

Sistema de control de acceso para el nivel educativo preescolar implementando tecnología de reconocimiento biométrico dactilar.

Access control system for a kindergarten implementing biometric fingerprint recognition technology.

Luis Ángel Méndez de León (1).
Estudiante, Instituto Tecnológico de Tuxtla Gutiérrez-Tecnológico Nacional de México.
lmendezleon@protonmail.com.

Efraín Díaz López (2). Estudiante, Instituto Tecnológico de Tuxtla Gutiérrez-Tecnológico Nacional de México,
efra_1094@outlook.com.

Rosy Ilda Basave Torres* (3). Instituto Tecnológico de Tuxtla Gutiérrez-Tecnológico Nacional de México,
rbasave@ittg.edu.mx.

Imelda Valles López (4). Instituto Tecnológico de Tuxtla Gutiérrez-Tecnológico Nacional de México,
imevalles@yahoo.com.mx.

Octavio Ariosto Ríos Tercero (5). Instituto Tecnológico de Tuxtla Gutiérrez-Tecnológico Nacional de México,
oarios_oarios@yahoo.com.mx.

Roberto Cruz Gordillo (6). Instituto Tecnológico de Tuxtla Gutiérrez-Tecnológico Nacional de México,
rcruz@ittg.edu.mx.

*corresponding author.

Artículo recibido en octubre 28, 2019; aceptado en diciembre 10, 2019.

Resumen.

En este artículo se describe el desarrollo de un sistema de seguridad denominado "SecurityK", el cual plantea resolver la problemática que existe actualmente en los procesos de control de acceso y seguridad en el nivel preescolar implementando una aplicación web, aplicación de escritorio y aplicaciones móviles. El sistema se apoya en un dispositivo físico para la captura de huellas y así gestionar el proceso de acceso a la institución.

Palabras clave: Sistema de seguridad, aplicación web, aplicaciones móviles, biometría dactilar, preescolar.

Abstract.

This article describes the development of a security system called "SecurityK", which raises solve the problems that currently exist in the access control and security processes at the preschool by implementing a web application, desktop application and mobile applications. The system relies on a physical device to capture fingerprints and thus manage the process of access to the institution.

Keywords: Security system, web application, mobile applications, fingerprint biometrics, preschool.

1. Introducción.

La SEP no brinda sistemas de seguridad a las escuelas; en nivel preescolar no se cuenta con registros de las personas que se llevan a los niños, los filtros son muy vulnerables y pueden presentarse fallas de criterio humano originando una tragedia familiar y problemas a la institución educativa.

En el último censo de población y vivienda realizado (INEGI, 2010) fueron censados 236,973 centros de trabajo, del total de escuelas censadas, 86.4% son de carácter público y 13.6% son privadas, el 40.1% representa el nivel preescolar. Existen muchos casos alarmantes sobre el robo de niños en México, algunos de ellos son afuera de las instituciones educativas. El número de niños y adolescentes desaparecidos ha sido tres veces más alto que la cifra registrada entre 2006 y 2012, de mil 584 casos reportados se pasó 4 mil 394 de 2013 a julio de 2017. El Registro Nacional de Datos de Personas Extraviadas o Desaparecidas (RNPED) reporta 33 mil 482 personas registradas como desaparecidas en México desde 1979 y hasta julio de 2017, de los cuales 6 mil 079 son niños y adolescentes, lo que representa el 18.2% del total de desapariciones (Claudia, 2017).

Existe la necesidad de proteger a los niños y reducir significativamente los incidentes en la entrega de los mismos mediante el uso de un sistema que integre tecnologías de reconocimiento biométrico dactilar y software libre moderno. Este sistema fue desarrollado para su implementación en el “jardín de niños Beatriz Ordoñez acuña”.

El proceso de control de acceso de esta institución constaba de tres partes:

- **Registro de asistencia de personal.** El registro de asistencia de los maestros se hace de manera física en una libreta en la cual deben firmar su hora de llegada y salida.
- **Entrada de menores.** Los niños son llevados al jardín y dejados en la entrada de la institución sin algún registro, se cuenta con la policía escolar la cual se encarga de recibirlos en la entrada y posteriormente son canalizados a sus correspondientes salones por los docentes. }
- **Salida de menores.** La parte más crucial es la hora de la salida, en esta parte se le da acceso a los tutores, los cuales únicamente portan una credencial de la institución y con ello se les permite el acceso. El nivel de seguridad depende de la policía escolar, debido a que debe ser rigurosa de revisar adecuadamente cada credencial y además queda a su criterio dejar entrar o no a una persona, y en segunda instancia depende de las maestras las cuales hacen la entrega final de los niños.

Anteriormente, previo a la implantación del sistema, se detectó un promedio de 14 incidencias al mes ocurridas en el plantel, como se muestra en la tabla 1, de las cuales cinco de ellas eran entradas no autorizadas, donde no se conocía a la persona pero pudo acceder y nueve de ellas corresponden a salidas no autorizadas donde la persona es un tutor registrado pero no está autorizado para retirarse con un determinado alumno, adicionalmente se detectó un promedio de tres accesos denegados. De esto se concluye que la seguridad en el acceso es un 37.5% efectiva debido a que de un total de ocho accesos no autorizados solo se evitan tres.

Tabla 1. Incidencias contabilizadas en promedio por mes.

Incidencias detectadas por mes.	
Factor de riesgo.	Total.
Entradas no autorizadas.	5
Salidas no autorizadas.	9
Total de incidencias.	14

La institución no contaba con un sistema de seguridad eficiente que permitiera controlar el acceso de personas a las instalaciones, lo que podría generar algún incidente en contra de los niños o el personal. Por lo tanto, fue necesario el desarrollo y la implementación de un sistema que gestione el acceso a la instalación y que permita tener registros digitales además de entregar información en el momento que se solicite.

2. Métodos.

Existen diferentes metodologías para desarrollar proyectos desde los más complejos hasta los más simples por lo cual no podemos utilizar la misma metodología para todos. Estas metodologías se adaptan a las diferentes necesidades, presupuestos, tiempos, personal entre otros factores. Actualmente se contemplan dos grandes grupos de metodologías las cuales son las tradicionales y las ágiles. De acuerdo con el libro *Ingeniería del software* (Somerville, 2005) la programación extrema es posiblemente el método ágil más conocido y ampliamente utilizado debido a que el enfoque fue desarrollado utilizando buenas prácticas reconocidas, como el desarrollo iterativo y con la participación del cliente a niveles “extremos”. Metodología formulada por Kent Beck y publicada en 1999 en el libro *Extreme Programming Explained: Embrace Change* (Beck, 1999). Esta metodología se divide en cuatro fases las cuales fueron implementadas durante el desarrollo del proyecto.

Fase de planificación del proyecto.

La metodología de programación XP marca que el primer paso es definir las historias de usuario (*Story board*). Se acudió a la institución y el cliente especificó los requisitos. Las historias de usuario constan de pocas líneas escritas por el cliente en un lenguaje no técnico sin hacer hincapié en los detalles. A través de entrevistas de personal y los principales actores involucrados se obtuvo información necesaria para analizar requerimientos funcionales.

Trabajar directamente con el cliente y uno de los usuarios finales (dirección) nos proporcionó una gran ventaja para desarrollar y realizar cambios o actualizaciones a algunas partes del proyecto tomando en cuenta todas las opiniones.

Fase de diseño.

En esta parte basados en la metodología se propusieron diseños simples a fin de conseguir hacerlo lo menos complicado posible para conseguir un diseño fácilmente entendible e implementable. Se crearon diagramas que representaran mejor los módulos necesarios para que el sistema funcione completamente, creando relaciones entre ellos a fin de entenderlo como un todo de manera clara y ordenada.

Fase de codificación.

Parte crucial del proyecto que fue desarrollada. Es importante tener en cuenta que el cliente formuló las historias de usuario, por lo que es importante que a la hora de terminar alguna de ellas, debe estar ahí para validar que realmente cumpla con lo establecido, además de poder ver y participar en la creación del test de verificación.

Pruebas realizadas al sistema.

El proceso de las pruebas, tal como lo marca la metodología XP, fue realizada en dos partes: luego de la finalización de cada módulo y al completar todos los módulos, pruebas de integración. Para cada módulo se diseñaron pruebas en conjunto con los usuarios finales.

3. Desarrollo.

Para el desarrollo del sistema de seguridad se plantearon tres módulos:

Módulo administración: aquí se pueden hacer modificaciones a la base de datos además de generar información sobre el alumnado, el personal y la validación de datos biométricos implementando un lector de huellas.

- Especificaciones hardware: monitor, procesador Intel Pentium dual core (en adelante), 4GB en RAM y 500GB de almacenamiento (requisitos mínimos recomendados)
- Especificaciones software: sistema operativo Windows 7, 8.1, 10, framework para trabajar la aplicación y los drivers necesarios del lector de huellas.

Módulo Acceso: el módulo de acceso recibe datos (huella), las valida y autoriza el acceso reflejado en una App móvil.

- Especificaciones hardware: Lector de Huella U.are.U 4500, dispositivo móvil (celular o Tablet)
- Especificaciones software: sistema operativo Android 4 o superior.

Módulo de control de Grupo: su función es brindar información relacionada del grupo a la maestra y confirmaciones de salida de los alumnos.

- Especificaciones hardware: dispositivo móvil.
- Especificaciones software: sistema operativo Android.

3.1 Aplicación web.

La aplicación web fue diseñada para tener el control de toda la información de alumnos, tutores y personal del plantel. Algunos datos importantes que se muestran son enviados y generados automáticamente por el módulo de control de acceso y el módulo de control de grupo. En la parte inicial (figura 1) se muestra una gráfica que representa el porcentaje de asistencia de alumnos, además al costado se muestra las entradas del personal en tiempo real.



Figura 1. Página de inicio.

El sistema genera reportes de asistencia, tanto de alumnos (figura 2) y personal para tener registros precisos con fecha y hora. Además se pueden generar archivos en formato PDF para su exportación e impresión.

Nombre	Apellido paterno	Apellido materno	Hora de entrada	Hora de salida
DANIEL	ALBUSAC	ALBUSAC	Sin información	Sin información
Nombre DANIEL ALBUSAC ALBUSAC Hora de salida Sin información Tutor Sin información				
IRENE	AMATE	GARRIDO	Sin información	Sin información
JOSE	ALONSO	BECERRA	Sin información	Sin información
MAGDALENA	APARICIO	GARCIA	Sin información	Sin información
ROSA MARIA	ACIEN	LOPEZ	Sin información	Sin información

Figura 2. Reporte de asistencias de alumnos.

Esta aplicación cuenta con un CRUD (en inglés; Create, Read, Update and Delete), la cual permite al administrador crear registros, verlos, editarlos y eliminarlos según convenga (figura 3).

Nombre	Apellido paterno	Apellido materno	Opciones
ROSA MARIA	ACIEN	LOPEZ	[Edit] [Add] [Delete] [Huella dactilar]
DANIEL	ALBUSAC	ALBUSAC	[Edit] [Add] [Delete]
JOSE	ALONSO	BECERRA	[Edit] [Add] [Delete]
IRENE	AMATE	GARRIDO	[Edit] [Add] [Delete]
MAGDALENA	APARICIO	GARCIA	[Edit] [Add] [Delete]

Figura 3. Administración de alumnos.

3.2 Aplicación de control de dispositivos.

Esta aplicación, desarrollada en java, se encarga de operar los lectores de huellas en sus distintos modos: captura de huellas y verificación de acceso. Para realizar un registro de huellas se accede a la sección de “Registro” (figura 4) donde se selecciona de la lista uno de los dispositivos conectados, el cual pasa a modo de captura de huella, en el recuadro irán apareciendo cada una de las tomas de las huellas. Como regla general se debe registrar dos huellas por usuario, cada una se escanea cuatro veces para tener una mejor lectura y precisión.

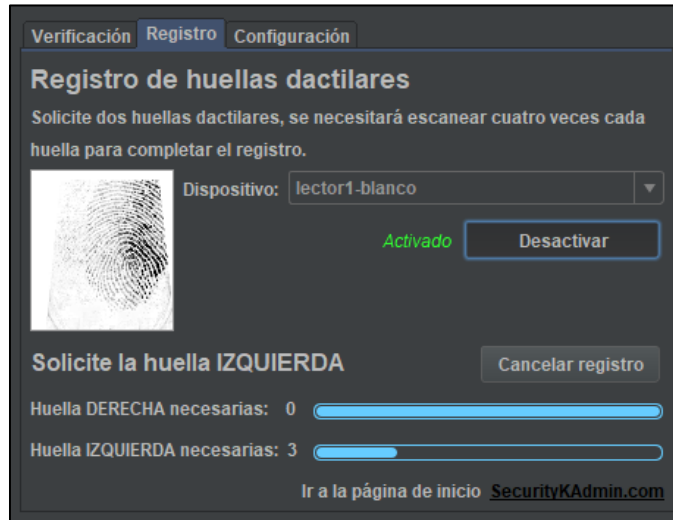


Figura 4. Registro de huellas dactilares.

La verificación de asistencia se realiza en la sección “Verificación” (figura 5) en esta se selecciona uno o dos lectores para la verificación de entrada. De la lista es posible elegir el tipo de verificación, para cada dispositivo, según el tipo de usuario (alumnos y/o personal).

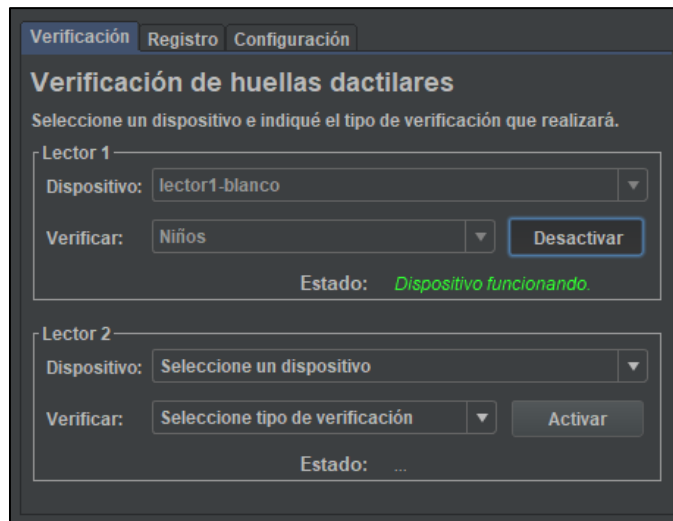


Figura 5. Verificación de huellas para el control de acceso.

3.3 Aplicación de control de acceso.

Para el módulo de control de acceso se desarrolló una aplicación para el sistema operativo Android, esta aplicación es utilizada únicamente por la guardia escolar, la cual se encarga únicamente de vigilar los accesos al plantel.

La aplicación muestra una “flecha” verde cuando un acceso es concedido (figura 6) y una “equis” roja cuando no sea una persona registrada. También se cuenta con un historial de accesos (figura 7) en el cual se visualizan los detalles de las personas accedieron y las fueron denegadas.

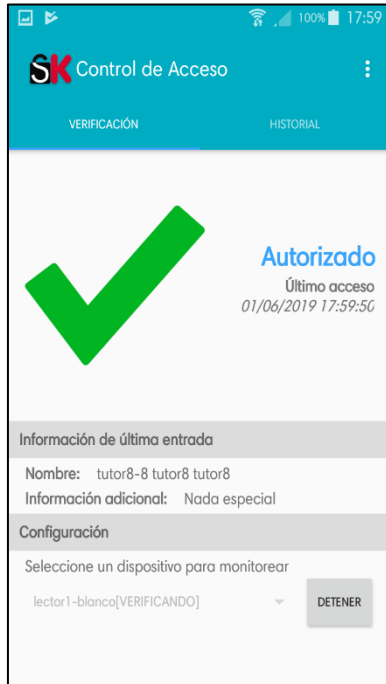


Figura 6. Información de último acceso.

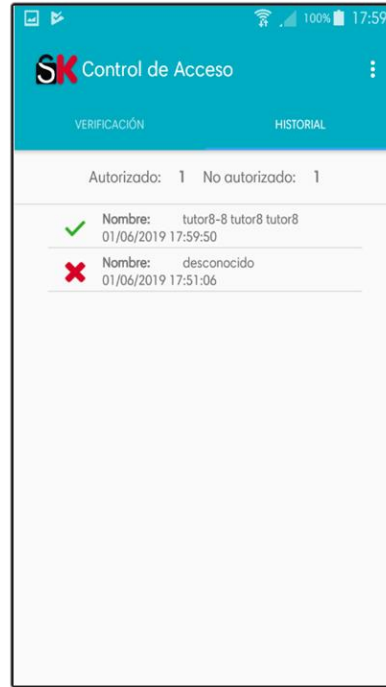


Figura 7. Historial de accesos del día.

3.4 Aplicación de control de grupo.

Esta aplicación muestra en forma de lista los alumnos del grupo que corresponde a cada docente (figura 8) así como su información relevante.

Cuenta con una lista de detalles del día donde se puede ver la hora de entrada he información de la salida de cada alumno (figura 9), en esta sección le corresponde al docente validar (figura 10) la salida de cada alumno con un tutor autorizado y generar el registro al autorizar dicha salida.

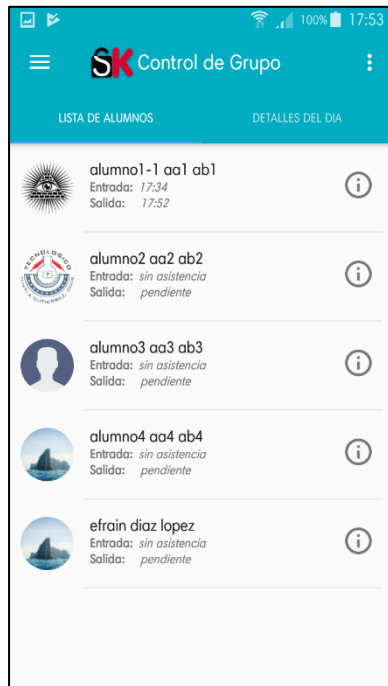


Figura 8. Lista de alumnos.



Figura 9. Detalles de entradas y salidas del grupo.

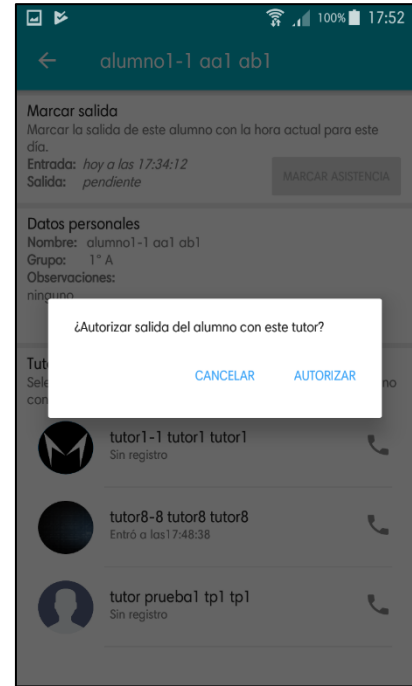


Figura 10. Detalles de entradas y salidas del grupo.

Resultados.

Se realizó la implementación del sistema de seguridad y se dejó funcionando por un mes con el objetivo de que los usuarios utilizarán todas sus funcionalidades, después se realizaron encuestas que permitieron obtener información respecto a las incidencias en entradas y salidas no autorizadas al plantel de manera que fuese posible realizar una comparación con los niveles de incidencias ocurridas en el pasado cuando no se contaba un ningún sistema de seguridad.

Tras obtener las cifras de incidencias actuales se notó un cambio significativo en el número total de estas en comparación con las mediciones anteriores como se aprecia en la gráfica de la figura 11.

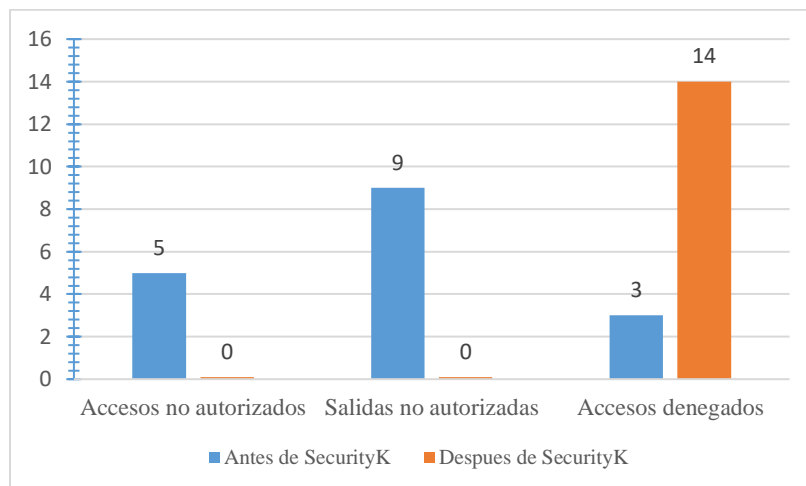


Figura 11. Comparación de incidencias ocurridas en el plantel.

El número de entradas no autorizadas fue de cero, por lo que su porcentaje de cambio fue una disminución del 100% en comparación con las lecturas anteriores, de igual forma el número de salidas no autorizadas fue de cero, obteniendo un porcentaje de cambio de disminución del 100%. Adicionalmente se obtuvo un total de 14 accesos que fueron denegados gracias a la información que proporciona el sistema de manera que el porcentaje de accesos denegados aumentó un 366.66% en contraste con las cifras anteriores.

Conclusiones.

En la actualidad existen cifras altas de incidentes relacionados con la seguridad de los planteles educativos, lamentablemente estas instituciones, en su mayoría, no cuentan con sistemas de seguridad.

Debido a las condiciones presentadas se ideó la propuesta de desarrollar un sistema de seguridad denominado *SecurityK*, el cual integra tecnología de reconocimiento biométrico dactilar para controlar las entradas al plantel y las salidas de los menores.

Durante el tiempo posterior a la implementación del sistema *SecurityK* en el plantel, se observó un aumento del nivel de seguridad. De esta forma se obtuvo un total de cero incidencias por lo que las cifras disminuyeron un 100%, además de eso, la cantidad de accesos denegados aumentó un 366.6% debido a que con el sistema se puede verificar en tiempo real cualquier persona sin autorización y de esta forma evitar su acceso. Por lo mencionado anteriormente, podemos decir que *SecurityK* demostró cumplir las necesidades del plantel educativo disminuyendo el número de incidentes que se presentaban en el control de entradas y salidas además de que se cumplieron las expectativas de los usuarios finales del sistema.

Agradecimientos.

Los autores agradecen al Instituto Tecnológico de Tuxtla Gutiérrez por la formación académica profesional, a la Lic. Mercedes Salustia Moreno Zea del jardín de niños Beatriz Ordoñez Acuña por el apoyo y la confianza brindada para el desarrollo de este proyecto en dicha institución.

Referencias Bibliográficas.

Beck, K. (1999). *Extreme programming explained: embrace change*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Claudia, A. (30 de noviembre de 2017). *animal politico*. Obtenido de <https://www.animalpolitico.com/2017/11/desaparicion-de-ninos-pena-nieto/>

INEGI. (2010). Obtenido de <http://www.beta.inegi.org.mx/proyectos/ccpv/2010/>

Somerville, I. (2005). *Ingeniería de software*. Madrid: PEARSON.

Información de los autores.



Luis Ángel Méndez de León, es egresado del Instituto Tecnológico de Tuxtla Gutiérrez de la carrera de Ingeniería en Sistemas Computacionales y por la realización de este proyecto ahora se especializa en el desarrollo de proyectos web y aplicaciones móviles.



Efraín Díaz López, es egresado del Instituto Tecnológico de Tuxtla Gutiérrez de la carrera de Ingeniería en Sistemas Computacionales, obtuvo el certificado de la especialidad Mantenimiento de equipos y sistemas computacionales en el Cecati 112 y por la realización de este proyecto ahora se especializa en el desarrollo de proyectos web y aplicaciones móviles.



Rosy Ilda Basave Torres es Maestra en Ciencias en Ciencias de la Computación egresada del Centro Nacional de Investigación y Desarrollo Tecnológico CENIDET. Es profesora de asignatura del Instituto Tecnológico de Tuxtla Gutiérrez en el área de Ingeniería en Sistemas Computacionales, donde imparte materias de especialidad, programación para Android, Tópicos Avanzados de Programación Web y Taller de Investigación, asesora proyectos de residencia profesional, titulación integral y tesis, ha dirigido y colaborado en diversos proyectos de investigación, es miembro del cuerpo académico ITTUXG-CA-7, colabora en la línea de investigación ITF-TGTZ-LIE-2018-0163, tiene el reconocimiento al perfil deseable y es miembro del Sistema Estatal de Investigadores.



Imelda Valles López, desde 1991, profesora del área de Ingeniería en Sistemas Computacionales del Instituto Tecnológico de Tuxtla Gutiérrez. Maestro en Administración por el I.T.T.G., en 2001 e Ingeniero en Sistemas Electrónicos por el ITESM en 1990. Docente de las materias de Redes, Teoría Matemática de la Computación y Compiladores. Logros importantes: Fundador de la línea de trabajo "Desarrollo de software para hablantes en lenguas nativas del estado de Chiapas" (2010), Líder de la línea de investigación "Cómputo Educativo", desde 2012, Integrante del cuerpo académico "Tecnología computacional para el desarrollo regional", ITTUXG-CA-4. Desde 2011, Profesor de tiempo completo con perfil deseable (2013-2019), Miembro del Sistema Estatal de Investigadores. Investigador Tecnólogo Nivel I desde 2012.



Octavio Ariosto Ríos Tercero es profesor en el área de Ingeniería en Sistemas Computacionales, es Maestro en Ciencias en Ciencias Computacionales egresado del Centro Nacional de Investigación y Desarrollo Tecnológico CENIDET. Su experiencia en docencia es en el área de ingeniería de software, matemáticas discretas y programación. Pertenece al cuerpo académico "tecnologías de información para el desarrollo regional". Es líder de la línea de investigación Inteligencia Artificial.



Roberto Cruz Gordillo es profesor en el área de Ingeniería en Sistemas Computacionales, es Maestro en Ciencias egresado del INAOE. Su experiencia en docencia es el área de matemáticas para la computación.