

PROPUESTA DE SISTEMA DE INFORMACIÓN PARA EL CONTROL DE INCIDENCIAS DEL PERSONAL

César Javier Jiménez Rodríguez Ing.¹, MTI. Jorge Carranza Gómez²,
Dr. Eduardo De La Cruz Gámez³ y MC. Juan Miguel Hernández Bravo⁴

Resumen—Hoy en día muchas empresas han implementado sistemas de control de asistencia para monitorizar el cumplimiento de la jornada laboral de sus empleados, y así llevar a cabo procedimientos de percepciones o deducciones de sueldo. Algunos de estos sistemas cuentan con dispositivos electrónicos de control de acceso biométrico, los cuales disminuyen la posibilidad de suplantación de la identidad al momento de checar asistencia. A pesar de esto, el personal encargado de gestionar la información del sistema puede manipular y corromper los datos, recayendo en el mismo problema. El Sistema de Información para el Control de Incidencias del Personal (SICIP) ofrece funciones de gestión de seguridad y auditoría para brindar mayor control y seguimiento de los datos registrados y los accesos a los mismos. También brinda la opción de generar diferentes tipos de reportes para presentar información confiable y que sirva como apoyo para la toma de decisiones en la empresa.

Palabras clave—Control de asistencia, Dispositivo biométrico, SICIP, Seguridad, Auditoría, Reportes.

Introducción

Muchas empresas hoy en día hacen uso de algún mecanismo o sistema para la gestión de las asistencias del personal, con el objetivo de poder valorar algunos aspectos como la puntualidad, asistencia y tiempo de estancia en el área laboral por parte de los trabajadores, y poder con ello, realizar procedimientos para la percepción o deducción de sueldos.

Estos sistemas implementan diferentes mecanismos con los cuales se puede ir generando un registro histórico de las incidencias y puede ser posteriormente consultado para diferentes fines.

Algunos de las mecanismos más utilizados es el uso de boletas o planillas impresas para el registro de las horas de entrada y de salida. Estas planillas pueden ser rellenas manualmente con un bolígrafo o por medio de algún dispositivo que las marque usando tinta o marcas por medio de presión.

Estos mecanismos son suficientes para empresas con una plantilla laboral pequeña, pero en el caso de empresas con un mayor número de trabajadores puede resultar impráctico debido al tiempo que toma llevar a cabo el registro de las incidencias. Tomando esto en consideración, se han introducido tarjetas con tecnología de radiofrecuencia, las cuales pueden ser leídas en instantes y se puede almacenar la información de forma digital en lugar de la forma física que ofrecen las planillas impresas.

Aunque se aumenta la practicidad, aún existe un factor más a cubrir y que puede ser de gran importancia para las empresas. Cualquier persona que tenga en su poder la tarjeta puede realizar el registro de la incidencia o en el peor de los casos, obtener acceso a algún lugar restringido, lo cual es un problema de seguridad. Para combatir esto se han creado dispositivos que permiten leer patrones anatómicos únicos para cada ser humano haciendo uso de la biometría.

Biometría es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos (Sihuas y Huayta, 2016). Cuando este estudio cuantitativo se automatiza utilizando métodos matemáticos y ayudado por computadoras, se llama biometría informática. La identidad que se construye utilizando estos procedimientos se llama identidad biométrica de la persona.

Algunos sistemas de control de asistencia implementan dispositivos electrónicos de control de acceso biométrico, con los cuales, se puede tener mayor seguridad y confiabilidad en los datos que son capturados para cada uno de los individuos que están registrados en el sistema. El hecho de restringir la identidad de cada trabajador utilizando un identificador biométrico, como puede ser la huella dactilar, disminuye en gran medida la posibilidad de que se presenten casos de suplantación de la identidad.

¹ César Javier Jiménez Rodríguez Ing. es Estudiante de la Maestría en Sistemas Computacionales en el Instituto Tecnológico de Acapulco, Guerrero, México. javier.jim.rod@gmail.com (autor correspondiente)

² El MTI. Jorge Carranza Gómez es Profesor de la Maestría en Sistemas Computacionales en el Instituto Tecnológico de Acapulco, Guerrero, México. jcarranzamx@hotmail.com

³ El Dr. Eduardo De La Cruz Gámez es Profesor de la Maestría en Sistemas Computacionales en el Instituto Tecnológico de Acapulco, Guerrero, México. gameduardo@hotmail.com

⁴ El MC. Juan Miguel Hernández Bravo es Profesor de la Maestría en Sistemas Computacionales en el Instituto Tecnológico de Acapulco, Guerrero, México. jmhernan@yahoo.com

Si bien utilizando dispositivos biométricos se puede tener mayor fiabilidad en la información del sistema de control de asistencia, no se está exento de la posibilidad de manipulación de los registros históricos por parte del personal encargado de manejar el sistema, esto con el objetivo de poder favorecer a empleados que no son cumplidos con su jornada laboral. Es por ello que es necesario contar con algún mecanismo que permita monitorear el estado de la información de este tipo de sistemas, para así tener mayor certeza de que los datos de las consultas o reportes generados muestran realmente información fidedigna y que no ha sido modificada con malos propósitos.

Sistema de Información para el Control de Incidencias del Personal (SICIP)

SICIP es un sistema que surge como una propuesta de solución para el control de incidencias del personal en cuanto a jornada laboral se refiere. SICIP ofrece diferentes funciones para gestionar la información de los empleados, horarios, asistencias y registro histórico de incidencias como justificaciones y permisos; además, brinda la posibilidad de generar reportes que permiten filtrar y organizar información específica con el fin de poder tomar decisiones o servir como referencia para posteriores procedimientos en la empresa.

Si bien existen sistemas de control de asistencia en el mercado que ofrecen estas funcionalidades, el factor innovador de SICIP recae en la gestión de la seguridad y la auditoría de la información.

SICIP cuenta con un módulo de seguridad con el cual se puede:

- Gestionar usuarios.
- Crear perfiles para definir el alcance de los usuarios en las funcionalidades del sistema.
- Conceder y revocar privilegios a determinados perfiles o usuarios, permitiendo restringir o escalar las funcionalidades de los mismos.
- Realizar auditoría de accesos y modificaciones de la información almacenada en el sistema, para conocer a detalle su estado, qué datos fueron accedidos y/o modificados, cuando fue realizada la acción y quién la realizó.

Así también, SICIP cuenta con un dispositivo biométrico con sensor para lectura de huellas dactilares, con el cual se da mayor seguridad para el registro de la información de los empleados, relacionando con un identificador biométrico único la información que a cada quién corresponde. Esto evita que entre los empleados pueda haber suplantación de la identidad para favorecer a los que no cumplen correctamente con su jornada laboral asignada.

Características y funcionalidades de SICIP

El sistema cuenta con cinco módulos definidos para un funcionamiento integral:

1. Inicio de sesión. Es la parte del sistema que se encarga de los procedimientos de autenticación de los usuarios para permitir su ingreso al sistema y acceder a las funcionalidades del mismo.
2. Catálogos. Brinda las opciones necesarias para poder realizar el registro, modificación, consulta y eliminación de datos de las distintas entidades del sistema, tal como los empleados, los departamentos, horarios, lista de incidencias y justificaciones.
3. Reportes. Ofrece la posibilidad de realizar consultas y generar reportes para el análisis y la toma de decisiones.
4. Incidencias. Para el registro de diferentes tipos de incidencias que se relacionan a diferentes eventos en la jornada laboral de los empleados, tal como justificaciones y permisos.
5. Seguridad. Ofrece las opciones para la gestión de usuarios y perfiles y así controlar el acceso a las diferentes funcionalidades e información del sistema. Además permite realizar auditorías de la información para verificar la fiabilidad de la información que se consulta o se genera en los reportes.

En la Figura 1 se da a conocer un gráfico con algunas de las opciones que brinda el sistema para llevar a cabo las funciones de tratamiento de la información de asistencias e incidencias de los trabajadores.



Figura 1. Características de SICIP.

Descripción del Método

Para el desarrollo de SICIP, se hizo uso de uno de los modelos de proceso de desarrollo de software más utilizados hoy en día, el Modelo Iterativo e Incremental propuesto por Harlan Mills (1970), el cual consta de las etapas de Análisis, Diseño, Codificación y Pruebas.

Para efectos prácticos del proyecto, se decidió definir cinco etapas a través de las cuales se desarrolló el mismo, pero conservando las bases del método de desarrollo de software antes mencionado. Estas etapas son las siguientes.

1) Especificación

En esta etapa se obtuvieron los requerimientos del cliente, para analizarse posteriormente, y establecer los elementos involucrados en el desarrollo de software, se realizó el análisis del problema y se hizo la recabación de los requerimientos.

En primera instancia se obtuvieron los requerimientos funcionales que son las acciones que puede llevar a cabo el sistema. Así mismo, se obtuvieron los requerimientos no funcionales que son aquellas restricciones del sistema y que se enfocan principalmente a características de rendimiento, usabilidad, eficiencia y dependencia.

Como producto final de la etapa se obtuvo el documento de especificación de requerimientos, el cual contiene una descripción detallada de lo que es necesitado por los usuarios en el sistema.

2) Diseño

En esta etapa se analizaron, definieron y diseñaron los elementos involucrados en el desarrollo del software. El objetivo principal fue crear los elementos de soporte para el seguimiento del proyecto, ya sea como marco de referencia de las reglas de negocio, de las vistas que van a poder acceder los usuarios o de los datos que se van generar y almacenar con el uso del software.

Para el caso de SICIP, aquí se definió la arquitectura del sistema, es decir, los módulos y componentes de los cuales está conformado.

Para el modelado de la arquitectura del sistema se hizo uso de la notación UML para el caso de los diagramas que describen el comportamiento, casos de uso, interacciones y flujos de datos en el sistema. Por otro lado, para la base de datos que almacena la información del sistema se utilizó los diagramas Entidad-Relación o ER para poder representar la estructura de la misma.

3) Codificación

En la etapa de codificación se generó el código necesario que conforma al software. Este proceso se basó en el análisis de los requerimientos y su representación en código funcional que permitan realizar lo que se necesita. Además de esto, se realizaron pruebas unitarias para verificar el funcionamiento de cada requerimiento.

La construcción de SICIP se realizó por módulos, los cuales sirven como base para los otros. Estos módulos contemplan las partes de Inicio de Sesión, Catálogos, Seguridad, Incidencias y Reportes.

El orden de implementación tomó en cuenta como primer elemento al módulo de Inicio de Sesión, el cual es la base del sistema al permitir el acceso de usuarios autorizados a las diferentes partes del sistema.

Seguidamente se implementó el módulo de Seguridad, dentro del cual se puede realizar la creación de usuarios y perfiles, así como la asignación de privilegios de acceso a partes y funciones del sistema. La parte de auditoría se decidió realizar al final para poder tomar en cuenta las demás funcionalidades de los otros módulos.

Posteriormente se implementó el módulo de Catálogos, el cual permite la gestión de elementos persistentes en el sistema, tal como la información del personal, horarios, listas de justificaciones e incidencias.

Después se procedió a implementar el módulo de Incidencias, el cual es el núcleo de las funciones del SICIP. En este módulo se puede hacer la gestión de todas las incidencias relacionadas al personal en cuanto a control de asistencias. Toda la información recabada puede ser consultada desde la interfaz del sistema, además de permitir el llevar un historial de todas las incidencias, con la posibilidad de poder filtrar la información que sea relevante para quien consulta.

Se tiene también el módulo de Reportes, el cual brinda todas las funcionalidades para poder generar reportes en diferentes formatos para poder valorar la información de las incidencias. Además de esto, se puede obtener información específica para diferentes propósitos, ordenando los datos y presentándolos de una forma que sea entendible para quien consulte la información.

Y finalmente, se implementan las funcionalidades de Auditoría en módulo de Seguridad, con lo cual se puede hacer uso de la información generada por los demás módulos y poder así realizar las tareas de verificación que la opción de auditoría ofrece.

4) Validación

La validación se refiere a un conjunto de actividades que aseguran que el software lleve a cabo de manera correcta una función específica. Aquí se buscó que el software tenga trazabilidad de acuerdo a los requerimientos planteados en la primera etapa. Las actividades que se consideraron en esta etapa son: pruebas, corrección de errores y solicitud de cambios.

En la etapa de Validación, el SICIP fue sometido a un primer uso de prueba, en donde se pueden verificar si las funcionalidades solicitadas fueron implementadas en el sistema, con lo cual, se pueden encontrar fallas u omisiones de diseño, para así poder realizar una reparación temprana que no afecte al funcionamiento del sistema posteriormente.

En caso de haberse encontrado fallas o comprobar que algunos de los requerimientos no son cumplidos, se puede realizar una solicitud de cambios, los cuales llevarán a una actualización del sistema para poder así hacerlo más fiable.

5) Operación y Mantenimiento

A partir de este momento es cuando los usuarios reales del sistema pudieron hacer uso de las funcionalidades y generar retroalimentación.

Esta última etapa se realiza de manera continua. Antes del uso del sistema, se llevó a cabo la capacitación de los usuarios que lo utilizarían. Aquí se mostró a los usuarios lo que pueden y lo que no pueden hacer en el sistema, y cómo llevar a cabo sus actividades.

Además de la capacitación, se debe llevar a cabo el mantenimiento del sistema, haciendo una revisión periódica del funcionamiento del sistema, cuidando de que se esté almacenando información de manera correcta y que no esté presentando fallas. En algunos casos se requiere de soporte técnico cuando se presente una problemática, que puede ser de ayuda para saber cómo funciona el sistema en determinada actividad, o la atención de fallas que se presenten en el mismo.

Con la aplicación de esta metodología, se aseguró contar con las etapas de desarrollo necesarias para la creación de un software de calidad y que cumple con los estándares mínimos, ofreciendo mayor confiabilidad a los usuarios de que el sistema puede funcionar de forma correcta ya que se consideraron todos los aspectos posibles en proyectos de este tipo.

Comentarios Finales

Con ayuda del SICIP se obtiene una mayor eficiencia en comparación con los procesos tradicionales del control de asistencia, ya que los registros de asistencias de los empleados se manejan en una base de datos, permitiendo conocer los resultados inmediatamente después que el empleado haya registrado su asistencia, así como de diferentes tipos de reportes según se necesite.

Además, mediante el sistema se mantiene un alto nivel de integridad de los datos, ya que los registros de asistencias pueden ser auditados y monitoreados solo por personal autorizado, reduciendo la posibilidad de adulterar o modificar la información, por lo tanto se asegura que los resultados obtenidos por medio del sistema de información son confiables.

Como todo proyecto de software, SICIP es susceptible a mejoras y cambios en las funcionalidades que ofrece, por lo cual, se debe realizar un estudio más a fondo de las necesidades de los usuarios del sistema y poder así añadir funciones complementarias que hagan más robusto el sistema y poder así tener un mayor alcance para las tareas de las que es requerido.

Referencias

Ccama, J. "Diseño e Implementación de un Sistema de Video Vigilancia y Control de Asistencia Biométrico de la Empresa Autoaccesorios de los Gemelos S.A.C de la Ciudad de Juliaca," Universidad Nacional del Altiplano Puno, 2014.

Gallego, J. "Formación Profesional Básica - Operaciones Auxiliares para la Configuración y la Explotación," Editex, 2014

Hurtado, P. y E. Ordoñez. "Implementación del Sistema de Seguridad y Control de Asistencia Biométrico para el Laboratorio de Automatización de Procesos Industriales en la Escuela de Ingeniería Industrial-Espoch," Escuela Superior Politécnica de Chimb, 2016.

Mills, H. "Top Down Programming in Large System," IBM Federal Systems Division, 1970.

Sihuas, M. y B. Huayta. "Propuesta de un Sistema Automatizado de Control de Asistencia para la Eficacia en el Registro del Personal en el Programa Subsectorial de Irrigaciones del Ministerio de Agricultura y Riego," Universidad Inca Garcilaso de la Vega, 2016.