal del CSIRT acceder, como pueden ser portales de juegos, apuestas, páginas infectadas con algún tipo de malware, entre otros. También incluyen las políticas qué archivos pueden ser descargados, o en su defecto, cuales archivos son los que se inspeccionan antes de su descarga. Para tener un control sobre el tráfico, es posible usar un

mecanismo de protección en tiempo real basado en Proxy (Tsia, Chang, Chung, & Li, 2010).

3.2 Correo electrónico

Se recomienda contar con un sistema de email, el cual tenga buenas capacidades de filtrado, búsquedas avanzadas e integrarlas con herramienta de respuesta automática (Penedo, 2006). El criptosistema PGP (Pretty Good Privacy) es utilizado como estándar entre los CSIRT para el envío y recepción de correo electrónico (CERT Carnegie Mellon University, 2012), creado por Phil Zimmermann, funciona utilizando cuatro procesos distintos de cifrado; el hashing, comprensión de datos, cifrado de clave simétrica y cifrado de clave pública.

3.3 Página web

Un sistema de seguridad para el sitio web es importante para un CSIRT, ya que podría ser un vector muy sensible y vulnerables a ataques como una denegación de servicios distribuida (DDOS) lo cual, resultaría en un golpe muy fuerte a la reputación del CSIRT (Penedo, 2006). Técnicas de defensa como el balanceo de cargas, puede hacer frente ante este riesgo de seguridad (Centro Criptológico Nacional, 2013).

3.4 Comunicaciones alternativas

Es posible implementar mecanismos de comunicación alternativas a las tradicionales en el caso que fallen, existen muchas opciones desde contar con una segunda línea ADSL, inclusive otro tipo de tecnologías como TETRA Network, Radio, WiMAX y comunicación por satélite (Meijer, Malenstein, & Vloothuis, 2007).

4. Equipo Hardware y buenas prácticas

El equipo que sea necesario adquirir lo define la organización basándose en una planificación honesta y continua en un periodo de tiempo, esto orientado a qué servicios y a qué sector de la población va dirigidos los servicios que brindará el CSIRT (Roldán, 2011). Desde que un CSIRT se encuentra disponible en internet, llega a ser objetivo sensible de ataques e intrusiones. Un CSIRT debe de estar preparado con software y hardware diseñado para incrementar su seguridad de los servicios internos y externos (Penedo, 2006). A continuación se mencionan los más básicos a tomar en cuenta.

4.1 IPS

El IPS (por sus siglas en inglés *Intrusion prevention system*) es un software o hardware que protege redes de amenazas conocidas o no bloqueando ataques (ITECO CERT, 2009). Estos dispositivos son encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. Las acciones más usuales son descartar los paquetes de un ataque o la modificación (scrubbing) para anular el objetivo malintencionado del atacante. Se podría decir que se clasifican en dispositivos proactivos, debido a que reaccionan de forma automática a situaciones anómalas (R. Alder, 2004).

4.2 Firewall

Son soluciones para organizaciones que desean proteger varios sistemas con el mismo mecanismo (ITECO CERT, 2009). Ofrecen servicios tales como bloqueo de paquetes y es posible utilizarlos como herramienta de análisis del comportamiento de sistema y la red, herramienta de análisis forense, defensa contra virus, gusanos y spam etc. Los firewalls se pueden clasificar de acuerdo a diferentes características como las siguientes (Picouto Ramos, Lorente Pérez, García-Moran, & Ramos Varón):

- **Modelo de arquitectura.** Es dependiendo del lugar en donde se coloque en la red puede funcionar de distinta manera. Se le denomina firewall de contención aquél que protege de otras redes e internet. Si únicamente se

utiliza un firewall y protege la red interna de la organización, se le denomina firewall bastion.

- **Firewall de software y hardware.** Existen algunas características dependiendo de a qué tipo de firewall se desee implementar:
    - Software
        - Soporta varios SO.
        - Soporta varias plataformas.
    - Hardware
        - Hardware especializado más software preinstalado.
        - Sistemas operativos propietarios.
        - Funcionalidades extras como VPN, caché, etc.
        - Contienen chips específicos ASIC para Firewall (optimizados para algoritmos de encriptación).
- **Firewall red y firewall de host.** Los firewall de red protegen redes enteras y son sistemas dedicados a la función de Firewall, en cambio los Firewall de host son firewalls personales, embebidos en el sistema operativo y son más baratos en comparación con los de red.

4.3 Respaldo de datos

Se recomienda establecer un sistema de redundancia de datos para contar con un respaldo a la hora de la perdida de información. Una opción es establecer un sistema de discos RAID (Redundant Array of Independent Disks), los cuales son copias espejos en tiempo real.

4.4 Honeypot

Es un recurso de computación, el cual su función es ser investigado, atacado, comprometido, usado o accedido de forma no autorizada. Su objetivo es recabar información sobre ejemplos de malware, seguir la actividad de un gusano en la red o estudiar el comportamiento de hackers, entre otros. Estos recursos deben estar aislados del ambiente de producción. Según un estudio realizado por

ENISA (Agencia Europea de Seguridad de las Redes y de la Información), el mejor honeypot de propósitos generales es Dionaea (Grudziecki, Jacewicz, Juszczyk, Kijewski, & Pawlinski, 2012).

4.5 Hardening

La terminología fortalecimiento (Hardening) se refiere al proceso de asegurar un sistema mediante la reducción de vulnerabilidades al mínimo, esto se logra eliminado software, servicios, usuarios y así como cerrando puertos que no estén en uso, además de muchos otros métodos y técnica (Ashiqur & Al-Shaer, 2013).

Es importante mencionar que tales mecanismos de seguridad perimetral no nos protegen de ataques cuyo tráfico no pase por ellos, de copias ilegales de información en medios de almacenamiento físico, de ataques de ingeniería social, de virus informáticos en archivos o software y de fallos de seguridad de los servicios y protocolos cuyo tráfico no se esté analizado o esté permitido (INTECO-CERT, 2010).

5. Sistema de gestión de información y eventos de seguridad

Es aconsejable la automatización de controles de seguridad informática mediante un sistema de gestión de información y eventos de seguridad (SIEM, por sus siglas en inglés *Security Information and Event Management*). El sistema se deriva de una combinación de gestión de tazas y reporteo de cumplimiento de regulaciones que son los sistemas SIM (Security Information Management) y la monitorización de eventos en tiempo real y gestión de incidentes de seguridad informática llamados sistemas SEM (Security Event Management) (Perurena, García, & Rubier, 2013). Las bitácoras que recolecta el sistema SIEM sobre

aplicaciones, herramientas y dispositivos de red pueden ser obtenidas mediante: formato syslog, agentes instaladas en dispositivos, línea de comandos, API (Application Programming Interface) (NICOLETT & KAVANAGH, 2011). Existen muchas soluciones SIEM, por ejemplo ArcSight de HP, SSIM de Symantec y OSSIM de AlienVault (Perurena, García, & Rubier, 2013).

6. Propuesta

De acuerdo a los resultados obtenidos durante esta investigación se presenta la siguiente propuesta, con una pequeña descripción debajo de la imagen.

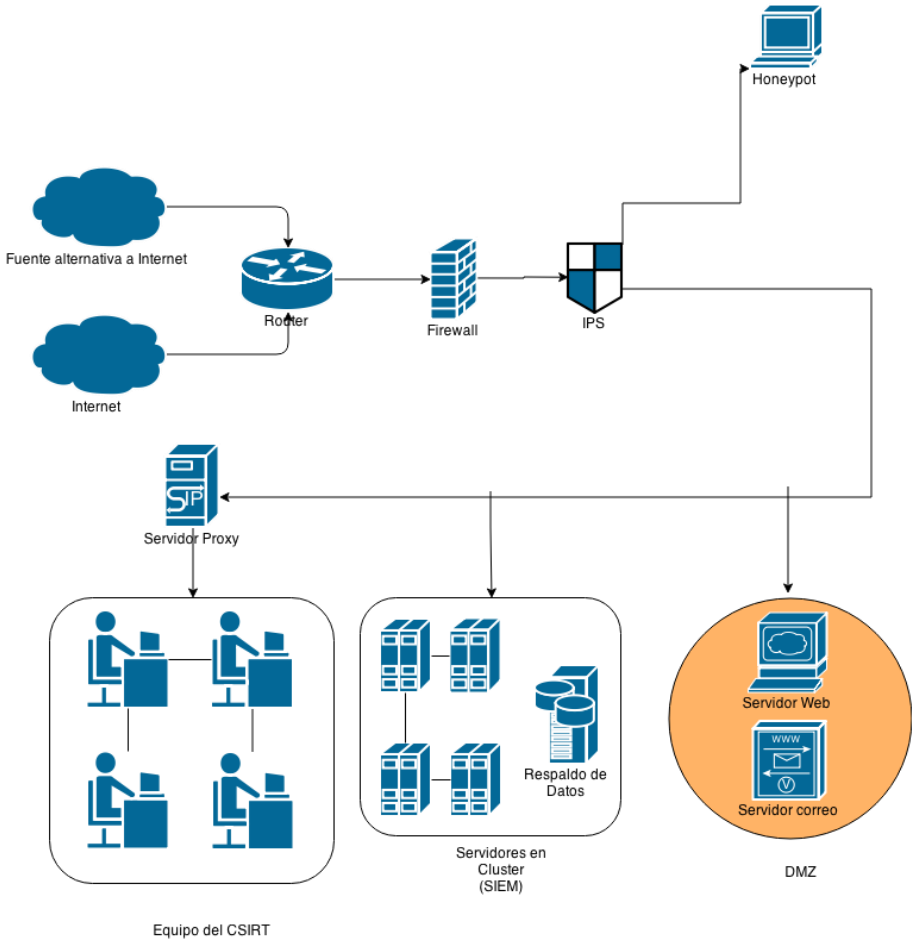

Figura 1. *Propuesta creada considerando las áreas de Telecomunicaciones, Equipo Hardware y sistemas SIEM.*

Como puede observarse en la figura anterior, el esquema general que debe considerar un CSIRT son las siguientes:

- El CSIRT tendrá como mínimo una fuente redundante de comunicación.
- Un Firewall se encuentra como primer elemento de seguridad, con el objetivo de bloquear posibles intrusiones a la red de la organización.
- Un IPS se encuentra después del Firewall, con el objetivo de examinar las firmas de las peticiones y así detectar las posibles amenazas de ataques a la red o modificar las firmas de las peticiones para que no logren su objetivo malicioso.
- Un Honeypot es utilizado para examinar las peticiones clasificadas como sospechosas.
- Se tendrán los servidores Web y de correo dentro de una DMZ (Demilitarized Zone) para que puedan ser accedidos de redes externas.
- El sistema SIEM junto con el respaldo de datos se encuentran dentro de un clúster de servidores para que procesen los activos del CSIRT de forma en conjunto.
- Los empleados del CSIRT cuentan con reglas establecidas sobre información que entra y sale de la red interna de CSIRT, siendo examinada por un Proxy y ejecutando una acción si es pertinente.

Existen documentos que hablan sobre cuestiones tecnológicas que se recomienda que incluya un CSIRT, sin embargo, estas propuestas no contemplan fuentes redundantes de la internet, ni un sistema de gestión de información y eventos de seguridad.

7. Conclusiones y trabajos futuros

Se buscaba en un principio obtener información acerca del hardware, software, tecnología y buenas prácticas que utilizan los CSIRTs en el mundo, a través de la revisión sistemática, con el fin de dirigir la propuesta hacia una tipología de

CSIRT. Sin embargo, en los resultados obtenidos no se encontró información relevante acerca de éstos debido a que tal información es de carácter sensible y por lo tanto la información no es compartida, únicamente se encontró información de manera general. Por lo tanto, también fueron analizadas páginas oficiales de CSIRTs, CERTs y de instituciones de seguridad como Kaspersky, Norton, INTECO obteniendo como resultado información relevante para establecer la propuesta. Esta propuesta permite tener una primera aproximación de los principales aspectos de Telecomunicaciones, equipo hardware, sistema SIEM y buenas prácticas sirviendo de ayuda a la constitución desde pequeños equipos dentro de una empresa, hasta los cimientos de un CSIRT escalable a grandes proporciones. Como trabajo futuro, la propuesta establecida se enriquecerá para incluir otros aspectos que se debe considerar diferentes hacia como lo es aspectos legales, límites de actuación, entre otras áreas.

Referencias

Centro Criptológico Nacional. (Junio de 2013). centro criptológico nacional del gobierno de España. Recuperado el 12 de Agosto de 2014, de www.ccn-cert.cni.es/: https://ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/820/820-Proteccion_contra_DoS-jun13.pdf

CERT Carnegie Mellon University. (2012). CERT Carnegie Mellon University. Recuperado el 12 de Agosto de 2014, de CERT Carnegie Mellon University: http://www.cert.org/contact/sensitive-information.cfm?

Tsia, D. R., Chang, A. Y., Chung, S. C., & Li, Y. S. (2010). A Proxy-based Real-time Protection Mechanism for Social Networking Sites. IEEE 978-1-4244-7402-8/10 .

Ashiqur , M. R., & Al-Shaer, E. (2013). A Formal Approach for Network Security Management Based on Qualitative Risk Analysis. International Symposium on Integrated Network Management (IM2013) .

ENISA. (2006). Cómo crear un CSIRT paso a paso. WP2006/5.1(CERT-D1/D2).

Grudziecki, T., Jacewicz, P., Juszczyk, t., Kijewski, P., & Pawlinski, P. (2012). Proactive Detection of Security Incidents. Polska: ENISA.

ITECO CERT. (13 de Agosto de 2009). Instituto Nacional de Tecnologias de la Comunicación. Recuperado el 12 de Agosto de 2014, de www.inteco.es: www.inteco.es/extfrontinteco/icd/pdf/Cortafuegos_VPN_IDS_IPS.pdf

Kaspersky Lab. (23 de Abril de 2014). latam.kaspersky.com. Obtenido de www.latam.kaspersky.com/mx: www.latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/primer-trimestre-2014-se-duplicaron-los-troya

Meijer, J., Malenstein, v., & Vloothuis. (2007). CERT Emergency Network. Amsterdam: System and Network Engineering.

Mian, P., Conte, T., Natali, A., Biolchini, J., & Travessos, G. (s.f.). A Systematic Review Process for Software Engineering. COPPE / UFRJ – Computer Science Department .

NICOLETT, M., & KAVANAGH, k. M. (Mayo de 2011). Critical Capabilities for Security Information and Event Management Technology. Recuperado el 30 de Agosto de 2014, de www.arcsight.com/library/download/Gartner - SIEM - Critical - Capabilities - for - SIEM - 2011/

Penedo, D. (2006). Technical Infrastructure of a CSIRT. IEEE 0-7695-2649-7/06 .

Perurena, M. R., García, B. W., & Rubier, P. J. (2013). Gestión automatizada e integrada de controles de seguridad informática. Revista de ingeniería electrónica Automática y Comunicaciones .

Roldán, F. S. (2011). Guía de creación de un CERT/CSIRT. Borrador, Centro criptológico nacional.

Notas biográficas:

Heltton Emmanuel Ramírez Luna Ingeniero en Sistemas Computacionales, egresado de la Universidad Politécnica de Zacatecas (UPZ), actualmente estudia la Maestría en Ingeniería del Software en el Centro de Investigación en Matemáticas (CIMAT) Unidad Zacatecas. Su interés es el desarrollo web con metodologías ágiles, modelos de calidad y la seguridad informática, ha desarrollado sistemas web en MVC y ha publicado artículos y posters presentados en congresos internacionales.

Jezreel Mejia Miranda Doctor en Informática por la Universidad Politécnica de Madrid (UPM), España con mención de "Doctorado Europeo". Realizó una estancia de investigación para obtener el doctorado europeo en la Universidad Fernando Pessoa en Oporto, Portugal. Previamente, en el Instituto Tecnológico de Orizaba, Veracruz, cursó la maestría en Ciencias de la Computación y la licenciatura en Informática. Actualmente es investigador del Centro de Investigación en Matemáticas, A.C. (Cimat), Unidad Zacatecas, en el área de Ingeniería de Software. Es miembro del grupo de investigación Cátedra de Mejora de Procesos Software en el Espacio Iberoamericano (MPSEI), donde participa en proyectos internacionales de investigación con entidades educativas y de vinculación con la industria. Es miembro del comité científico de diversos congresos. Ha publicado diversos artículos técnicos en temas relacionados con la gestión de proyectos, entornos multi-modelo, modelos y estándares de calidad y temas relacionados en entornos outsourcing. También ha participado en proyectos de la empresa multinacional everis consulting. Además, forma parte del equipo oficial de traducción al español del libro CMMI-DEV v1.2 y 1.3, versiones reconocidas por el prestigioso Software Engineering Institute (SEI) de la Carnegie Mellon University. Como investigador, sus áreas de interés son: entornos multi-modelo, gestión de proyectos software, modelos y estándares de calidad (CMMI, ISO, TSP, PSP, etc.), metodologías ágiles, métricas, mejora de procesos en entornos

outsourcing y entornos de desarrollo tradicional. Cuenta con certificación en CMMI e ISO 20000.