

**Instituto Tecnológico de Tuxtla Gutiérrez Chiapas**

INGENIERIA EN SISTEMAS COMPUTACIONALES

Propuesta para el desarrollo del proyecto del titulado:

Sistema de Control de Accesos y Administración de Áreas

Presenta:

Jesús Alejandro Jiménez Jiménez

Nom. Control:

20271069

Asesor interno:

Mtra. Rosy Ilda Basave Laguna

Ciudad: Fecha:

San Cristóbal de las casas Chiapas 18/09/2024

**Índice**

[Agradecimientos 3](#_Toc177803792)

[Resumen 4](#_Toc177803793)

[1.1 Introduccion 6](#_Toc177803794)

[1.2 Descripcion de la empresa 7](#_Toc177803795)

[1.3 Problemas a resolver 8](#_Toc177803796)

[1.4 Objetivos 10](#_Toc177803797)

[**1.4.1 Objetivos Específicos:** 10](#_Toc177803798)

[1.5 Justificacion 11](#_Toc177803799)

[2.1 La gestión de accesos y seguridad 13](#_Toc177803800)

[**2.2.1 Sistema de Acceso fisico** 13](#_Toc177803801)

[**Componentes de un Sistema de Control Físico** 13](#_Toc177803802)

[**2.2.2 Sistema de Acceso Logico** 14](#_Toc177803803)

[**Aspectos Cruciales del Control Lógico** 14](#_Toc177803804)

# **Agradecimientos**

A lo largo de este camino, no puedo dejar de agradecer a Dios, quien ha sido mi fortaleza y guía constante. Ha sido la luz en mi vida, iluminando mi sendero y dándome las fuerzas necesarias para enfrentar cada obstáculo que ha surgido en el transcurso de mi carrera y mi vida personal. En los momentos más oscuros, su presencia ha sido mi consuelo, y su sabiduría, el faro que ha guiado mis decisiones.

Quiero extender mi más profundo agradecimiento a mi madre. Ella ha sido, sin duda, la piedra angular en mi vida, la persona que, con su amor incondicional, ha estado a mi lado en cada paso del camino. Gracias, mamá, por tu inagotable dedicación y sacrificio, por ser el modelo de vida que me ha inspirado a seguir adelante, incluso en los momentos más difíciles. Tus consejos, tu apoyo inquebrantable y tu amor son los pilares que han sostenido mis aspiraciones y mis sueños.

A mi padrastro, quien ha sido un apoyo invaluable en mi vida y en mi carrera, le extiendo mi más sincero agradecimiento. Tu presencia y respaldo han sido fundamentales para que hoy pueda estar donde estoy. Agradezco profundamente tu confianza en mí, tu paciencia y, sobre todo, tu disposición para ayudarme en cada etapa de este proceso. Has estado ahí, no solo en los momentos de éxito, sino también en los momentos de mayor dificultad, ofreciéndome tu mano cuando más lo necesitaba y dándome el impulso necesario para seguir adelante.

No puedo dejar de mencionar a quienes me brindaron la oportunidad de desarrollarme profesionalmente y de llevar a cabo mi proyecto de residencia. Agradezco de todo corazón por haber confiado en mí y por haberme permitido formar parte de su equipo. Cada consejo, cada palabra de aliento, y cada uno de los conocimientos compartidos han sido de un valor incalculable para mi crecimiento profesional y personal. La experiencia adquirida durante este tiempo no solo me ha permitido fortalecer mis habilidades, sino también comprender mejor el entorno en el que me desenvuelvo, y por ello, estoy profundamente agradecido.

# **Resumen**

**CAPITULO I: GENERALIDADES DEL PROYECTO**

# **1.1 Introducción**

En un mundo cada vez más digitalizado y competitivo, la seguridad se ha convertido en un pilar esencial para las empresas. La adopción de tecnologías avanzadas y el conocimiento de los riesgos actuales y futuros son fundamentales para proteger tanto la información como las instalaciones. Hoy en día, estar desprotegido y desinformado frente a las amenazas representa un grave peligro para cualquier organización.

Con el objetivo de reforzar la seguridad, BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS S.A. DE C.V. busca implementar un Sistema de Control de Accesos y Administración de Áreas que se adapte a sus necesidades particulares. Este software no solo fortalecerá la protección de las instalaciones, sino que también se integrará eficazmente en las operaciones diarias de la empresa.

El sistema aprovechará tecnologías actuales, manteniendo la compatibilidad con las tarjetas magnéticas ya existentes en la empresa, como los lectores de tarjetas. Ofrecerá una plataforma intuitiva para los administradores, facilitando la gestión de permisos de acceso, el monitoreo de entradas y salidas, y la generación de reportes detallados sobre el uso de las áreas.

Además, se incluirán funcionalidades específicas para la gestión de áreas sensibles, lo que permitirá un mayor control y optimización de los niveles de seguridad y confidencialidad. Con la implementación de este sistema, la empresa busca una mejora en la infraestructura de seguridad, garantizando un acceso controlado y eficiente para sus colaboradores y visitantes.

# **1.2 Descripción de la empresa**

BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS S.A. DE CV es una empresa orgullosamente chiapaneca, 100% comprometida con la producción y distribución de botanas elaboradas a partir de productos derivados del maíz. Con una profunda conexión a las raíces culturales y geográficas de Chiapas, esta empresa busca destacar por la calidad de sus productos, como también por su dedicación a la responsabilidad social y ambiental.

En cada etapa de su proceso productivo, BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS se esfuerzan día con día para lograr garantizar el equilibrio en su crecimiento económico, preservar el medio ambiente y bienestar social, logrando asegurar un futuro sostenible para las generaciones venideras. La empresa no solo está enfocada en el crecimiento empresarial y económico, sino también tienen presente el poder crear un impacto positivo en la sociedad, demostrando la posibilidad del desarrollo económico a la par con la conservación del entorno natural.

**1.2.1 Misión:**

La misión de BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS es clara: producir y distribuir alimentos de la más alta calidad, garantizando que cada producto cumpla con los más exigentes estándares de excelencia en calidad. Buscan no solo satisfacer los gustos de los consumidores, también superar expectativas que tiene los consumidores hacia la empresa, logrando ofrecer botanas para combinar un sabor inigualable teniendo un proceso de producción que refleja un compromiso inquebrantable con la calidad y la sostenibilidad.

**1.2.2 Visión:**

La visión de BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS es lograr convertirse en una empresa líder del sureste mexicano en producción y distribución de botanas. Están dirigidos no solo a ser reconocidos por la calidad y excelencia de los productos, sino también con un compromiso con la nutrición de sus consumidores. En la actualidad con un mercado en constante evolución, la empresa aspira a lograr destacarse no solo por la capacidad de innovación, también por la atención personalizada que brinda a sus clientes, permitiendo forjar relaciones duraderas basadas en la confianza y el respeto.

# **1.3 Problemas a resolver**

Realizado una exhaustiva evaluación en BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS S.A. DE CV., se llegó a la conclusión que los accesos son llevados cabo de manera manual, lo que presenta varias limitaciones y desafíos operativos en diversas áreas dentro de la empresa. Actualmente, los registros tanto de entrada y salida de colaboradores, visitantes y trabajadores por contrato se realizan mediante documentos en papel con diversos formatos de visitas, salidas, jornadas de labor amiento. Este proceso implica que cada empleado, visitante o trabajador por contrato deba anotar su hora de entrada y salida en listas físicas, lo que puede ser propenso a errores y falta de precisión.

**Procedimientos Actuales:**

**Registro Manual:**

Actualmente los colaboradores registran su acceso mediante listas en hojas las cuales se encuentran en los puntos de entrada y salida de las instalaciones. El método requiere de una supervisión constante del personal de seguridad y personal encargados de las áreas, lo que genera congestión en la administración de registros, llevando a la acumulación excesiva de registros de acceso a diversas áreas que con el paso del tiempo ha llevado a generar un gran consumo de hojas para el listado de accesos generando una cantidad exagerada de hojas acumuladas de años anteriores y continuando la acumulación.

**Conteo de Jornadas Laboradas:**

El conteo de las jornadas laborales es llevado a cabo mediante verificación diariamente en las listas de acceso, implicando una revisión manual exhaustiva por parte del departamento de recursos humanos y personal de seguridad, lo que provoca discrepancias en el registro de horas laboradas y a la generación de informes, haciendo que la tarea de conteo de horas sea un proceso lento y propenso a errores.

**Tarjetas de Presentación:**

Se realiza uso de tarjetas con el fin ser de identificación de los colaboradores, éstas no son empleadas con un uso de registros de acceso. Se implementará el uso de tarjetas con bandas magnéticas con el fin de aprovechar herramientas como seria el sistema a crear de seguridad, así logrando un potencial de seguridad y eficiencia que estas pueden brindar con un sistema de control utilizando el sistema de banda magnética que proporcionara las tarjetas.

**Limitaciones del Sistema Actual:**

**Propenso a Errores:** La dependencia de registros manuales da lugar a errores en la anotación de datos de suma importancia tanto en accesos y conteo de jornadas de los colaboradores, afectando la fiabilidad de la información recabada diariamente.

**Ineficiencia Operativa:** El proceso actual realizado manualmente genera ser laborioso y consumir tiempo de suma importancia en las áreas como son área de seguridad y procesos de contabilidad, dificultando el flujo de trabajo y generando retrasos en la verificación de accesos y verificación de jornadas laboradas por el personal.

**Dificultad en la Generación de Reportes:** La recopilación de datos mediante el proceso actual de revisión de listas diariamente para generar informes sobre las jornadas laborales y los accesos resulta ser tediosa y generando en información desactualizada o incompleta.

**Falta de Seguridad:** El no contar con un sistema que automatice los accesos, limita la capacidad de la empresa para poder gestionar de manera efectiva las áreas restringidas y proteger la información confidencial en áreas de mayor delicadeza.

# **1.4 Objetivos**

El objetivo del proyecto tiene como finalidad el diseñar, desarrollar e implementar un sistema de software integral para la gestión de accesos en la empresa BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS S.A. DE CV., que sea plenamente compatible con las tarjetas de acceso magnéticas actualmente en uso. Este sistema tiene como finalidad mejorar la seguridad y la eficiencia operativa en sectores específicos mediante el control riguroso de los permisos de acceso y la administración de áreas específicas dentro de las instalaciones. El sistema de software deberá integrarse sin problemas con el hardware existente de tarjetas magnéticas, asegurando una comunicación eficaz con los lectores de tarjetas y otros dispositivos de control de acceso, la compatibilidad garantizada permitirá que el nuevo sistema opere de manera fluida sin necesidad de reemplazar equipo físico actual.

## **1.4.1 Objetivos Específicos:**

**Desarrollar un sistema de software**: Se realizará el sistema que logre la gestión de manera centralizada los permisos de acceso para las áreas específicas de la empresa, optimizando procesos de acceso y operaciones diarias.

**Integración del software**: El sistema debe ser compatible con los dispositivos de control de acceso existentes, logrando una compatibilidad con las tarjetas de acceso y lectores actuales utilizados en las instalaciones.

**Implementación de monitoreo y reportes**: Permitirá el registro de entradas y salidas en tiempo real, así como generar informes detallados sobre los accesos en áreas específicas, realizando un control de las horas laborales de los colaboradores en cada área.

**Optimización de áreas sensibles**: Se brindará un mayor control en los accesos a zonas restringidas y delicadas, como tanto visitas y jornadas laborales, mejorando los niveles de seguridad, confidencialidad y gestión de reportes de acceso.

**Aseguración de comunicación entre el software y el hardware existente**: El sistema está diseñado para evitar la necesidad de reemplazar los equipos actuales, buscando la compatibilidad con las tarjetas magnéticas y sus lectores.

# **1.5 Justificación**

La gestión eficiente y segura de accesos es fundamental para garantizar la protección tanto de la información confidencial como de los productos de alto valor, especialmente en una empresa dedicada a la producción de alimentos de alta calidad como BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS S.A. DE C.V. En el contexto actual, donde la seguridad física juega un papel esencial en la operación diaria de las organizaciones, la implementación de tecnologías como lectores de banda magnética y cerraduras electrónicas es vital para mantener el control y la protección de las instalaciones.

Este proyecto tiene como objetivo integrar un sistema de control de accesos que se ajuste a las necesidades específicas de la empresa, permitiendo la gestión de permisos de manera centralizada y garantizando la compatibilidad con las tarjetas magnéticas actualmente en uso. Esta solución no solo mejorará la seguridad en las áreas sensibles de la empresa, sino que también optimizará la eficiencia operativa al automatizar y simplificar el control de entradas y salidas.

Con esta implementación, BOTANAS Y FRITURAS DE LOS ALTOS DE CHIAPAS S.A. DE C.V. podrá consolidar un entorno más seguro para sus colaboradores y visitantes, asegurando que solo el personal autorizado tenga acceso a zonas restringidas, al mismo tiempo que mejora la administración de sus recursos y reduce los riesgos asociados a accesos no controlados.

**Capitulo II: Marco teórico**

# **2.1 La gestión de accesos y seguridad**

La seguridad en organizaciones y empresas es un elemento vital que abarca múltiples dimensiones, entre ellas, el control de acceso físico y el control de acceso lógico. Estas medidas son implementadas para proteger no solo los activos físicos y la integridad de las personas, sino también para salvaguardar la información crítica y los sistemas informativos. Aunque ambos controles son fundamentales, operan en planos distintos y atienden amenazas de diferente naturaleza. Este artículo profundiza en las características, implementaciones y diferencias esenciales de cada tipo de control de acceso.

## **2.1.1 Sistema de Acceso físico**

El control de acceso físico se refiere a las medidas de seguridad implementadas para restringir y monitorear la entrada y salida de personas a un espacio físico determinado. Estos protocolos están diseñados para prevenir accesos no autorizados, protegiendo así, tanto los recursos tangibles como a los individuos presentes en el lugar.

Los sistemas de control de acceso físico pueden incluir diversas tecnologías y estrategias, desde cerraduras y llaves tradicionales hasta tarjetas magnéticas, lectores biométricos y sistemas de video vigilancia de última generación.

### **Componentes de un Sistema de Control Físico**

* Cerraduras y llaves
* Tarjetas de proximidad
* Teclados numéricos
* Lectores biométricos
* Barreras físicas como torniquetes y puertas de seguridad
* Sistemas de alarma
* Circuitos cerrados de televisión (CCTV)

## **2.1.2 Sistema de Acceso Lógico**

Por su parte, el control de acceso lógico se enfoca en la protección de sistemas informáticos, redes y datos. A través de la identificación, autenticación y autorización de usuarios, se busca restringir y monitorear el acceso a los recursos digitales de una organización.

Estas medidas incluyen el uso de nombres de usuario y contraseñas, autenticación de dos factores, tokens de seguridad y políticas de

encriptación, entre otras herramientas diseñadas para evitar la vulneración de la información.

### **Aspectos Cruciales del Control Lógico**

* Autenticación de usuarios
* Gestión de privilegios y roles
* Cifrado de datos
* Firewalls y sistemas de prevención de intrusiones
* Software de seguridad y antivirus
* Políticas de seguridad de la información

# **2.2 Tipos de control de acceso**

## **2.2.1 Principales funciones del control de acceso**

## **Identificación**

Este paso supone que la persona que desea acceder a las instalaciones es reconocida. Para ello, existen diferentes métodos que describiremos más abajo.

**Autenticación**

La autenticación se encarga de verificar si la persona que ha sido identificada tiene permiso para acceder a las instalaciones y, por tanto, forma parte de la base de datos de ese control de acceso concreto.

**Autorización**

El tercer paso determina si, en base a la identificación y la autenticación, se debe permitir el acceso a las instalaciones.

## **2.2.2 Tipos de control de acceso**

**Control de acceso por proximidad**

El control de acceso por proximidad es el que más se observa instalado en las empresas, ya que se activa con ayuda de una tarjeta o etiqueta. Se llama control de acceso por proximidad ya que se tiene que acercar la tarjeta o etiqueta al lector. El lector revisa los datos y abre la puerta.

La mayoría de las empresas, edificios gubernamentales y hospitales utilizan estos tipos de control de accesos porque sirven para controlar quién accede a áreas confidenta les o sensibles, además de que sirven para zonas de parking donde solo pueden estacionar ciertos vehículos.

**Control de acceso biométrico**

Los tipos de control de accesos biométricos tienen una seguridad alta porque permiten el acceso con datos físicos o conductuales, como las huellas dactilares. Para que este dispositivo funcione, recopila datos personales y luego los compara con una base de datos.

En esta base de datos están almacenados todos los datos de las personas autorizadas para acceder a una zona restringida. Si los datos coinciden con algunos de los que están dentro de la base de datos, el control de acceso biométrico entiende que estás autorizado.

**Control de acceso por reconocimiento facial**

El control de acceso por reconocimiento facial u ocular es otro de los tipos de control de accesos biométricos que existen en el mercado. Este dispositivo también se encarga de permitir el acceso a zonas restringidas valiéndose de la información física de la persona.

El objetivo del control de acceso por reconocimiento facial es almacenar los datos de los rostros u ojos para después compararlos con los datos que ya tiene guardados en la base de datos. Si el rostro u ojos coinciden con los que el sistema tiene registrados, permitirá el acceso.

**Capítulo 3: Desarrollo**

# **3.1 Requerimientos**

## **3.1.1 Requerimientos Funcionales:**

Gestión de Permisos de Acceso:

El sistema debe ofrecer un control de los permisos de acceso, permitiendo a los administradores configurar diferentes niveles de autorización para el personal. Cada usuario, basado en su rol o departamento, tendrá acceso restringido o permitido a ciertas áreas dentro de las instalaciones. Por ejemplo, los empleados de producción tendrán acceso únicamente a las áreas de manufactura, mientras que el personal administrativo podrá acceder a las oficinas y salas de juntas. Esta gestión debe ser flexible, lo que implica que se puedan actualizar los permisos rápidamente, de forma manual o a través de reglas predefinidas. Permitirá permisos para personal externo, como contratistas o visitantes, los cuales se mantendrá el registro de horas dentro de las instalaciones desde su ingreso asta su salida.

**Compatibilidad con Tarjetas:**

El software debe ser completamente compatible con las tarjetas Tarjeta MIFARE Classic / Tipo ISO Card, permitiendo realizar operaciones de lectura y escritura en estas tarjetas. El sistema deberá reconocer cuando una tarjeta es colocada en un lector compatible, decodificar los datos almacenados en el chip y validar dicha información mediante una base de datos interna para así tomar pase de lista, otorgar o denegar el acceso. Además de esto, el sistema deberá permitir la reprogramación de tarjetas, lo que implica que, en caso de cambio de rol o permiso de un usuario, la tarjeta podrá ser actualizada sin necesidad de reemplazo. La compatibilidad se realizara particularmente con aquellos lectores que se comunican a través de USB, y debe integrarse sin problemas con sistemas para asegurar la interoperabilidad entre dispositivos y software.

**Registro de Eventos y Auditoría:**

El sistema deberá registrar meticulosamente cada evento de acceso, proporcionando un log detallado que incluya la información del usuario, el área a la que intentó acceder, la fecha y la hora exacta del evento, y si el acceso fue concedido o denegado. Este registro no solo servirá para fines de auditoría interna, sino también como una herramienta útil en caso de incidentes de seguridad o investigaciones. Los informes de auditoría deben ser personalizables, permitiendo a los administradores filtrar eventos por fecha, usuario, área o tipo de incidente (por ejemplo, intentos de acceso fallidos).

## **3.1.2 Requerimientos No Funcionales:**

**Interfaz de Usuario:**

La interfaz del software debe ser intuitiva y fácil de usar, con especial énfasis en la accesibilidad y la usabilidad. Se debe diseñar pensando en usuarios que no necesariamente tengan conocimientos técnicos avanzados, como el personal de seguridad o administración. Esto significa que los elementos de la interfaz, como botones, menús y campos de texto, deberán ser grandes y claramente visibles, facilitando su uso. Además, se incluirá un sistema de ayuda interactiva, donde el usuario pueda acceder a guías o tutoriales directamente desde la aplicación.

**Rendimiento:**

El software debe ser capaz de procesar solicitudes de acceso en tiempo real, lo que significa que desde el momento en que un usuario presenta su tarjeta, el sistema debe validar la identidad y otorgar o denegar el acceso en un lapso de no más de 10 segundos. Esto es crucial para evitar cuellos de botella en áreas de alta afluencia, como entradas principales o puntos de control en zonas de producción. Además, el software debe ser capaz de manejar múltiples solicitudes simultáneamente, sin degradar el rendimiento. Esto implica que la infraestructura del sistema (servidores, base de datos, etc.) debe estar optimizada para soportar un alto volumen de transacciones sin interrupciones.

**Seguridad:**

Aunque el enfoque principal del proyecto no es la ciberseguridad, el sistema debe incorporar medidas de seguridad básicas para proteger la información sensible que maneja, como los datos personales. Esto incluye como la implementación de controles de acceso para la administración del sistema (por ejemplo, solo el personal autorizado podrá realizar cambios en la configuración del sistema o revisar los logs de auditoría). Además, se deben establecer políticas de contraseñas robustas y la posibilidad de activar autenticación de dos factores para los administradores del sistema. Aunque no se centrará en la ciberseguridad avanzada, estas medidas asegurarán que el sistema cumpla con las normativas básicas de protección de datos y seguridad de la información.

## **Requerimientos Técnicos:**

**Compatibilidad con Dispositivos de Acceso:**

El sistema deberá ser compatible dispositivos de acceso, principalmente aquellos que utilizan Tarjetas MIFARE Classic / Tipo ISO Card y se comunican mediante puertos USB. Esto garantiza que las tarjetas puedan ser leídas y programadas sin problemas. El software debe incluir controladores integrados o la capacidad de descargar e instalar controladores adicionales para soportar nuevos dispositivos si se añaden en el futuro. Esto garantiza que el sistema sea escalable y adaptable a medida que cambien las necesidades de la empresa o se actualicen los equipos de hardware.

**Capacidad de Almacenamiento:**

La base de datos del sistema debe ser lo suficientemente robusta para manejar usuarios simultáneos, almacenando información sobre las tarjetas, permisos de acceso. Además, el sistema debe ser capaz de manejar grandes volúmenes de registros de eventos sin pérdida de rendimiento. Se debe diseñar para que los datos más antiguos se archiven de manera eficiente o se puedan respaldar automáticamente en servidores externos para liberar espacio en la base de datos activa.