Plataforma para la gestión de riesgos ocupacionales bajo la normatividad colombiana existente

Omar David Ramírez Garzón, Kevin Alexander Alarcon Escandon, Karen Álvarez Bernal

Fundación Universitaria Compensar

Facultad de Ingeniería, Ingeniería de Sistemas

Bogotá, Colombia

2024



salus

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Agradecimientos

Queremos expresar nuestra más profunda gratitud a nuestros padres, quienes con su amor, paciencia y apoyo incondicional han sido nuestra fortaleza en este camino. A nuestros docentes, por guiarnos con su conocimiento y dedicación, enseñándonos no solo lecciones académicas, sino también valores que llevaremos con nosotros para siempre. Y a nuestros amigos, que estuvieron a nuestro lado en los momentos buenos y en los desafiantes, ofreciéndonos su compañía y ánimo.

Gracias a cada uno de ustedes por ser parte de esta etapa tan importante. Su apoyo ha sido fundamental para llegar hasta aquí.

Resumen

La implementación de una solución tecnológica para el Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST) es esencial para cumplir con el Decreto 1072 de 2015 en Colombia, al permitir una gestión estructurada y eficaz de los riesgos laborales. Esta tecnología es particularmente relevante en sectores con recursos limitados, como la construcción, la petroquímica, el transporte y las pymes, donde la administración de grandes volúmenes de datos resulta ineficiente con métodos tradicionales.

Estudios recientes destacan la importancia de herramientas digitales en el SGSST.) señalan que la capacitación y la digitalización mejoran la cultura de seguridad y la implementación del ciclo PHVA (Planear, Hacer, Verificar y Actuar), mientras que muestra que una plataforma tecnológica optimiza recursos y facilita el cumplimiento normativo. Investigaciones internacionales coinciden en que estas soluciones tecnológicas reducen la carga manual y mejoran la precisión de los registros, facilitando la toma de decisiones en tiempo real.

Para las pymes, esta digitalización representa una oportunidad de gestionar los riesgos de manera eficiente y organizada, sin un aumento significativo de costos. En conclusión, una solución tecnológica integral en el SGSST facilita la adaptación a cambios regulatorios, fortalece la cultura de seguridad y mejora el ambiente laboral, permitiendo a las empresas cumplir con la normativa y promover un entorno laboral seguro y saludable.

Abstract

The implementation of a technological solution for the Occupational Health and Safety Management System (SGSST) is essential to comply with Decree 1072 of 2015 in Colombia, by enabling structured and effective management of occupational risks. This technology is particularly relevant in sectors with limited resources, such as construction, petrochemicals, transportation and PYMES, where managing large volumes of data is inefficient with traditional methods.

Recent studies highlight the importance of digital tools in the SGSST) point out that training and digitization improve the safety culture and the implementation of the PHVA cycle (Plan, Do, Check and Act), while showing that a technological platform optimizes resources and facilitates regulatory compliance. International research agrees that these technological solutions reduce the manual burden and improve the accuracy of records, facilitating real-time decision making.

For PYMES , this digitization represents an opportunity to manage risks in an efficient and organized manner, without a significant increase in costs. In conclusion, a comprehensive technological solution in the SGSST facilitates adaptation to regulatory changes, strengthens the safety culture and improves the work environment, allowing companies to comply with regulations and promote a safe and healthy work environment.

Contenido

PÁG.

AGRADECIMIENTOS ..... **III**

RESUMEN ..... **V**

LISTA DE FIGURAS ..... **XI**

LISTA DE TABLAS ..... **XII**

INTRODUCCIÓN **1**

ANTECEDENTES Y JUSTIFICACIÓN **3**

ANTECEDENTES 3
JUSTIFICACIÓN 4

PLANTEAMIENTO DEL PROBLEMA **5**

DESCRIPCIÓN DEL PROBLEMA 5

OBJETIVOS **6**

OBJETIVO GENERAL 6
Objetivos Específicos *6*

ALCANCES Y LIMITACIONES **7**

MARCO TEÓRICO **9**

1.1 SOFTWARE EXISTENTE 9
1.2 13
1.2.1 SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SGSST) *13*
1.2.2 ACCIDENTE DE TRABAJO *18*
1.2.3 ENFERMEDAD LABORAL *19*
1.2.4 RIESGOS LABORALES *19*
1.2.5 SISTEMA DE GESTIÓN *20*
1.2.6 ARQUITECTURA DE SOFTWARE *21*
1.2.7 SEGURIDAD INFORMÁTICA *26*
1.2.8 CIBERSEGURIDAD *28*
1.2.9 INGENIERIA DE SOFTWARE Y DISEÑO DEL SOFTWARE *29*
1.3 MARCO LEGAL 31

METODOLOGÍA DE INVESTIGACIÓN **39**

2.1 *DESARROLLO DE SISTEMAS DE INFORMACIÓN BASADOS EN WEB* 39

2.2 ANALISIS METODOLOGÍAS PARA EL DESARROLLO DE SOFTWARE WEB 40
2.2.1 DEFINICIÓN *40*
2.2.2 ANÁLISIS *40*

DESARROLLO DEL PROYECTO **44**

3.1 LEVANTAMIENTO DE *REQUERIMIENTOS* 44
3.1.1 Requerimientos Funcionales *44*
3.1.2 Requerimientos No Funcionales *50*
3.2 ROLES, RESPONSABILIDADES Y PERMISOS 52
3.3 SCRITP DE LA BASE DE DATOS 53
3.4 DESCRIPCIÓN CASOS DE USO 64
3.5 DIAGRAMAS 70
3.5.1 Diagramas de Casos de Uso *70*
3.5.2 Diagrama de Clases *76*
3.5.3 Diagrama Base de Datos *77*
3.5.4 Diagrama de procesos *77*
3.6 VISTA DEL SOFTWARE 79

CONCLUSIONES **86**

BIBLIOGRAFÍA **87**

Lista de figuras

PÁG.

Figura 1Elementos de una Gestión Salud y Seguridad Ocupacional (Castillo , 2015) 13
Figura 2 Ciclo Del Proceso De Mejoramiento Continuo De Salud Y Seguridad Ocupacional (Castillo , 2015) 14
Figura 3 Patrón cliente-servidor (OpenWebinars S.L, 2022) 22
Figura 4 Patrón de capas (OpenWebinars S.L, 2022) 23
Figura 5 Patrón master-slave (OpenWebinars S.L, 2022).....23
Figura 6 Patrón modelo-vista-controlador (MVC) (OpenWebinars S.L, 2022).....24
Figura 7 Patrón broker (OpenWebinars S.L, 2022).....25
Figura 8 Fases del ciclo de vida de un software.....30
Figura 9 Fases de la metodología ICDM (Kosasi, 2016) 41
Figura 10 Login.....70
Figura 11 Gestión de Eventos 70
Figura 12 Gestión de diagnostico.....71
Figura 13 Gestión Factor de Riesgo 71
Figura 14 Gestionar alta médica 72
Figura 15 Gestionar recomendaciones 72
Figura 16 Gestionar restricciones 73
Figura 17 Gestionar Seguimiento 73
Figura 18 Gestionar reubicación.....74
Figura 19 Gestionar Incapacidad. 74
Figura 20 Gestionar Evaluación. 75
Figura 21 Gestionar Reportes 75
Figura 22 Diagrama de Clases 76
Figura 23 Diagrama Base de Datos 77
Figura 24 Login.....79
Figura 25 Interfaz de inicio.....79
Figura 26 Dashboard 80
Figura 27 Registro de Empleados 80
Figura 28 Lista de Empleados 81
Figura 29 Registrar Accidente.....82
Figura 30 Registrar Accidente.....83
Figura 31 Lista de Accidentes.....84

Figura 32 Registro de Usuarios 84

Lista de tablas

PÁG.

Tabla 1 Software de gestión para prevención de riesgos laborales. 11
Tabla 2. Software de gestión para formación de riesgos laborales 12
Tabla 3 .Software de asesoramiento y auditoria 12
Tabla 4 Registro y autenticación de usuarios 44
Tabla 5 Asignación de roles y privilegios.....45
Tabla 6 Control de acceso basado en roles.....46
Tabla 7 Gestión de contraseñas seguras y políticas de contraseña.....47
Tabla 8 Alertas automáticas ante actividades sospechosas.....47
Tabla 9 Registro de logs para auditoría y análisis forense.....48
Tabla 10 Control de acceso a datos sensibles 49
Tabla 11 Escalabilidad.....50
Tabla 12 Rendimiento 50
Tabla 13 Usabilidad 51
Tabla 14 Disponibilidad.....51
Tabla 15 Compatibilidad 51
Tabla 16 Portabilidad 51
Tabla 17 Accesibilidad.....51
Tabla 18 Login.....64
Tabla 19 Gestión Eventos.....65
Tabla 20 Gestionar Diagnostico 65
Tabla 21Gestionar Factores de Riesgos.....66
Tabla 22 Gestionar alta médica. 66
Tabla 23 Gestionar recomendaciones. 67
Tabla 24 Gestionar restricciones. 67
Tabla 25 Gestionar Seguimiento.....68
Tabla 26 Gestionar Reubicación 68
Tabla 27 Gestionar Incapacidad. 69
Tabla 28 Gestionar Evaluación. 69
Tabla 29 Gestionar Reportes.....69

Introducción

La adopción de soluciones tecnológicas para la gestión del Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST) ha ganado importancia en Colombia, sobre todo a partir del Decreto 1072 de 2015, que obliga a las empresas a implementar un sistema efectivo de control de riesgos laborales. Esta normativa es clave para reducir accidentes y enfermedades ocupacionales, alineándose con el compromiso del Ministerio de Trabajo en fortalecer la seguridad y el bienestar de los trabajadores en todos los sectores.

Digitalizar los procesos del SGSST permite un control de riesgos más ágil y preciso, lo cual es vital en sectores como la construcción, la petroquímica, el transporte y en pymes, donde los recursos suelen ser limitados y las necesidades de manejo de datos son amplias y complejas. En estos contextos, el uso de herramientas tradicionales, como Excel, puede quedarse corto al enfrentar la complejidad y volumen de información, lo que incrementa el riesgo de errores, inconsistencias y falta de seguimiento adecuado.

Diversos estudios respaldan la efectividad de las soluciones tecnológicas en la gestión del SGSST. En su investigación con Calzado Anyelme S.A.S., Castilla (2021) subraya la importancia de capacitar a todo el personal en SGSST y de fomentar una cultura de seguridad que abarque tanto áreas administrativas como operativas. Castilla destaca que la digitalización no solo ayuda a cumplir la normativa, sino que facilita la unificación de conocimientos y prácticas en toda la organización. Por su parte, Ávila (2021) analizó el ciclo PHVA (Planear, Hacer, Verificar, Actuar) en el manejo de riesgos y propuso un plan anual apoyado en herramientas tecnológicas para mejorar la recolección de datos y la supervisión. Otro ejemplo es la plataforma de Jiménez (2024) para un laboratorio en el sector petroquímico, que optimizó el uso de recursos y redujo costos en personal, además de mejorar el cumplimiento regulatorio.

La digitalización también permite implementar dashboards interactivos que monitorean en tiempo real indicadores clave de seguridad laboral, detectando patrones de riesgo y áreas de mejora. Estas herramientas incluyen alertas automáticas y notificaciones que permiten una respuesta rápida en caso de incidentes. Para las pymes, que suelen contar con recursos

limitados, la digitalización del SGSST representa una forma organizada y económica de cumplir con la normativa y optimizar el entorno laboral sin generar una carga financiera importante.

Además, tecnologías como el Internet de las Cosas (IoT) y la inteligencia artificial (IA) están transformando la seguridad y salud laboral. Sensores conectados permiten monitorear en tiempo real factores como la temperatura o la presencia de sustancias peligrosas en espacios de alto riesgo. La IA, por su parte, permite analizar grandes volúmenes de datos para identificar tendencias y prever posibles riesgos, lo cual es clave para prevenir accidentes y planificar la seguridad laboral.

Las aplicaciones móviles también representan un avance importante, ya que permiten a los trabajadores reportar de inmediato incidentes o condiciones inseguras. Estas herramientas, junto con los dashboards, crean un flujo de información constante en todos los niveles de la organización, mejorando la capacidad de respuesta y optimizando la toma de decisiones. Este tipo de soluciones resulta particularmente útil en industrias con entornos laborales cambiantes, como la construcción o el sector energético.

En conclusión, el desarrollo de soluciones tecnológicas integrales para el SGSST es esencial para que las empresas en Colombia se mantengan en línea con el Decreto 1072 de 2015 y promuevan ambientes de trabajo seguros y saludables. La integración de estas herramientas facilita la adaptación a cambios regulatorios, fortalece la cultura de seguridad y permite implementar el ciclo PHVA de forma continua y ajustada a las necesidades particulares de cada empresa. A la vez, estas soluciones contribuyen al bienestar de los trabajadores, al desarrollo organizacional y al desempeño en seguridad, reduciendo incidentes y enfermedades, evitando sanciones y fomentando un entorno laboral seguro y eficiente.

Antecedentes y Justificación

Antecedentes

Según el ministerio de trabajo se estableció Sistema de gestión de seguridad y salud en el Trabajo-Ministerio de Trabajo “SG-SST”, el cual debe ser implementado por los empleadores el cual consiste en el desarrollo de un proceso lógico y por etapas basado en la mejora continua, aplica para todo tipo de organizaciones el cual fue determinado por el decreto 1072 de 2015, (2024).

Por otra parte, se realizó una investigación denominada Sistema de Gestión de Seguridad y Salud en el Trabajo en la empresa Calzado Anyelme s.a.s constituido principalmente en conocer principal el estado actual de las áreas administrativas y operativas, lo cual permite que logren el cumplimento de existente en la temática y se genere mayor conocimiento en los empleados, Castilla (2021).

Asimismo, Ávila (2021) con la investigación realizada buscaba proporcionar a la empresa un documento organizado con los hallazgos del ciclo PHVA del SG-SST, para cumplir con la normativa legal y desarrollar medidas de intervención contra riesgos laborales. Se verificó la normativa vigente, se evaluaron los riesgos y se establecieron objetivos para cubrir todos los niveles de la organización. El proceso de investigación mixto incluyó información cuantitativa y cualitativa, resultando en una carpeta digital con instrumentos y un plan anual de trabajo para fortalecer los procesos del SG-SST.

Por otro lado, el proyecto de Jiménez (2024), se enfoca en analizar y gestionar los riesgos laborales en un laboratorio de control industrial de una empresa petroquímica. La evaluación de riesgos actual está desactualizada, por lo que se busca actualizarla y establecer medidas de control a través de acciones correctivas y preventivas. Se desarrolla una plataforma unificada que facilita la evaluación de riesgos laborales, mostrando que solo el 42% requiere intervención, con diferentes niveles de acción necesarios. Se implementan medidas para mejorar la seguridad y salud laboral, logrando actualizar la evaluación de riesgos y garantizando un entorno laboral más seguro que puede ser replicado en otras organizaciones.

Por otra parte, Silva (2023) realizo el analiza sobre situación actual de Paraguay, en relación con la seguridad y salud laboral en la construcción, y se observan las deficiencias del sistema en general y en cuanto a empresas de construcción y las obras.

Trujillo (2024), realizo un estudio denominado *análisis de riesgos ocupacionales en el desplazamiento del personal de salud*, se aborda la pregunta científica sobre los riesgos laborales asociados al transporte de trabajadores del centro de salud Jambi Huasi, ubicado en Puerto Francisco de Orellana. Los resultados muestran una distribución de frecuencias de exposición a riesgos biológicos en distintos niveles, siendo el nivel "Medio" el más frecuente, con 27 casos, lo que representa el 45% del total de observaciones.

Justificación

La gestión de la Seguridad y Salud en el Trabajo (SST) es fundamental para asegurar tanto el bienestar de los empleados como el cumplimiento de la normativa vigente en Colombia. En el caso de las pequeñas y medianas empresas (pymes) de Bogotá, la falta de una solución eficiente para la gestión de riesgos laborales ha generado un problema crítico. Este no solo compromete la seguridad de los trabajadores, sino que también expone a las empresas a sanciones legales y pone en riesgo su operatividad.

El Decreto 1072 de 2015 establece obligaciones específicas para las empresas en cuanto a SST, pero muchas pymes aún dependen de herramientas limitadas, como Excel, para registrar accidentes laborales y gestionar la información relacionada. Esto no solo dificulta el análisis detallado de los datos, sino que también impide la detección temprana de riesgos, lo cual se traduce en una ausencia de medidas preventivas eficaces.

Frente a este panorama, la creación de un prototipo funcional para gestionar los riesgos ocupacionales en las pymes bogotanas se justifica plenamente. Este sistema permitiría una gestión más eficiente, dinámica y conforme a la normativa vigente. Además de mejorar el cumplimiento legal, contribuiría directamente a la prevención de accidentes y a la mejora de las condiciones laborales. A largo plazo, esto impactaría positivamente en la productividad y sostenibilidad de las empresas.

En resumen, este proyecto busca dotar a las pymes de una herramienta tecnológica adecuada para optimizar la gestión de la SST, mejorar las condiciones laborales de sus empleados y asegurar el

cumplimiento de la normativa colombiana. Así, se minimizaría el riesgo de sanciones y se promovería una cultura de prevención y seguridad en el entorno laboral.

Planteamiento del Problema

Descripción del Problema

La mayoría de las pequeñas y medianas empresas (pymes) en Colombia enfrentan un desafío importante: carecen de una solución tecnológica adecuada para gestionar de manera eficiente la información sobre los accidentes laborales de sus empleados. Esta falta de herramientas limita el cumplimiento normativo y dificulta la gestión efectiva de la Seguridad y Salud en el Trabajo (SST). Actualmente, muchas empresas registran estos incidentes utilizando archivos de Excel, un método que no solo resulta ineficiente para manejar grandes volúmenes de datos a lo largo del tiempo, sino que también carece de la automatización necesaria para evitar errores humanos y mantener los datos actualizados.

Además, la información sobre accidentes laborales suele estar dispersa en distintas áreas de la empresa, lo que dificulta su integración y análisis oportuno. Esta dispersión impide la identificación temprana de patrones o factores de riesgo, limitando la capacidad de implementar medidas preventivas de manera eficaz. La falta de un sistema especializado también dificulta la adaptación a los cambios normativos, como los establecidos en el Decreto 1072 de 2015, exponiendo a las empresas a sanciones legales y afectando su operatividad.

La gestión manual de la SST no solo complica la generación de reportes detallados, sino que también impide el análisis estadístico profundo. Esto limita la toma de decisiones basada en datos y afecta la implementación de medidas preventivas para mejorar la seguridad en el entorno laboral. Estas deficiencias no solo repercuten en el cumplimiento normativo, sino también en la productividad y los costos operativos, ya que el incumplimiento puede resultar en multas, sanciones y pérdida de productividad debido a accidentes laborales.

En conclusión, la falta de una solución tecnológica adecuada para gestionar los accidentes laborales pone en riesgo tanto la estabilidad operativa y financiera de las pymes como el bienestar de sus trabajadores. Esto hace imprescindible la implementación de un software especializado que facilite un control integral y dinámico de la SST, garantizando así un entorno laboral más seguro y eficiente.

Formulación del Problema

¿De qué forma se pueden mejorar los procesos de gestión de sistemas de seguridad y salud en el trabajo bajo la normatividad colombiana existente en las empresas?

Objetivos

Objetivo General

Desarrollar un prototipo funcional para gestión de riesgos ocupacionales en Pymes Bogotanas bajo la normatividad existente.

Objetivos Específicos

- Analizar los requerimientos funcionales y no funcionales que permitan el funcionamiento del sistema de visualización para gestión de riesgos ocupacionales.
- Aplicar los principios de la ingeniería en sistemas para el modelamiento de datos y la estructuración lógica del sistema como fundamento principal en el desarrollo de la aplicación.
- Validar el prototipo funcional con el fin determinar la mejora en el proceso de PRL.

Alcances y Limitaciones

El proyecto tiene como objetivo desarrollar un prototipo tecnológico integral que permita innovar la gestión de riesgos ocupacionales en Pymes Colombianas. Este sistema será diseñado para cubrir varios aspectos clave:

1. Gestión de Información: La plataforma permitirá la recolección, tabulación y análisis de datos relacionados con la accidentalidad laboral, facilitando el seguimiento detallado de cada incidente y la evolución médica de los empleados afectados.

2. Optimización de Procesos: A través de la integración de distintas soluciones de software, la plataforma ofrecerá un control estadístico robusto, permitiendo identificar factores de riesgo y áreas de mejora en tiempo real. Esto contribuirá a la reducción de incidentes y mejorará la toma de decisiones en materia de seguridad laboral.

3. Cumplimiento Normativo: La herramienta asegurará que la empresa cumpla con los requerimientos legales estipulados en el Decreto 1072 de 2015, minimizando el riesgo de sanciones y promoviendo un entorno laboral seguro y saludable.

Marco Teórico

1.1 Software Existente

A continuación, se describen las características y funciones fundamentales de diverso software, los cuales son los más utilizados en las organizaciones para la prevención de riesgos laborales. Estos aparecen clasificados según su área de aplicación, así:

a) Software de prevención de riesgos.

Está diseñado para gestionar y mitigar los riesgos laborares, promoviendo la seguridad de los empleados y el cumplimiento normativo, algunas de las funciones más comunes son: gestión de riesgos laborales, auditorías e inspecciones, gestión de incidentes y accidentes, capacitación y formación, cumplimiento normativo, reportes y análisis.

b) Software formación en riesgos laborales.

Está diseñado para gestionar y realizar un seguimiento de la capacitación y el desarrollo de los empleados en temas relacionados con la seguridad laboral. Este tipo de herramientas suele ser fundamental para garantizar que los trabajadores reciban la formación necesaria para identificar y mitigar riesgos en el lugar de trabajo, algunas de las funciones mas comunes son: gestión de programas de formación, seguimiento del progreso, certificación y documentación, e-learning, evaluaciones, cumplimiento normativo, informes y análisis.

c) Software asesoramiento y auditoria

Facilita la evaluación de riesgos, el cumplimiento normativo, la realización de auditorías de seguridad y la consultoría en materia de prevención de riesgos laborales. Estas herramientas son esenciales para identificar deficiencias en el sistema de gestión de la seguridad, hacer un seguimiento de las medidas correctivas y garantizar que las empresas cumplan con las normativas legales, algunas de sus funciones claves son: gestión de auditorías, evaluación de riesgos, automatización de procesos, planes de acción y seguimiento, cumplimiento normativo, generación de informes, consultoría virtual, historial y registros de auditoría.

Nombre	Empresa Responsable	Función /Característica
PrevGes	ReM Informática	Software o Programa de Gestión de Prevención de Riesgos Laborales compuesto de los módulos: agenda, plantilla, consulta, evaluación de riesgos, incidentes, estadísticas, control de mantenimiento, imagen, subcontratas y productos peligrosos. (Club REM , 2024) Personaliza la documentación. Importe la información de otras Bases de Datos. Multiusuario y trabaje simultáneamente. Busque registros fácilmente. Módulos diferenciados por colores.
SISPRO	Ministerio de salud y protección social	El Sistema Integral de Información de la Protección Social (SISPRO) es una plataforma diseñada para consolidar y procesar datos del sector de la protección social. Su objetivo es facilitar la toma de decisiones, la formulación de políticas, el monitoreo regulatorio y la gestión de servicios, proporcionando información sobre aseguramiento, financiamiento, y uso de servicios, accesible al público. El SISPRO está compuesto por instituciones, normativas y procesos tecnológicos que regulan los derechos y deberes en el sector. Su estructura se basa en una Bodega de Datos que integra información de múltiples fuentes, permitiendo la elaboración de indicadores y reportes útiles para toda la ciudadanía (Gov.co, 2024).
Nexus Safety	Nexus defining safety	Nexus Safety Solutions Pvt Ltd ofrece tecnologías innovadoras, fiables y de calidad, centradas en el avance tecnológico. Se especializa en diseñar productos y servicios que mejoran la seguridad de personas y bienes. La empresa personaliza, instala y mantiene soluciones de alta calidad, adaptadas a las necesidades del cliente (Nexussafety.net, 2021).
SAP EHS	SAP	Es la gestión de medioambiente, salud y seguridad garantiza un entorno laboral seguro, minimice riesgos y cumpla con

		normativas con SAP EHS Management. Sus aplicaciones permiten reducir el impacto ambiental y proteger a los empleados. Ofrece implementación on-premise o en la nube, integración con otras soluciones de SAP, y sirve como fuente de datos clave para la sostenibilidad, en una plataforma modular y unificada (Sap.com, 2024).
PYMES ON LINE	PYMES ON LINE	Ofrece asesoría, capacitación, auditoría y herramientas tecnológicas para implementar protocolos que mejoren la calidad de vida de los trabajadores y reduzcan costos por accidentes y ausentismo. Su software en la nube permite gestionar documentos de manera segura desde cualquier lugar, y su software de gestión de proyectos facilita el seguimiento en tiempo real de la implementación y continuidad del Sistema de Seguridad y Salud en el Trabajo (Pymes On Line , 2020).

Tabla 1 Software de gestión para prevención de riesgos laborales.

Nombre	Empresa Responsable	Función /Característica
EdApp	SC Training	Una plataforma de micro aprendizaje que permite crear módulos cortos y efectivos para la formación en seguridad y salud en el trabajo. También cuenta con una librería de cursos prediseñados sobre SST (SC Training , 2024)
TalentLMS	TalentLMS	Este sistema de gestión de aprendizaje es popular para formar a los empleados en diversos temas, incluida la SST. Tiene capacidades para personalizar el contenido, hacer seguimiento y emitir certificaciones (TalentLMS, 2024).
Moodle	Moodle	Una plataforma de código abierto que permite a las empresas personalizar sus cursos y hacer un seguimiento detallado del progreso de los empleados en SST. Se puede adaptar para ofrecer formación específica en riesgos laborales (Moodle LMS , 2024).

360Learning	360Learning	Ofrece una plataforma colaborativa de aprendizaje que puede ser utilizada para desarrollar y gestionar la formación en SST, incluyendo funcionalidades de e-learning y reportes detallados, también utiliza una int6eligencia artificial (360learning, 2024).

Tabla 2. Software de gestión para formación de riesgos laborales

Nombre	Empresa Responsable	Función /Característica
Cority	Cority empowen letten	Es una solución integral de gestión de SST que incluye módulos para auditorías y consultoría. Facilita la identificación de riesgos, la planificación de auditorías, el seguimiento del cumplimiento y la generación de informes detallados (Cority , 2023).
Intelex	Intelex	Es un software especializado en la gestión de riesgos y auditorías de SST. Permite realizar auditorías personalizadas, gestionar no conformidades y generar informes detallados para identificar áreas de mejora. Está diseñadas para expertos en EHSQ por expertos en EHSQ (Intelex, 2024).
EcoOnline	EcoOnline	Ofrece una solución para gestionar las auditorías de SST con listas de verificación personalizables, generación automática de informes, seguimiento de acciones correctivas y cumplimiento normativo. Está diseñado para mejorar la eficiencia y precisión de las auditorías (EcoOnline, 2024).
Qualsys	Qualsys	Es un software de gestión de calidad también incluye módulos para auditorías y cumplimiento en SST. Facilita la creación de auditorías, la evaluación de riesgos y la gestión del ciclo de vida completo de las no conformidades (Qualys, 2024).

Tabla 3 .Software de asesoramiento y auditoria

Este apartado presenta investigaciones sobre software para la gestión de riesgos ocupacionales y la accidentalidad laboral, haciendo hincapié en el desarrollo y la implementación de estas tecnologías con el objetivo de beneficiar al sector empresarial. En particular, se destaca su

relevancia para organizaciones cuyos sectores económicos están enfocados en los servicios, el comercio y la industrialización.

A partir de las investigaciones, se identifican las siguientes características comunes en la mayoría de estas aplicaciones:

- Son complejas para el usuario final.
- Tienen costos elevados.
- Están diseñadas para manejar un solo campo de acción y no son escalables.
- Están orientadas a la web.
- Requieren experiencia y capacitación para su uso adecuado.
- Se alinean con el Sistema de Gestión de la Calidad.
- Ofrecen reportes y estadísticas que facilitan la toma de decisiones.

1.2

A continuación, se describen los aspectos clave para comprender la teoría necesaria para el desarrollo del proyecto, entre los cuales se incluyen la estructura, las características, la clasificación y las funciones. Estos elementos son fundamentales para establecer una base sólida que guíe el diseño y desarrollo del proyecto.

1.2.1 *SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SGSST)*

El Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) abarca una disciplina orientada a prevenir lesiones y enfermedades causadas por las condiciones laborales, mediante el desarrollo de un proceso lógico y por etapas, basado en la mejora continua Gov.co, (2021).Este apartado incluye los requisitos generales para el establecimiento de dicho sistema, contemplando la estructura organizacional, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos necesarios para desarrollar, implementar, cumplir, revisar y mantener la política y los objetivos del SG-SST.

Figura 1Elementos de una Gestión Salud y Seguridad Ocupacional (Castillo , 2015)

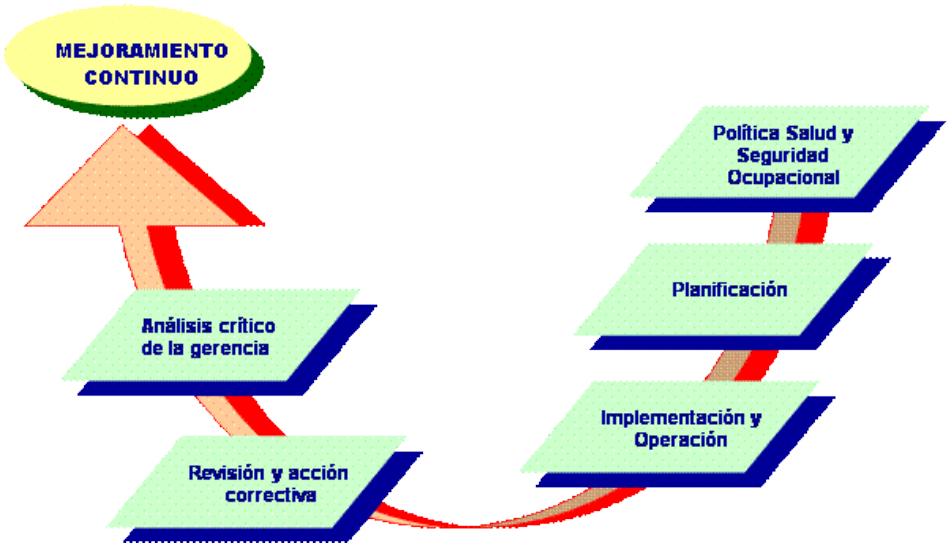
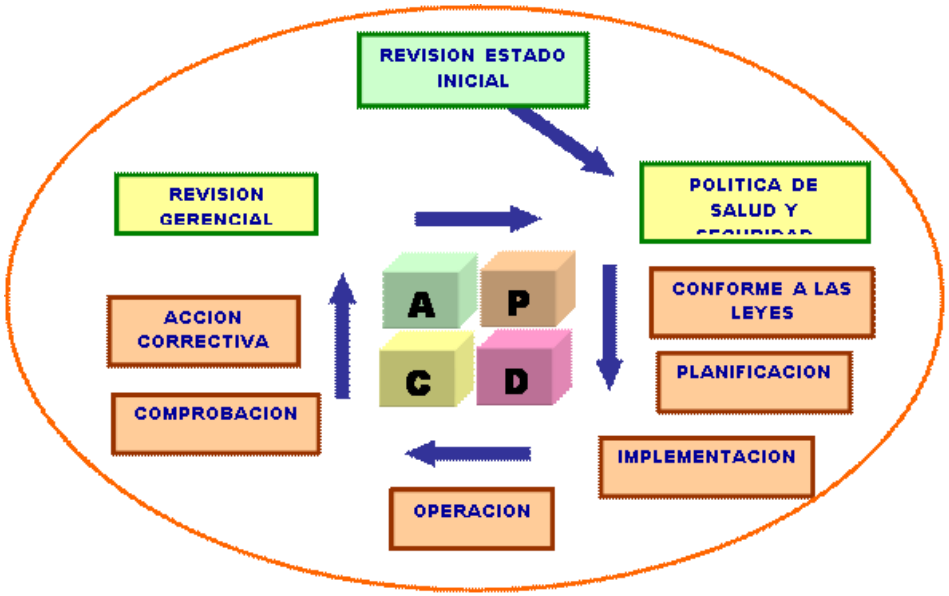


Figura 2 Ciclo Del Proceso De Mejoramiento Continuo De Salud Y Seguridad Ocupacional (Castillo , 2015)



En los anteriores gráficos (Figura 1, Figura 2) se observan elementos y las etapas para desarrollar el sistema de gestión SGSST, a continuación, se presenta una breve descripción de cada uno de los elementos que componen el sistema de gestión

1.2.1.1 POLÍTICA DEL SISTEMA DE GESTIÓN DE SALUD Y SEGURIDAD OCUPACIONAL

La política del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) de la empresa contratista constituye el punto de partida esencial para la correcta implementación del sistema.

Este enfoque está alineado con normas internacionales como ISO 9000, ISO 14000 y OHSAS 18001, lo que implica que la empresa contratista debe elaborar su política conforme al esquema descrito en la Figura 2.

Esta política debe ser desarrollada considerando los efectos del entorno laboral y el nivel de seguridad requerido, basándose en un análisis detallado que permita identificar los riesgos y establecer las medidas de control adecuadas a las necesidades de la organización. Así se garantiza que el sistema esté alineado con las regulaciones vigentes y las particularidades del ambiente laboral. (Castillo , 2015)

Por otro lado, la política de SG-SST debe cumplir con los siguientes puntos clave:

Adaptarse a la naturaleza, visión, misión, objetivos y nivel de riesgo que enfrentan los trabajadores.

Incluir un compromiso explícito de mejora continua.

- Cumplir de las leyes vigentes en materia de Seguridad y Salud en el Trabajo.
- Estar documentada y ser revisada periódicamente para asegurar su cumplimiento.
- Ser comunicada a todos los empleados, para que comprendan sus responsabilidades en cuanto a la seguridad y salud ocupacional.

Estos lineamientos aseguran que la política esté en concordancia con las mejores prácticas internacionales, además de promover un entorno de trabajo seguro y en cumplimiento con las normativas legales.

1.2.1.2 *PLANIFICACIÓN*

En el Sistema de Gestión de Salud y Seguridad Ocupacional implica organizar de manera adecuada quién, cómo y cuándo se deben realizar las acciones, basándose en los resultados de una revisión inicial. Se establecen objetivos y metas tanto para todo el sistema como para cada nivel operativo, asignando prioridades, plazos, recursos y medios en función de las responsabilidades y la integración con otros sistemas de gestión.

Es fundamental definir un procedimiento dentro del sistema, que regule la planificación de estos objetivos y metas, adaptado a la naturaleza de la empresa y del propio sistema. Este procedimiento parte de dos etapas clave: una revisión inicial de la acción preventiva y una evaluación inicial de los riesgos. (Castillo , 2015)

1.2.1.3 IMPLEMENTACIÓN Y OPERACIÓN

La empresa contratista debe desarrollar una estructura administrativa que permita implementar el sistema de gestión de salud y seguridad ocupacional (SG-SST) y asignar los recursos necesarios para su funcionamiento. El responsable de seguridad y salud ocupacional coordina y audita el sistema. Al igual que en la gestión de calidad, se requiere un manual que defina las responsabilidades de los actores y los estándares a cumplir.

- Los documentos clave del sistema incluyen:
- Política y programa de SG-SST.
- Legislación y normativa aplicable.
- Manual de SG-SST.
- Procedimientos de trabajo para puestos con riesgos elevados.
- Plan de emergencias.

Estos documentos deben ser accesibles, legibles, revisados periódicamente y actualizados según sea necesario. El plan de emergencias debe incluir la asignación de responsabilidades, distribución y comunicación, adaptándose a cambios como la rotación de personal.

La comunicación debe ser tanto interna como externa, por ejemplo, para abordar quejas del personal (comunicación interna) o de la comunidad (comunicación externa).

El entrenamiento debe abarcar a todo el personal y contratistas, cubriendo temas como la identificación de riesgos, uso de equipos de protección personal, procedimientos de seguridad y respuestas ante emergencias. Además, debe haber reentrenamiento periódico, documentado mediante un registro de capacitaciones.

El entrenamiento no solo desarrolla habilidades, sino que fomenta la conciencia de seguridad entre los trabajadores al comprender los riesgos ocupacionales. También debe cubrir roles y responsabilidades dentro del sistema de gestión.

En cuanto al control operacional, el supervisor es clave y debe asumir su responsabilidad. Los contratistas representan un punto crítico, y su incumplimiento de las normas de seguridad debe contemplar sanciones en los contratos de servicio.

Finalmente, la gestión de emergencias es un aspecto crucial. El plan de emergencias debe incluir procedimientos para situaciones como fugas de sustancias tóxicas, incendios, explosiones y desastres naturales. (Castillo , 2015)

1.2.1.4 ACCIÓN CORRECTIVA

El control en el sistema de seguridad y salud ocupacional es esencial para evaluar la exposición de los trabajadores al ambiente laboral y controlar las variables que la afectan. Esto incluye controles ambientales, biológicos y psicológicos. Una vez que se planifican y ejecutan las acciones (Plan y Do), se verifica si los resultados coinciden con lo previsto (Check). Si no es así, se implementan acciones correctivas (Act), lo que permite mejorar el sistema continuamente. La detección de no conformidades impulsa acciones preventivas y correctivas mediante la investigación de las causas. El control asegura que se cumplan los objetivos del sistema, garantizando el cumplimiento de los requisitos y la minimización del impacto laboral en la salud. Este proceso también verifica si las actividades realizadas cumplen con los procedimientos establecidos (Castillo , 2015).

Control activo

El control activo se realiza antes de que ocurra un accidente o enfermedad laboral, evaluando la eficacia de las actividades preventivas. Este tipo de control refuerza los aciertos y corrige los errores sin penalizar. Los programas de control deben supervisar la implementación de recomendaciones, verificar la eficacia de las medidas correctivas, y evaluar nuevos sistemas, procesos o equipos. Se basan en registros que incluyen accidentes, enfermedades, exámenes médicos, monitoreo ambiental, entrenamientos y equipos de seguridad.

Verificación

La verificación implica procedimientos para confirmar que se cumplen los requisitos del sistema de gestión de seguridad y salud ocupacional. Estos procedimientos deben mantenerse actualizados y proporcionar información sobre el nivel de riesgo existente. Las inspecciones y mediciones son herramientas clave para verificar el cumplimiento.

Control reactivo

El control reactivo se activa después de incidentes o accidentes laborales. Se centra en analizar, registrar e informar sobre los eventos, desde daños menores hasta reclamaciones de seguros o incendios. Con esta información, se evalúa la efectividad de los procedimientos existentes y se implementan medidas correctivas necesarias para prevenir futuros incidentes.

En resumen, los controles proactivos y reactivos son esenciales para mantener un entorno de trabajo seguro y para la mejora continua del sistema de gestión de seguridad y salud ocupacional.

1.2.1.5 REVISIÓN GERENCIAL

Es fundamental realizar una revisión periódica del sistema de gestión de seguridad y salud ocupacional para identificar puntos débiles en el cumplimiento y aplicar medidas correctivas. En la última fase del ciclo de mejora, la Dirección debe asumir la responsabilidad de evaluar las acciones realizadas en un período determinado. Esto incluye verificar el cumplimiento de la política, la prevención de riesgos laborales, y los objetivos de mejora. La evaluación debe basarse en los resultados obtenidos, considerando cambios en las circunstancias y el compromiso con la mejora continua (Castillo , 2015).

La revisión debe abarcar toda la organización y sus actividades, e incluir:

Recomendaciones de las auditorías y cómo implementarlas.

Garantizar que la política de prevención sigue siendo adecuada, y si requiere modificaciones, justificar claramente los motivos.

Asegurar que los objetivos y metas se ajusten al compromiso de mejora continua y al programa de gestión preventiva, según lo estipulado en la documentación.

Este proceso asegura que la organización se mantenga alineada con sus metas preventivas y en constante mejora.

1.2.2 ACCIDENTE DE TRABAJO

Es un suceso inesperado relacionado con el trabajo que causa lesión, invalidez o muerte al trabajador. También incluye incidentes ocurridos durante el cumplimiento de órdenes del empleador, aunque sucedan fuera del lugar o horario laboral. Las legislaciones de cada país definen estos casos de manera específico (Gov.Co, 2024) .Según el artículo 30 de la ley 1562 de 2012 es un evento inesperado relacionado con el trabajo que causa una lesión física, perturbación funcional, invalidez o muerte al trabajador. También se incluye el que ocurre durante la ejecución de órdenes del empleador, incluso fuera del lugar y horario laboral. Además, se considera accidente de trabajo aquel que sucede durante el traslado entre el hogar y el trabajo, si el transporte es proporcionado por el empleador.

Asimismo, los accidentes durante actividades sindicales, recreativas, deportivas o culturales también se consideran accidentes de trabajo, siempre que el trabajador actúe en representación o

por cuenta del empleador o de la empresa usuaria, en el caso de trabajadores temporales en misión, CORZO ROMÁN y otros,(2024).

1.2.3 ENFERMEDAD LABORAL.

En Colombia está definida en el artículo 4 de la Ley 1562 de 2012, la cual modifica el Sistema de Riesgos Laborales. Se considera enfermedad laboral aquella que surge por la exposición a factores de riesgo propios del trabajo o del entorno en que el trabajador desempeña su labor. El Gobierno Nacional actualiza periódicamente la lista de enfermedades laborales, y si una enfermedad no está en la tabla pero se demuestra su relación con los riesgos laborales, será reconocida como tal.

Además, el artículo 142 del Decreto Ley 019 de 2012 establece que entidades como Colpensiones, ARP y EPS deben calificar la pérdida de capacidad laboral y el grado de invalidez. Si el afectado no está de acuerdo, puede solicitar una revisión ante las Juntas Regionales de Calificación de Invalidez, cuya decisión puede ser apelada ante la Junta Nacional.
El Decreto 1477 de 2014 introduce la Tabla de Enfermedades Laborales y regula aspectos relacionados con la relación de causalidad, prestaciones económicas y vigencia de la norma, garantizando que las enfermedades laborales y sus consecuencias se gestionen de acuerdo con los estándares legales (Gov.co, 2024).

1.2.4 RIESGOS LABORALES

La Subdirección de Riesgos Laborales del Ministerio de Salud y Protección Social es responsable de desarrollar las políticas del Sistema Nacional de Riesgos Laborales y de coordinar con la Dirección de Riesgos Laborales del Ministerio del Trabajo. Sus funciones incluyen:

- Establecer mecanismos de afiliación al Sistema General de Riesgos Laborales.
- Definir el uso de los sistemas de información para la afiliación.
- Proponer prestaciones en salud relacionadas con riesgos laborales.
- Emitir conceptos técnicos dentro de su área de competencia.
- Apoyar el Sistema Integrado de Gestión Institucional y cumplir con sus recomendaciones.

Además, gestiona indicadores y cifras del sector, el Sistema de Afiliación Transaccional (SAT), y licencias de seguridad y salud en el trabajo (Gov.co, 2024).

1.2.5 SISTEMA DE GESTIÓN

Un sistema de gestión describe cómo las empresas organizan sus estructuras y procesos para operar de manera sistemática, asegurar la fluidez de las operaciones y alcanzar los objetivos previstos. Basados en el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), estos sistemas permiten la mejora continua mediante procesos optimizados y controlados.

Los sistemas de gestión se aplican en diversos sectores, adaptándose a los objetivos de la organización, y siguen una estructura común basada en las normas ISO. La más reconocida es ISO 9001 para la gestión de la calidad, pero también existen otras para áreas específicas como ISO 14001 (gestión medioambiental), ISO 45001 (seguridad y salud laboral), ISO 27001 (seguridad de la información), entre otras. Cada uno está diseñado para asegurar mejoras constantes en el ámbito correspondiente (DQS Colombia, 2024).

1.2.5.1 TIPOS DE SISTEMAS DE GESTIÓN

Los sistemas de gestión empresarial abordan diferentes necesidades de las empresas a través de soluciones tecnológicas específicas:

- ERP (Enterprise Resource Planning): Estos sistemas integran y conectan varios procesos empresariales, facilitando el flujo de información y brindando un soporte integral para la gestión de la empresa (Evaluando ERP, 2024).
- CRM (Customer Relationship Management): Los sistemas CRM están enfocados en gestionar las relaciones con los clientes, abarcando tanto la preventa como la postventa. Aunque algunos ERP incluyen esta funcionalidad, también existen soluciones CRM independientes que se centran exclusivamente en la gestión comercial y de clientes (Evaluando ERP, 2024).
- SGA (Sistemas de Gestión de Almacenes): Diseñados para gestionar la logística y el inventario de almacenes, estos sistemas pueden encontrarse integrados en un ERP o como soluciones especializadas para automatizar la gestión de almacenes (Evaluando ERP, 2024).

- DMS (Sistemas de Gestión Documental): Estos sistemas se encargan de gestionar grandes volúmenes de documentos, ya sea en formato digital o imágenes de documentos físicos, facilitando el almacenamiento, rastreo y organización (Evaluando ERP, 2024).
- BPM (Business Process Management): Se refiere a la capacidad de coordinar el flujo de trabajo entre departamentos, secuenciar tareas y mejorar la eficiencia operativa. Algunos ERP actuales ya incluyen esta funcionalidad de gestión de procesos empresariales (Evaluando ERP, 2024).
- B.I. (Business Intelligence): Herramientas orientadas al análisis de datos y toma de decisiones, especialmente dirigidas a la dirección. En la actualidad, muchas soluciones ERP integran herramientas de B.I., combinando la gestión operativa con el análisis de información. (Evaluando ERP, 2024)

1.2.6 ARQUITECTURA DE SOFTWARE

La arquitectura, comúnmente asociada con el diseño de edificios y espacios, también se refiere a la planificación de sistemas a un nivel abstracto. En el ámbito del software, este concepto surgió en los años 60 y se basa en modelos, patrones y abstracciones teóricas que guían la creación de software complejo antes de su implementación. Estos patrones proporcionan una solución general y reutilizable para problemas recurrentes en el desarrollo de software, similar a los patrones de programación, pero aplicados a un nivel estructural más alto.

La arquitectura es fundamental para planificar el desarrollo de software, ya que influye en la elección de herramientas, el ritmo de trabajo y factores económicos y humanos. A la hora de elegir un patrón arquitectónico, es importante considerar aspectos como:

- Coste: ¿Cuánto se está dispuesto a invertir en el desarrollo y mantenimiento del sistema? Algunos patrones requieren más infraestructura y desarrollo, lo que afecta el costo total.
- Tiempo de desarrollo: ¿Cuánto tiempo hay disponible para crear el producto? Esto influye en la selección de un patrón, especialmente si hay una fecha límite cercana.
- Número de usuarios: ¿Cuántos usuarios soportará el producto y qué tipo de sistema es? Estas preguntas ayudan a determinar si es necesario un patrón más distribuido, como el patrón broker, o algo menos distribuido, como el de capas.

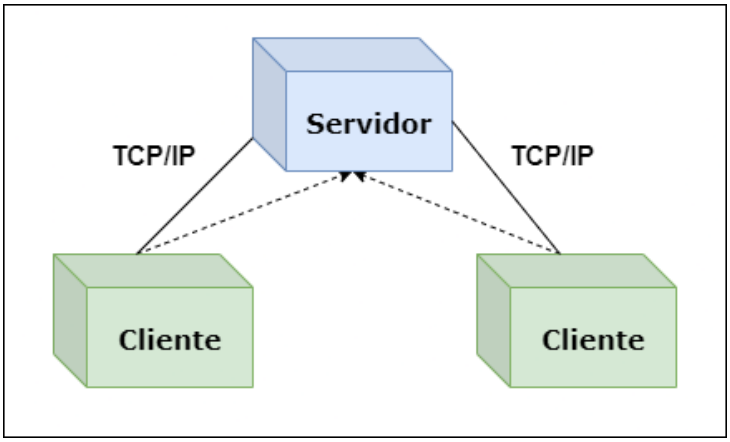
- Nivel de aislamiento: ¿El producto funcionará de manera independiente o deberá integrarse con otros sistemas? Algunos patrones, como el de capas, pueden dificultar la integración con terceros.

Además de estos factores, la familiaridad y comodidad con los diferentes patrones también juegan un papel importante en su elección. Probar diferentes enfoques permite adquirir experiencia con los distintos flujos de trabajo que cada patrón propone (OpenWebinars S.L, 2022).

1.2.6.1 TIPOS DE ARQUITECTURA DE SOFTWARE

1. **Patrón cliente-servidor**: Este patrón se utiliza ampliamente en webs y servicios online, donde un servidor centralizado proporciona servicios a múltiples clientes (OpenWebinars S.L, 2022).

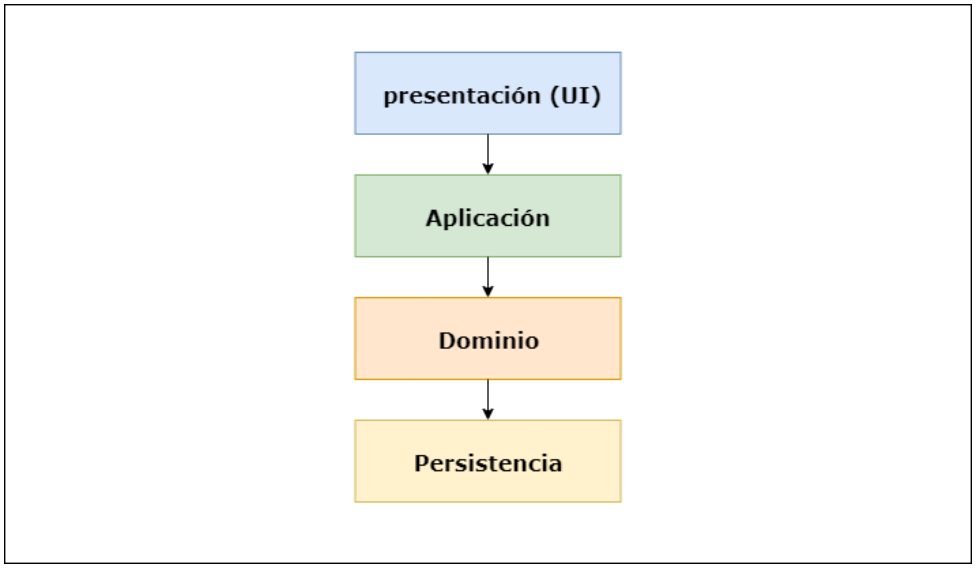
Figura 3 Patrón cliente-servidor (OpenWebinars S.L, 2022)



- **Ventajas**:
  - Centralización de recursos, facilitando la administración.
  - Escalabilidad al mejorar o agregar nodos sin afectar a otros.
  - Mantenimiento más sencillo por la clara separación de responsabilidades.
- **Desventajas**:
  - Alta dependencia del servidor; su caída afecta a todo el sistema.
  - Requiere hardware/software de servidor robusto.
  - El cliente no tiene control sobre los recursos en caso de fallo del servidor.

2. **Patrón de capas**: Estructura el software en capas, cada una con una función específica, proporcionando un servicio a la capa superior (OpenWebinars S.L, 2022).

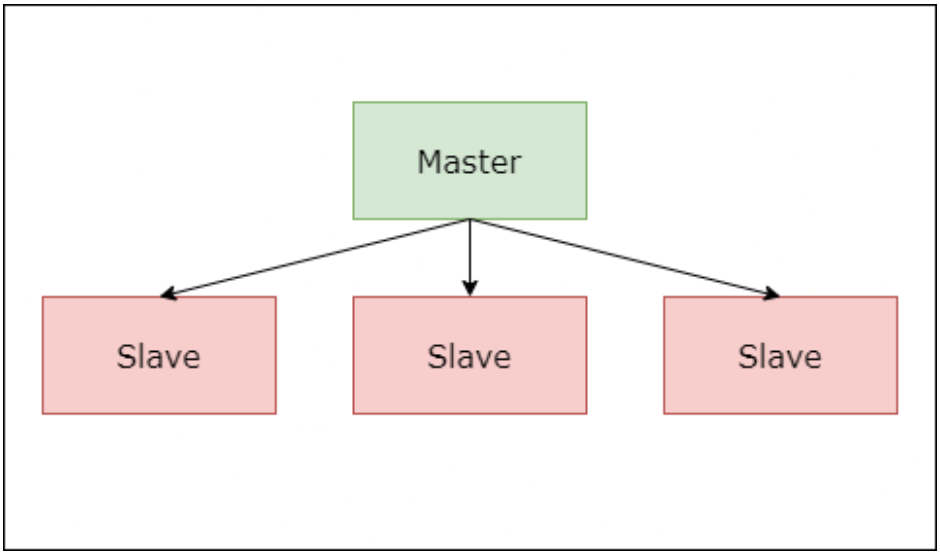
Figura 4 Patrón de capas (OpenWebinars S.L, 2022)



   - **Ventajas**:
     - Facilita pruebas individuales por capa.
     - Sencillez en el desarrollo, con equipos separados trabajando en distintas capas.
   - **Desventajas**:
     - Menor rendimiento al tener que atravesar cada capa.
     - Modificar una capa puede requerir cambios en todas las demás, complicando la escalabilidad.

3. **Patrón master-slave**: Un "maestro" delega tareas a varios "esclavos" que las procesan y retornan resultados (OpenWebinars S.L, 2022).

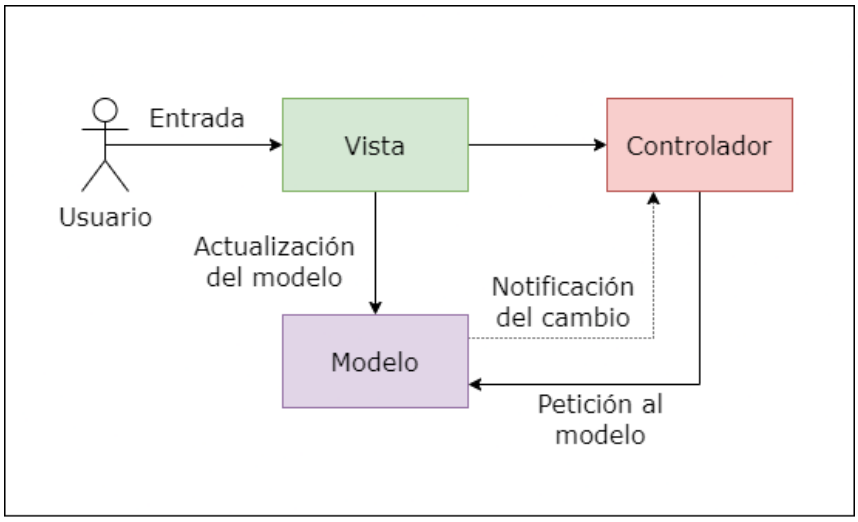
Figura 5 Patrón master-slave (OpenWebinars S.L, 2022)



- **Ventajas**:
  - Ideal para tareas multitarea, con control centralizado.
  - Fácil escalabilidad añadiendo más nodos esclavos.
- **Desventajas**:
  - No siempre se puede aplicar, ya que requiere que las tareas puedan dividirse.
  - Dependencia del sistema maestro, dificultando la portabilidad.

4. **Patrón modelo-vista-controlador (MVC)**: Divide una aplicación en tres partes: modelo (datos), vista (interfaz) y controlador (gestión de entradas) (OpenWebinars S.L, 2022).

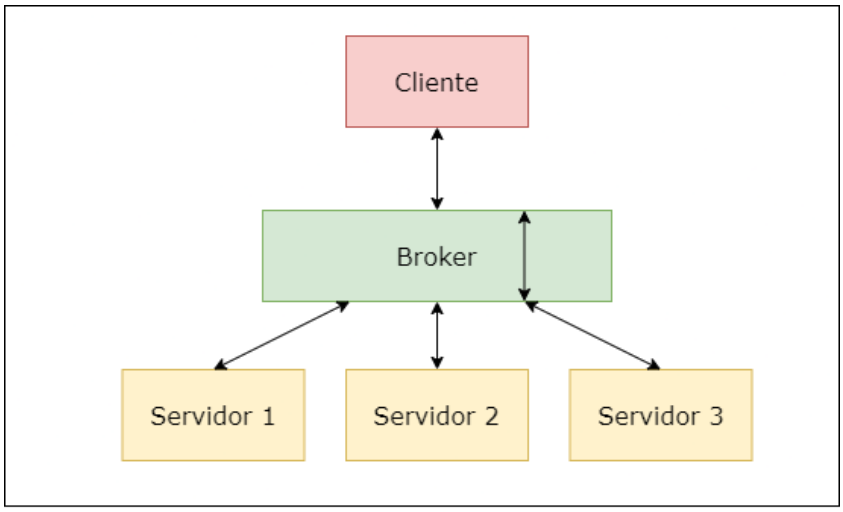
Figura 6 Patrón modelo-vista-controlador (MVC) (OpenWebinars S.L, 2022)



- **Ventajas**:
  - Facilita la colaboración y el desarrollo por separado.
  - Permite aplicaciones con múltiples vistas.
- **Desventajas**:
  - Complejidad en la implementación.
  - A veces, realizar cambios puede ser más lento y complicado en comparación con otros patrones.

5. **Patrón broker**: Utilizado en sistemas distribuidos, este patrón permite la interacción entre componentes desacoplados a través de un "broker" que gestiona la comunicación (OpenWebinars S.L, 2022).

Figura 7 Patrón broker (OpenWebinars S.L, 2022)



- **Ventajas**:
  - Escalabilidad al distribuir tareas entre múltiples nodos.
  - Buen rendimiento al poder redistribuir peticiones en caso de saturación.
- **Desventajas**:
  - Requiere una infraestructura extensa y costosa con múltiples servidores.
  - Mantenimiento complejo, ya que cualquier fallo puede estar en cualquier componente del sistema.

En resumen, estos patrones ofrecen diferentes enfoques para estructurar sistemas dependiendo de las necesidades de escalabilidad, rendimiento y complejidad de la aplicación.

1.2.7 SEGURIDAD INFORMÁTICA

La seguridad informática se encarga de resguardar los datos frente a manipulaciones por individuos no autorizados, asegurando la integridad tanto de los dispositivos como de la información. Su objetivo principal es evitar daños y amenazas externas mediante el uso de prácticas y herramientas especializadas (U de Cataluña, 2024).

1.2.7.1 CARACTERÍSTICAS

Entre las principales características de la seguridad informática se destacan las siguientes (universitat carlemany , 2023):

- **Autenticación autorizada**: En un sistema seguro, solo pueden autenticarse los usuarios con permisos adecuados. Nadie más puede acceder a los recursos ni a los datos del sistema.
- **Confidencialidad**: Los datos y recursos del sistema, al estar protegidos, permanecen inaccesibles para personas no autorizadas, garantizando su privacidad.
- **Integridad**: Únicamente los usuarios con autorización pueden modificar, eliminar o descargar datos, así como acceder a los recursos, lo que asegura un alto nivel de integridad en el sistema
- **Disponibilidad**: Los usuarios autorizados tienen acceso a los sistemas y datos cuando lo requieran
- **Acceso controlado**: El acceso a funciones y datos está limitado a usuarios con los permisos necesarios; sin autorización, no se permite el acceso
- **Backup**: También conocido como copia de seguridad, permite crear réplicas de datos y configuraciones para restaurar el sistema en caso de fallo
- **Cifrado**: Los datos sensibles deben estar encriptados para impedir que usuarios no autorizados los consulten
- **Vigilancia**: Los sistemas deben ser monitoreados constantemente para detectar y reaccionar rápidamente ante actividades sospechosas
- **Auditoría**: Se debe llevar un registro detallado de las actividades en el sistema, facilitando la identificación de accesos no autorizados o comportamientos anómalos
- **Mantenimiento adecuado**: El sistema debe estar siempre actualizado y correctamente mantenido para prevenir vulnerabilidades que puedan ser explotadas (2023)

1.2.7.2 ISO 27000

La serie ISO/IEC 27000 es un conjunto de estándares internacionales desarrollados por ISO e IEC, ampliamente reconocidos y utilizados en todo el mundo, que establecen buenas prácticas para la gestión de la seguridad de la información (Alonso, 2015).

Características clave:

- Enfoque principal: Establecer, mantener y gestionar un Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo la mejora continua y la mitigación de riesgos.
- Aplicabilidad: Estas normas son útiles para cualquier organización, sin importar su tamaño o naturaleza (pública o privada).

- ISO 27000: Proporciona las bases y un lenguaje común para entender e implementar las demás normas de la serie.

El objetivo es garantizar la protección de la información como un activo clave para las empresas mediante prácticas reconocidas a nivel global.

1.2.8 CIBERSEGURIDAD

La ciberseguridad abarca un conjunto de tecnologías, prácticas y políticas orientadas a prevenir y reducir el impacto de los ciberataques. Su propósito principal es resguardar sistemas informáticos, aplicaciones, dispositivos, datos, activos financieros y personas de amenazas como el ransomware, phishing, robo de datos y otros riesgos cibernéticos.

En el entorno empresarial, la ciberseguridad se ha vuelto un componente esencial para la gestión de riesgos. Según estimaciones de Cybersecurity Ventures, el gasto global en productos y servicios de ciberseguridad superará los 1.75 billones de dólares entre 2021 y 2025, reflejando la creciente relevancia de este sector. Asimismo, la Oficina de Estadísticas Laborales de EE. UU. proyecta que la demanda de analistas de seguridad de la información crecerá un 32 % entre 2022 y 2032, una tasa mucho mayor al promedio de otras profesiones, lo que destaca la necesidad de proteger entornos digitales en una era interconectada (Kaspersky Lab, 2020).

Las principales áreas de la ciberseguridad son:

1. Seguridad de red: Protección de redes informáticas frente a intrusiones y malware.

2. Seguridad de aplicaciones: Defensa contra amenazas desde la fase de diseño de software y dispositivos.

3. Seguridad de la información: Resguardo de la integridad y privacidad de los datos en almacenamiento y tránsito.

4. Seguridad operativa: Control de acceso y gestión de datos en la organización.

5. Recuperación ante desastres y continuidad del negocio: Planificación para restablecer operaciones tras incidentes de ciberseguridad.

6. Capacitación de usuarios finales: Instrucción a empleados para prevenir errores humanos que puedan comprometer la seguridad.

Este conjunto de prácticas es fundamental para mantener la integridad, confidencialidad y disponibilidad de los recursos digitales y asegurar la continuidad operativa de las empresas.

1.2.9 INGENIERIA DE SOFTWARE Y DISEÑO DEL SOFTWARE

1.2.9.1 INGENIERIA DE SOFTWARE

La Ingeniería de Software es esencial en el mundo moderno, ya que muchas infraestructuras y servicios dependen de sistemas basados en computadoras. Desde productos eléctricos hasta el entretenimiento, la fabricación y el sistema financiero, todos usan software para su funcionamiento. Esta disciplina es clave para el desarrollo de sociedades a nivel global, ya que facilita la creación de sistemas complejos y altamente integrados.

Aunque el software no está limitado por las leyes físicas o los materiales, su desarrollo puede volverse complicado y costoso debido a su naturaleza abstracta. Existen distintos tipos de software, desde sistemas embebidos hasta complejos sistemas de información, lo que implica que no todas las soluciones de ingeniería pueden aplicarse de manera universal. Un sistema de información organizacional requiere enfoques muy distintos a los de un juego de computadora con gráficos intensivos.

A pesar de los avances, siguen existiendo reportes de proyectos fallidos y problemas en el software. Estos, en su mayoría, se deben a dos factores principales: el aumento constante en las demandas y la falta de expectativas claras. La necesidad de sistemas más complejos y rápidos está superando las capacidades actuales de la ingeniería de software, lo que exige el desarrollo de nuevas técnicas. Además, muchas compañías no implementan adecuadamente estas metodologías, lo que provoca software costoso y poco confiable.

Sin embargo, la Ingeniería de Software ha logrado avances notables, como la exploración espacial y el desarrollo de internet. A pesar de sus desafíos, seguirá siendo crucial en el futuro, especialmente en un contexto donde la transformación digital es indispensable para las empresas.

En países como Colombia, la demanda de profesionales en esta área ha crecido significativamente, impulsada por la pandemia y la necesidad de innovación tecnológica. Los ingenieros de software son esenciales para desarrollar plataformas que mejoren la vida de los usuarios, lo que convierte esta carrera en una de las más prometedoras y demandadas.

Finalmente, el software se puede definir como un conjunto de programas y reglas que permiten a una computadora realizar tareas específicas. Estudiar Ingeniería de Software abre las puertas a un campo lleno de oportunidades, que sigue creciendo con la digitalización de las empresas y las nuevas necesidades tecnológicas (Sommerville, 2011).

1.2.9.2 DISEÑO DEL SOFTWARE

Diseñar un software puede parecer una tarea compleja, ya que implica desarrollar algo muy articulado y a veces difícil de manejar. Sin embargo, no es necesario alarmarse. La digitalización ha

impulsado a muchas empresas a necesitar soluciones personalizadas que se ajusten a sus necesidades específicas, lo que ha incrementado la demanda de plataformas a medida.

El problema surge cuando estas empresas no están preparadas para seguir todas las fases del proceso correctamente. A menudo, omiten etapas clave como el análisis o no le dan suficiente importancia a las pruebas. Para obtener buenos resultados, es esencial contar con un equipo especializado que siga cada paso del diseño de manera detallada.

El proceso de diseño de un software consta de seis fases interrelacionadas: análisis de requerimientos, diseño, programación, pruebas, implementación y mantenimiento. Todas son necesarias para garantizar un resultado exitoso (W&B Asset Studio, 2022).

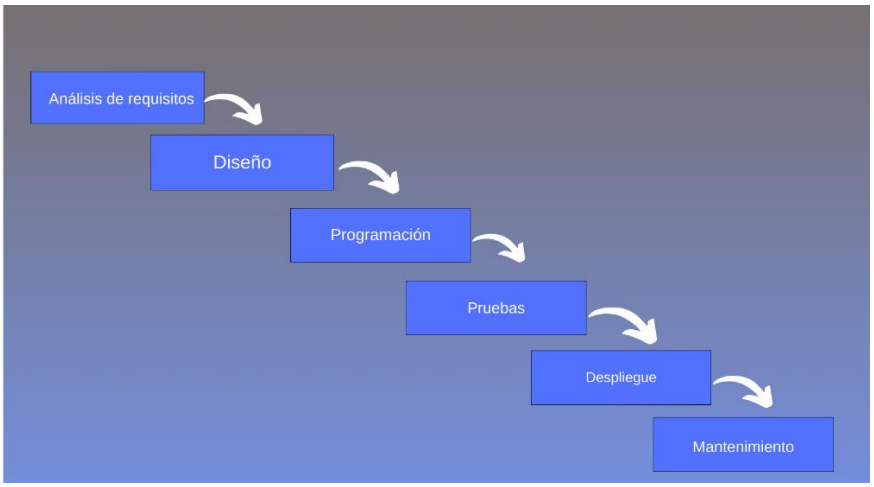
1.2.9.2.1 LAS FASES DEL CICLO DE VIDA DE UN SOFTWARE

La fase preliminar del ciclo de vida de un software es clave antes de iniciar el desarrollo. Su propósito es contextualizar el producto en términos de los beneficios que ofrecerá, los problemas que resolverá y los objetivos que justifican su creación. En esta etapa, se debe preparar un informe que incluya los requisitos funcionales, que son las características obligatorias del software, y los requisitos no funcionales, que son características opcionales.

Una herramienta útil en esta fase es la tabla MoSCoW, que clasifica las funciones del software como Must Have (imprescindibles) o Should Have (deseables).

El modelo de desarrollo más comúnmente utilizado es el modelo en cascada, que sigue una secuencia lineal en la que cada fase depende de la anterior, progresando de manera ordenada (W&B Asset Studio, 2022).

Figura 8 Fases del ciclo de vida de un software



El ciclo de vida de un software se compone de seis fases fundamentales, basadas en el modelo en cascada, donde cada fase sigue a la anterior de manera secuencial. Aquí te resumo cada una de ellas:

Análisis de requisitos: Se define el entorno en el que funcionará el software, sus funciones, características de los usuarios, limitaciones, rendimiento e interfaz. Es una fase crucial, ya que los errores aquí pueden causar pérdidas de tiempo y dinero más adelante.

Diseño: Se establece la arquitectura del software, definiendo la estructura de datos, funciones y restricciones. Esta fase organiza los componentes del sistema y su interrelación, considerando las tecnologías a utilizar para garantizar una implementación eficiente.

Programación: En esta etapa se escribe el código del software, usando un entorno de desarrollo integrado (IDE) que facilita la tarea. La calidad del código es clave, ya que errores en esta fase pueden comprometer todo el proyecto.

Pruebas: Se verifica que el software funcione según los requisitos establecidos, buscando errores lógicos o conceptuales que no se detectaron durante la depuración inicial.

Despliegue: Una vez superadas las pruebas, el software se implementa y se pone en funcionamiento. Esta fase varía según si el software es para venta, un cliente específico o una aplicación web.

Mantenimiento: A lo largo de su vida operativa, el software requiere actualizaciones y correcciones. El mantenimiento puede ser correctivo (para resolver errores) o evolutivo (para agregar nuevas funciones).

Este modelo lineal tiene el inconveniente de ser poco flexible, ya que volver a fases anteriores es complicado y puede causar retrasos en la entrega del proyecto.

1.3 Marco Legal

En Colombia, la regulación en Seguridad y Salud en el Trabajo (SST) se basa principalmente en la Ley 1562 de 2012 y el Decreto 1443 de 2014, que establecen las directrices generales para promover la salud y prevenir riesgos en el entorno laboral. El propósito central de estas normativas es asegurar que los trabajadores cuenten con un entorno laboral seguro y saludable (HSE Software, 2024).

A continuación, se resumen algunos aspectos clave de la normatividad en Seguridad y Salud en el Trabajo (SST) en Colombia:

- Ley 1562 de 2012: Regula la promoción de la salud y la prevención de riesgos laborales, asignando responsabilidades tanto a trabajadores como a trabajadores en temas de SST. Establece las obligaciones de las empresas para implementar programas de prevención y regula la investigación de accidentes laborales y enfermedades relacionadas con el trabajo.
- Decreto 1443 de 2014: Detalla la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), el cual es obligatorio para todas las empresas, sin importar su tamaño o sector. Este decreto especifica elementos clave como la identificación de peligros, la evaluación de riesgos, la planificación de actividades preventivas y la capacitación de los empleados.
- Resolución 0312 de 2019: Definir los requisitos para implementar el Programa de Gestión en Seguridad y Salud en el Trabajo (PG-SST) y establecer cómo las empresas deben reportar la información relacionada con la SST al Ministerio de Trabajo.

- El Decreto 1072 de 2015, que compila el Decreto 1443 de 2014, surge como respuesta a la Ley 1562 de 2012 y define el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST). Este sistema no solo es un requisito legal, sino que también aporta importantes beneficios a las organizaciones, mejorando la eficiencia de los procesos y optimizando los recursos.

  El SG-SST, según el Decreto 1072, sigue el ciclo PHVA (Planificar, Hacer, Verificar, Actuar), lo que implica revisiones periódicas por parte de la Alta Dirección y auditorías internas. Este sistema debe integrarse con otros procesos organizacionales para mejorar la gestión general de la empresa.

  El Decreto 1072 está alineado con la norma OHSAS 18001, que establece parámetros para garantizar la mejora continua en la gestión de la seguridad y salud en el trabajo. Además, este decreto unifica y simplifica toda la normativa relacionada con la SST en Colombia.

  Un aspecto clave del decreto es la obligatoriedad de implementar un SG-SST en todas las empresas del país, sin importar su tamaño o número de empleados, siguiendo los lineamientos de OHSAS 18001 para su implementación y certificación (Isotools.us, 2024).

- El Decreto 0472 de 2015, emitido el 17 de marzo, establece los criterios de Colombia para evaluar las multas por violaciones a las normas de seguridad y salud en el trabajo y riesgos laborales (Gov.co, 2024).

  Los puntos clave son los siguientes:

- Propósito

Establecer estándares de evaluación de multas, asegurar los debidos procedimientos legales y estandarizar suspensiones y suspensiones por infracciones.

- Ámbito

Aplicable a actuaciones administrativas. Inspectores de Trabajo y Previsión Social y demás departamentos del Ministerio de Trabajo.

- Principios

Incluyen el debido proceso, la prohibición de sanciones más severas contra los solicitantes, la igualdad ante la ley, la imparcialidad, la ética, la apertura, la eficiencia, la rapidez y la proporcionalidad de las sanciones.

- Basado en los criterios de evaluación

Las multas tendrán en cuenta lo siguiente factores, tales como:

  - Reincidencia.
  - Obstaculizando la investigación.
  - Uso de medios engañosos
  - Grado de cumplimiento de las normas.
  - Daño causado.

- Proporcionalidad y Razonabilidad

Las sanciones deben ser proporcionales al tamaño de la empresa y al número de empleados.

- Plan de mejora

Los inspectores pueden ordenar un plan de mejora para corregir infracciones. El incumplimiento de estos planes puede dar lugar a sanciones.

- Cierres y cierres de empresas

Los inspectores podrán ordenar cierres de lugares de trabajo por riesgos para la salud y seguridad de los trabajadores, con límites de tiempo y cierres permanentes

- Procedimiento

Las decisiones deben estar motivadas y comunicadas claramente a todas las partes involucradas. Los derechos laborales de los trabajadores no serán vulnerados durante los períodos de suspensión del trabajo o negocio.

- Informe de accidente

El empleador debe informar los accidentes graves y las enfermedades profesionales a la autoridad local en un plazo de dos días laborables.

- Período de validez

El decreto entrará en vigor tras su emisión. En vigor a partir de la fecha de publicación y reemplaza cualquier disposición anterior en conflicto.

Este marco regulatorio tiene como objetivo garantizar la protección de los trabajadores y la correcta aplicación de las leyes de seguridad y salud en el trabajo.

- La Resolución 1016 de 1989 establece las normas para la organización y funcionamiento de los Programas de Salud Ocupacional en Colombia, dirigidos a los empleadores públicos y privados. Estos programas incluyen actividades de Medicina Preventiva, Medicina del Trabajo, Higiene y Seguridad Industrial, con el fin de proteger la salud de los trabajadores.

  Se especifica que las empresas deben contar con un programa adaptado a sus riesgos y características. Este programa debe ser aprobado y firmado por el representante legal, mantenerse actualizado y disponible para las autoridades. Se permite su ejecución de forma exclusiva, compartida con otras empresas o a través de entidades especializadas.

  El programa incluye subprogramas de Medicina Preventiva, del Trabajo, Higiene y Seguridad Industrial, así como la constitución de Comités de Medicina, Higiene y Seguridad Industrial. Estos subprogramas deben realizar actividades como exámenes médicos, prevención de riesgos, investigación de accidentes y control de condiciones de trabajo.

  Se exigen registros mínimos, como listado de riesgos, protección personal, estadísticas de accidentes, entre otros. Además, el programa debe ser evaluado semestralmente y reajustado anualmente. Las empresas tienen entre seis y dieciocho meses para implementarlo, dependiendo del número de trabajadores (Gov.co, s.f.).
- La Resolución 1111 de 2017 define los Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) para empleadores y contratantes en Colombia. Establece las obligaciones que deben cumplir las empresas en el marco del Sistema General de Riesgos Laborales, asegurando condiciones adecuadas de capacidad tecnológica, científica, patrimonial y administrativa.

  - Puntos clave:

1. Campo de aplicación

Abarca a empleadores públicos y privados, contratistas, organizaciones del sector cooperativo, y otros actores relacionados con el trabajo, incluyendo estudiantes y personal civil de las fuerzas militares y la Policía Nacional.

2. Objeto

Implementar los Estándares Mínimos del SG-SST, un conjunto de normas y procedimientos que las empresas deben seguir para garantizar la seguridad y salud de los trabajadores. Estos estándares son graduables y dinámicos, ajustándose al número de empleados, la actividad económica y los riesgos inherentes de cada empresa.

3. Responsabilidad

Cada empresa debe implementar su propio SG-SST y puede compartir recursos con otras, siempre garantizando que cada una cumpla con sus propias obligaciones.

4. Compromiso de la alta dirección

Las empresas deben integrar los estándares en sus sistemas de gestión, liderando la implementación y realizando auditorías internas para identificar mejoras.

Esta resolución busca estandarizar las condiciones básicas que deben cumplir las organizaciones para proteger la salud de sus trabajadores, ajustándose a las particularidades de cada entidad (Setraria juridica distrital , 2024)

En Colombia, existen diversas leyes y decretos diseñados para salvaguardar los datos personales, proteger la privacidad y establecer normas claras sobre el manejo responsable de la información. A continuación, se presentan algunas de las normativas más destacadas:

- La Ley 1273 de 2009 en Colombia establece una serie de modificaciones al Código Penal con el fin de proteger los datos e información personales, así como los sistemas informáticos. A través de esta ley, se crea un nuevo bien jurídico denominado "protección de la información y de los datos", que abarca delitos específicos y sanciones asociadas a violaciones a la seguridad digital. Aquí se resumen los puntos principales:

    1. **Acceso no autorizado**: Penado con prisión y multas para quien acceda o permanezca sin permiso en sistemas informáticos.
    2. **Obstrucción de sistemas**: Se castiga con prisión y multas a quien interfiera en el funcionamiento de redes o sistemas sin autorización.
    3. **Interceptación de datos**: La ley sanciona a quien intercepte comunicaciones digitales o datos sin orden judicial.

4. **Daños a sistemas informáticos**: Quien destruya, altere o borre información sin autorización enfrenta penas de prisión y multas.
5. **Uso de software malicioso**: Penaliza la distribución y uso de programas que dañen sistemas informáticos.
6. **Violación de datos personales**: Sanciona la obtención o difusión de datos personales sin autorización.
7. **Suplantación de sitios web**: Penaliza la creación de sitios falsos para captar datos personales, con agravantes si se involucran víctimas en el proceso.
8. **Circunstancias agravantes**: Las penas aumentan en situaciones específicas, como cuando el delito afecta a sistemas gubernamentales o del sector financiero, involucra a funcionarios públicos o busca fines terroristas.

Además, la ley establece sanciones por hurto y transferencias no autorizadas realizadas mediante manipulación informática. También modifica el Código Penal y el Código de Procedimiento Penal para incluir delitos informáticos como causales de mayor punibilidad y asigna competencias específicas a los jueces para su tratamiento. La Ley 1273 entró en vigor tras su promulgación y derogó cualquier normativa que se opusiera a sus disposiciones, en especial el artículo 195 del Código Penal (Secretaría Jurídica Distrital, 2024).

- La Ley Estatutaria 1581 de 2012 en Colombia establece disposiciones para proteger los datos personales y el derecho de las personas a conocer, actualizar y corregir su información en bases de datos. Aplica a datos registrados en bases manejadas por entidades públicas o privadas dentro del país y, en ciertos casos, fuera de él.

  Excepciones: La ley excluye de su aplicación a datos de uso personal, aquellos relacionados con seguridad y defensa nacional, prevención de lavado de activos, información de inteligencia y contrainteligencia, contenido periodístico, y bases de datos reguladas por leyes específicas como la Ley 1266 de 2008 y la Ley 79 de 1993.

  Definiciones clave:

  - **Autorización**: Consentimiento del titular de los datos.
  - **Base de Datos**: Conjunto organizado de datos personales.
  - **Dato Personal**: Información vinculada a una persona natural.
  - **Encargado del Tratamiento**: Quien maneja los datos por encargo.
  - **Responsable del Tratamiento**: Quien decide sobre el manejo de datos.
  - **Titular**: Persona dueña de los datos.
  - **Tratamiento**: Cualquier operación realizada sobre los datos.

  Esta ley regula el uso y tratamiento de datos personales, buscando un equilibrio entre el derecho a la privacidad y la necesidad de acceso a la información (Secretaría Jurídica Distrital, 2024).

- El Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 de 2012, estableciendo directrices adicionales para la protección de datos personales en Colombia. Define aspectos claves para facilitar la aplicación de la ley, especialmente sobre la autorización para el

tratamiento de datos, las políticas de uso por parte de responsables y encargados, y las obligaciones de transparencia y rendición de cuentas.

Aspectos destacados:

- **Ámbito personal/doméstico**: Las bases de datos utilizadas exclusivamente en entornos personales o familiares están exentas de la aplicación de la ley.
- **Definiciones**:
    - **Aviso de privacidad**: Comunicación para informar al titular sobre el uso de sus datos y las políticas aplicables.
    - **Dato público**: Información de carácter general, como el estado civil o profesión, que no es privada o sensible y puede estar en registros oficiales.
    - **Datos sensibles**: Incluye información íntima o que podría causar discriminación, como datos raciales, religiosos, de salud o biométricos.
    - **Transferencia y Transmisión de datos**: La **transferencia** implica enviar datos a otro responsable dentro o fuera del país, mientras que la **transmisión** es cuando el encargado del tratamiento procesa los datos por orden del responsable, dentro o fuera de Colombia.
- Este decreto detalla cómo deben manejarse y compartirse los datos personales, con un enfoque en los derechos de los titulares y el deber de informar a quienes manejan esta información (Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, 2024).

  El Decreto 886 de 2014 reglamenta el artículo 25 de la Ley 1581 de 2012, estableciendo los lineamientos para el **Registro Nacional de Bases de Datos** (RNBD) en Colombia, un directorio público de bases de datos personales administrado por la Superintendencia de Industria y Comercio (SIC). Su propósito es facilitar la consulta ciudadana y supervisar el cumplimiento de los derechos de protección de datos.

  Aspectos clave del decreto:

  1. **Ámbito de Aplicación**: Deben inscribirse en el RNBD las bases de datos con tratamiento automatizado o manual, gestionadas tanto por entidades públicas como privadas dentro o fuera de Colombia, siempre que estén sujetas a la legislación colombiana.
  2. **Deber de Inscripción**: Los responsables del tratamiento deben inscribir cada base de datos de forma independiente, proporcionando información básica como datos de contacto, finalidad de la base de datos, canales de atención y política de tratamiento de la información.
  3. **Consulta Ciudadana**: Los ciudadanos pueden consultar el RNBD para conocer cómo y quién trata sus datos personales, y ejercer sus derechos de actualización, rectificación, supresión de datos o revocación de la autorización.
  4. **Términos de Inscripción**: La inscripción en el RNBD debe realizarse dentro del año posterior a la habilitación del registro. Las bases de datos nuevas deben registrarse en los dos meses siguientes a su creación.
  5. **Facultad Sancionatoria**: La SIC tiene autoridad para sancionar el incumplimiento de estas disposiciones y de la Ley 1581 de 2012.

Este decreto define los elementos básicos del RNBD, facilita el control ciudadano sobre el uso de sus datos personales y asegura la transparencia en el tratamiento de datos en Colombia (Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, 2024).

- La Ley 1928 de 2018 aprueba en Colombia el "Convenio sobre la Ciberdelincuencia", firmado en Budapest el 23 de noviembre de 2001. Este convenio internacional establece compromisos y normas para combatir los delitos informáticos y mejorar la cooperación entre países en la lucha contra la ciberdelincuencia.

  Aspectos principales de la ley:

1. **Aprobación del Convenio**: La ley ratifica el acuerdo internacional, comprometiendo a Colombia a aplicar sus disposiciones para mejorar la seguridad cibernética.
2. **Vigencia Internacional**: El convenio será vinculante para Colombia a partir de la formalización del vínculo internacional.
3. **Aplicación**: La ley entra en vigor desde su publicación oficial.

Con esta ley, Colombia reafirma su compromiso en la cooperación internacional para combatir delitos en el ciberespacio y fortalecer la seguridad digital (Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, 2024).

Metodología De Investigación

2.1 *DESARROLLO DE SISTEMAS DE INFORMACIÓN BASADOS EN WEB*

El desarrollo de sistemas de información basados en web requiere una metodología bien estructurada que permita completar el proyecto con eficiencia y cumpliendo altos estándares de calidad. La plataforma web, desde su aparición, se ha integrado en prácticamente todos los aspectos de nuestra vida cotidiana, evolucionando en diferentes formas y categorías. Hoy en día, esta tecnología es robusta y segura, lo cual la convierte en una opción viable tanto para usuarios como para desarrolladores. Sin embargo, al principio su desarrollo era complicado, carecía de un proceso claro y organizado, similar a los retos iniciales de la Ingeniería de Software (Pressman, 2010).

Para enfrentar esta situación, los desarrolladores comenzaron a adaptar metodologías tradicionales de software, aunque muchas de estas no lograban satisfacer completamente los requisitos o carecían de una estructura eficiente para la web. Así nace la Ingeniería Web, una disciplina que aporta un enfoque sistemático y disciplinado al desarrollo y mantenimiento de sistemas y sitios web. A partir de aquí, se diseñaron metodologías centradas en las necesidades específicas de la plataforma web, enfocándose no solo en el ciclo de vida del software, sino también en buenas prácticas de diseño.

En esta investigación se analizaron distintas metodologías de desarrollo aplicables al ámbito web, tanto en software tradicional como en software específicamente web, con el fin de generar una metodología propia que integre las mejores prácticas de ambas. Esta metodología fue probada en dos casos prácticos y evaluada posteriormente (Aguirre Caracheo, Metodología del desarrollo para sistemas de información basados en web, 2014).

Metodologías comunes para el desarrollo web

- Agile: Enfoque iterativo y adaptable.
- Scrum: Subconjunto de Agile, basado en sprints y roles específicos.
- Waterfall: Secuencial, útil para proyectos con requisitos claros.
- DevOps: Promueve la colaboración entre desarrollo y operaciones.

Esta metodología puede ajustarse según el tamaño del proyecto, el equipo de desarrollo y las herramientas tecnológicas empleadas.

2.2 ANALISIS METODOLOGÍAS PARA EL DESARROLLO DE SOFTWARE WEB

2.2.1 DEFINICIÓN

El desarrollo web ha evolucionado desde enfoques ad hoc hacia metodologías más estructuradas. Inicialmente, se utilizaban métodos informales, lo que limitaba la sistematicidad en los procesos de desarrollo. Autores como Achebe (2002) y Suh (2005) destacaron la necesidad de formalizar estos procesos (Aguirre Caracheo, 2014).

Se propusieron adaptaciones del modelo en cascada, como la metodología de "remolinos" (Whirlpool), que incorpora iteraciones en las etapas iniciales para refinar los requerimientos del proyecto. Con el tiempo, surgieron metodologías ligeras que incluyen cinco etapas: desarrollo de estrategia de e-business, reingeniería de procesos, requerimientos de desarrollo, diseño/codificación y pruebas. La Metodología de Desarrollo de Comercio en Internet (ICDM) también se desarrolló, centrándose en el análisis del entorno de negocio. Estas metodologías buscan enfrentar los retos del desarrollo web moderno y mejorar la calidad de los proyectos (Aguirre Caracheo, 2014).

2.2.2 ANÁLISIS

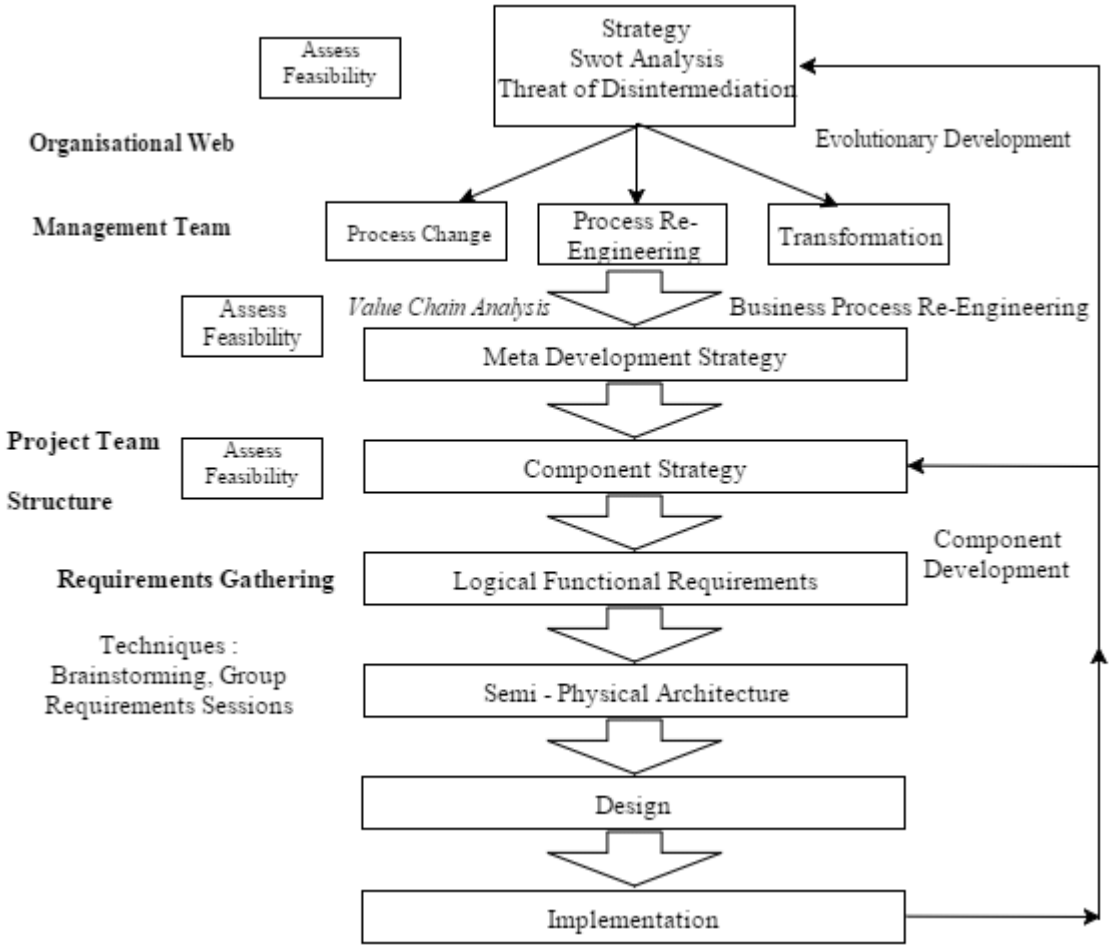
2.2.2.1*ICMC*

La metodología ICDM (Internet Commerce Development Methodology) se centra en el comercio electrónico y aborda problemáticas estratégicas, administrativas y culturales, además de los aspectos técnicos de diseño e implementación. Reconoce que la efectividad en el e-business es subjetiva y socialmente construida, y utiliza el análisis competitivo para guiar a las organizaciones en su dirección estratégica.

ICDM enfatiza el entorno organizacional y utiliza métodos sociales para definir requerimientos y estrategias, integrando el análisis FODA para identificar oportunidades en un contexto global. No se trata de una metodología rígida con muchos pasos, sino de un enfoque flexible que se adapta a diversas situaciones en las que las organizaciones buscan beneficios del comercio en línea. A diferencia de otras metodologías, ICDM vincula de manera directa las estrategias de desarrollo con las necesidades del negocio, asegurando que el enfoque del proyecto esté alineado con los intereses empresariales (Aguirre Caracheo, 2014).

Las fases que componen a esta metodología (Figura 9) tanto en la parte de análisis de negocio y de desarrollo del proyecto son las siguientes:

Figura 9 Fases de la metodología ICDM (Kosasi, 2016)



2.2.2.2 OOHDM

La metodología OOHDM (Object-Oriented Hypermedia Design Method) es un enfoque basado en el modelado para la construcción de aplicaciones de hipermedia de gran tamaño y se basa en el método HDM (Hypermedia Design Method). Se compone de cuatro actividades principales:

1. **Diseño Conceptual**: Se construye un modelo del dominio de la aplicación utilizando principios de modelado orientado a objetos con una notación similar a UML, incorporando atributos de múltiples valores y relaciones explícitas.

2. **Diseño de Navegación**: La aplicación se ve como una vista de navegación sobre el modelo conceptual. Esta fase introduce el concepto de nodos, que son objetos de navegación construidos a partir de objetos conceptuales, permitiendo una separación clara entre navegación y contenido.

3. **Diseño de la Interfaz Abstracta**: Se especifican los objetos de la interfaz visibles para el usuario, diferenciando entre elementos de navegación y otros componentes de la interfaz. Se utiliza el modelo ADV (Abstract Data View) para describir formalmente la interfaz de usuario.

4. **Implementación**: En esta fase, los elementos del diseño se implementan, teniendo en cuenta el entorno de desarrollo. Aunque OOHDM es orientado a objetos, su implementación no necesariamente requiere que sea así.

Esta metodología combina un enfoque prototípico, incremental e iterativo, permitiendo un diseño modular y reutilizable, lo que facilita el manejo de cada aspecto del desarrollo de aplicaciones de hipermedia (Aguirre Caracheo, 2014).

2.2.2.3 WSDM

La metodología WSDM (Web Site Design Method), también conocida como Wisdom, se centra en el usuario en lugar de en los datos, lo que la distingue de metodologías anteriores. Su enfoque implica primero identificar los diferentes tipos de usuarios y describir sus características y requerimientos de información, lo que se traduce en "perspectivas". Solo después de esta etapa se inicia el diseño conceptual del sitio web, utilizando las perspectivas y el modelo de objetos de negocio de la organización como base.

Es importante señalar que WSDM es una metodología centrada en el usuario, pero no guiada por él. Dado que las aplicaciones web son a menudo distribuidas a nivel mundial, es difícil conocer las necesidades específicas de todos los usuarios. Por lo tanto, la metodología busca equilibrar las necesidades tanto del proveedor como del usuario.

El método WSDM consta de las siguientes fases:

1. Modelado del Usuario: Incluye sub-fases como la clasificación del usuario y la descripción de la clase del usuario.

2. Diseño Conceptual: Comprende el modelado de objetos y el diseño de navegación.

3. Diseño de la Implementación.

4. implementación Final.

Esta estructura permite un desarrollo más efectivo y adaptado a las necesidades del usuario, sin depender exclusivamente de sus requerimientos individuales (Aguirre Caracheo, 2014).

2.2.2.4 HOWCROFT & CARROLL

La metodología de desarrollo de sitios web propuesta por Debra Howcroft y John Carroll se compone de cuatro fases: análisis, diseño, generación e implementación, cada una con pasos específicos que buscan facilitar el ciclo de vida del proyecto.

Fase Uno: Análisis

En esta fase se define la estrategia web y se analizan los requerimientos para evitar riesgos comunes en proyectos de software. Incluye el desarrollo de la estrategia web, la definición de objetivos y el análisis de estos junto a los recursos disponibles.

Fase Dos: Diseño

Basado en el Documento de Objetivos, aquí se estructura y diseña el sitio, considerando la escalabilidad para adaptarse a futuros cambios. Se realizan pruebas tempranas para detectar problemas de diseño

Fase Tres: Generación

Esta fase se enfoca en crear el sitio según el Documento de Diseño, seleccionando recursos, verificando la compatibilidad y generando el código. Finalmente, se ejecutan pruebas exhaustivas en diversos entornos.

Fase Cuatro: Implementación

Incluye la promoción y el mantenimiento del sitio, asegurando su visibilidad y contenido actualizado. Se revisan objetivos previos y se integran mejoras, enfatizando la naturaleza iterativa de la metodología.

Este proceso ordenado permite una evaluación constante, adaptándose a cambios tecnológicos y nuevos objetivos (Aguirre Caracheo, 2014).

Desarrollo Del Proyecto

Tras aplicar la información recolección de información, se realizó el tratamiento adecuado para su análisis, así como el diseño y desarrollo de la aplicación y las pruebas correspondientes. A continuación, se presenta la información detallada sobre el producto final y las conclusiones obtenidas en la investigación.

3.1 Levantamiento De *Requerimientos*

3.1.1 Requerimientos Funcionales

Tabla 4 Registro y autenticación de usuarios

Código	**Nombre**			**Grado de Necesidad**
RF-01	Registro y autenticación de usuarios			Alto
Descripción	El sistema deberá permitir a los usuarios registrarse y autenticarse para acceder a las funcionalidades del sistema. Los usuarios deberán proporcionar información personal para el registro, que incluirá al menos nombre de usuario, contraseña y correo electrónico. Una vez registrados, los usuarios podrán iniciar sesión en el sistema utilizando sus credenciales.			
Entradas	**Fuente**	**Salida**	**Destino**	**Restricciones**
Nombre de usuario, contraseña, correo electrónico	Usuarios	Confirmación de registro, acceso al sistema	Base de datos de usuarios, sesión de usuario	Los nombres de usuario deben ser únicos, las contraseñas deben cumplir con las políticas de seguridad establecidas (longitud mínima,

				caracteres especiales.)
Proceso	1. El usuario accede a la página de registro del sistema. 2. El usuario completa el formulario de registro con su información personal. 3. El sistema valida la información proporcionada por el usuario. 4. Si la validación es exitosa, el sistema registra al usuario en la base de datos y le proporciona acceso al sistema. 5. Si la validación falla, el sistema muestra un mensaje de error al usuario y solicita que corrija la información proporcionada.			
Efecto Colateral	• Los usuarios podrán acceder a las funcionalidades del sistema después de registrarse y autenticarse. • Se mantendrá un registro de usuarios en la base de datos del sistema.			

Tabla 5 Asignación de roles y privilegios

Código	**Nombre**		**Grado de Necesidad**	
RF-02	Asignación de roles y privilegios		Alto	
Descripción	El sistema deberá permitir asignar roles y privilegios a los usuarios para controlar su acceso a las diferentes funcionalidades y datos del sistema. Los roles determinarán las acciones que los usuarios pueden realizar, mientras que los privilegios especificarán los niveles de acceso a los datos.			
Entradas	**Fuente**	**Salida**	**Destino**	**Restricciones**
Usuario, roles, privilegios	Administrador del sistema	Confirmación de asignación de roles y privilegios	Base de datos de roles y privilegios, sesión de usuario	Los roles y privilegios solo pueden ser asignados por el administrador del sistema.
Proceso	1. El administrador del sistema accede a la herramienta de administración de roles y privilegios. 2. El administrador selecciona un usuario al que desea asignar un rol. 3. El administrador elige el rol deseado para el usuario de una lista predefinida.			

	4. El administrador configura los privilegios asociados al rol seleccionado. 5. El sistema guarda la asignación de roles y privilegios en la base de datos.
Efecto Colateral	• Los usuarios tendrán acceso solo a las funcionalidades y datos autorizados según sus roles y privilegios asignados.

Tabla 6 Control de acceso basado en roles

Código	**Nombre**			**Grado de Necesidad**
RF-03	Control de acceso basado en roles			Alto
Descripción	El sistema deberá controlar el acceso a las diferentes funcionalidades y datos basado en los roles asignados a los usuarios. Esto garantizará que cada usuario tenga acceso solo a las áreas del sistema que sean relevantes para sus responsabilidades y funciones.			
Entradas	**Fuente**	**Salida**	**Destino**	**Restricciones**
Usuario, función solicitada	Usuarios, sistema	Autorización de acceso o denegación de acceso	Funcionalidades o datos solicitados	Los usuarios solo podrán acceder a funcionalidades y datos para los que tengan los roles y privilegios adecuados.
Proceso	1. El usuario solicita acceso a una funcionalidad o dato específico del sistema. 2. El sistema verifica los roles asignados al usuario. 3. El sistema compara los roles del usuario con los roles requeridos para acceder a la funcionalidad o dato solicitado. 4. Si el usuario tiene los roles adecuados, el sistema autoriza el acceso. 5. Si el usuario no tiene los roles adecuados, el sistema deniega el acceso y muestra un mensaje de error.			
Efecto Colateral	• Se garantiza que los usuarios solo tengan acceso a las áreas del sistema relevantes para sus roles y responsabilidades.			

Tabla 7 Gestión de contraseñas seguras y políticas de contraseña

Código	**Nombre**			**Grado de Necesidad**
RF-04	Gestión de contraseñas seguras y políticas de contraseña			Alto
Descripción	El sistema deberá implementar medidas para garantizar contraseñas seguras y aplicar políticas de contraseña que cumplan con los estándares de seguridad. Esto ayudará a proteger las cuentas de usuario contra accesos no autorizados y evitará violaciones de seguridad debido a contraseñas débiles.			
Entradas	**Fuente**	**Salida**	**Destino**	**Restricciones**
Contraseñas nuevas, políticas de contraseña	Usuarios, políticas de seguridad	Confirmación de cambio de contraseña	Base de datos de contraseñas	Las contraseñas deben cumplir con las políticas de contraseña establecidas, como longitud mínima, uso de caracteres especiales.
Proceso	1. El usuario intenta cambiar su contraseña o crear una nueva. 2. El sistema verifica que la contraseña propuesta cumpla con las políticas de contraseña establecidas. 3. Si la contraseña cumple con las políticas, el sistema la acepta y la guarda en la base de datos. 4. Si la contraseña no cumple con las políticas, el sistema rechaza el cambio y muestra un mensaje de error al usuario.			
Efecto Colateral	• Se garantiza que todas las contraseñas en el sistema cumplan con los estándares de seguridad establecidos, lo que reduce el riesgo de violaciones de seguridad debido a contraseñas débiles.			

Tabla 8 Alertas automáticas ante actividades sospechosas

Código	**Nombre**	**Grado de Necesidad**
RF-05	Alertas automáticas ante actividades sospechosas	Alto

Descripción	El sistema deberá generar alertas automáticas cuando se detecten actividades sospechosas o potencialmente maliciosas. Estas alertas permitirán a los administradores del sistema tomar medidas rápidas y adecuadas para mitigar posibles riesgos de seguridad.			
Entradas	**Fuente**	**Salida**	**Destino**	**Restricciones**
Datos de eventos de seguridad, detecciones de intrusiones	Sistema de monitoreo de seguridad	Alertas de seguridad	Administradores del sistema	Las alertas deben ser configuradas para priorizar y notificar eventos críticos de seguridad de manera inmediata.
Proceso	1. El sistema monitorea continuamente los eventos de seguridad y las detecciones de intrusiones en busca de actividades sospechosas. 2. Se establecen reglas y criterios para identificar eventos que puedan indicar una amenaza de seguridad. 3. Cuando se detecta una actividad sospechosa, el sistema genera automáticamente una alerta de seguridad. 4. Las alertas son enviadas a los administradores del sistema a través de diversos canales de comunicación, como correos electrónicos, mensajes de texto o notificaciones en la interfaz del sistema.			
Efecto Colateral	• Se agiliza la detección y respuesta a posibles amenazas de seguridad, permitiendo a los administradores del sistema tomar medidas rápidas para proteger los activos de la organización.			

Tabla 9 Registro de logs para auditoría y análisis forense

Código	**Nombre**		**Grado de Necesidad**	
RF-06	Registro de logs para auditoría y análisis forense		Alto	
Descripción	El sistema deberá mantener registros detallados de todas las actividades y eventos relevantes para fines de auditoría y análisis forense. Estos registros proporcionarán una trazabilidad completa de las acciones realizadas en el sistema y facilitarán la investigación de incidentes de seguridad.			
Entradas	**Fuente**	**Salida**	**Destino**	**Restricciones**

Eventos de seguridad, acciones del usuario	Sistema, usuarios	Registros de logs	Almacenamiento seguro	Los registros deben ser protegidos contra modificaciones no autorizadas y estar disponibles para su análisis durante un período de tiempo especificado.
Proceso	1. El sistema registra todas las actividades y eventos relevantes, incluyendo accesos de usuarios, cambios de configuración y detecciones de intrusiones. 2. Los registros son almacenados de forma segura en una ubicación protegida contra accesos no autorizados. 3. Se establecen políticas y procedimientos para el mantenimiento y la retención de registros, de acuerdo con los requisitos regulatorios y de cumplimiento. 4. Los registros están disponibles para su análisis por parte de los administradores del sistema y los equipos de respuesta a incidentes de seguridad.			
Efecto Colateral	• Se garantiza la integridad y disponibilidad de los registros de logs, lo que facilita la auditoría, el análisis forense y la investigación de incidentes de seguridad.			

Tabla 10 Control de acceso a datos sensibles

Código	Nombre			Grado de Necesidad
RF-07	Control de acceso a datos sensibles			Alto
Descripción	El sistema deberá controlar el acceso a los datos sensibles, asegurando que solo usuarios autorizados puedan acceder a ellos según sus roles y privilegios asignados.			
Entradas	Fuente	Salida	Destino	Restricciones
Solicitudes de acceso, políticas de acceso	Usuarios, administradores de seguridad	Autorización de acceso	Datos sensibles	Se deben establecer políticas de acceso granular para garantizar que cada usuario tenga acceso

				solo a los datos necesarios para realizar sus funciones.
Proceso	1. Los usuarios solicitan acceso a datos sensibles a través del sistema. 2. Se verifica la identidad y los privilegios del usuario para determinar si se le debe conceder acceso. 3. Se aplican políticas de acceso granular para garantizar que el usuario solo tenga acceso a los datos necesarios para realizar sus funciones. 4. Se registra y audita cada acceso a datos sensibles para garantizar la trazabilidad y la rendición. 5. Se aplican controles de acceso adicionales, como autenticación multifactorial, para reforzar la seguridad de los datos sensibles.			
Efecto Colateral	• Se garantiza que solo usuarios autorizados puedan acceder a los datos sensibles, protegiéndolos contra accesos no autorizados y posibles fugas de información.			

3.1.2 Requerimientos No Funcionales

Tabla 11 Escalabilidad

Código	Nombre	Grado de Necesidad
RNF-01	Escalabilidad	Bajo
Descripción	. El sistema debe ser capaz de manejar un crecimiento en el número de usuarios y datos sin pérdida de rendimiento.	

Tabla 12 Rendimiento

Código	Nombre	Grado de Necesidad
RNF-02	Rendimiento	Bajo
Descripción	El sistema debe responder a las solicitudes de los usuarios en menos de 2 segundos.	

Tabla 13 Usabilidad

Código	Nombre	Grado de Necesidad
RNF-03	Usabilidad	Bajo
Descripción	El sistema debe tener una interfaz intuitiva y fácil de usar para minimizar la necesidad de capacitación.	

Tabla 14 Disponibilidad

Código	**Nombre**	**Grado de Necesidad**
RNF-04	Disponibilidad	Bajo
Descripción	El sistema debe estar disponible 99.9% del tiempo, excluyendo tiempos de mantenimiento planificado.	

Tabla 15 Compatibilidad

Código	**Nombre**	**Grado de Necesidad**
RNF-05	Compatibilidad	Bajo
Descripción	El sistema debe ser compatible con los navegadores web más utilizados (Chrome, Firefox, Edge).	

Tabla 16 Portabilidad

Código	**Nombre**	**Grado de Necesidad**
RNF-06	Portabilidad	Bajo
Descripción	El sistema debe ser capaz de ejecutarse en diferentes plataformas (Windows, macOS, Linux).	

Tabla 17 Accesibilidad

Código	**Nombre**	**Grado de Necesidad**
RNF-07	Accesibilidad	Bajo

Descripción	El sistema debe cumplir con los estándares de accesibilidad para personas con discapacidades.

3.2 Roles, Responsabilidades y Permisos

- **Administrador del Sistema**

  Responsabilidades: Configuración del sistema, gestión de usuarios y permisos, mantenimiento de la base de datos, y supervisión del rendimiento del sistema.

  Permisos: Acceso completo a todas las funcionalidades del sistema.

- **Gestor de Seguridad**

  Responsabilidades: Supervisión de incidentes de seguridad, implementación de políticas de seguridad, y coordinación de auditorías internas.

  Permisos: Acceso a la gestión de incidentes, reportes y auditorías.

- **Coordinador de Capacitación**

  Responsabilidades: Diseño y programación de cursos de capacitación, seguimiento de la asistencia y evaluación de los empleados.

  Permisos: Acceso a la gestión de capacitaciones y reportes de progreso.

- **Responsable de EPP**

  Responsabilidades: Gestión de la entrega y estado de los equipos de protección personal, asegurando que todos los empleados tengan los EPP necesarios.

  Permisos: Acceso a la gestión de EPP y reportes asociados.

- **Auditor Interno**

  Responsabilidades: Realización de auditorías internas, evaluación de riesgos y cumplimiento de normativas.

  Permisos: Acceso a la planificación y registro de auditorías, así como a la evaluación de riesgos.

- **Analista de Datos de Seguridad**

  Responsabilidades: Análisis de datos relacionados con incidentes y accidentes, generación de reportes y recomendaciones basadas en datos.

  Permisos: Acceso a reportes, historial de incidentes, y herramientas de análisis.

- **Empleados**

  Responsabilidades: Reportar incidentes, asistir a capacitaciones y utilizar adecuadamente los EPP.

  Permisos: Acceso limitado para registrar incidentes y consultar su propio historial de capacitaciones.

- **Responsable de Comunicación**

  Responsabilidades: Gestionar las comunicaciones relacionadas con incidentes de seguridad, notificaciones a los responsables y divulgación de información.

  Permisos: Acceso a la gestión de notificaciones y reportes.

3.3 Scritp de la base de datos.

```
USE [salud]

GO

/****** Object:  Table [dbo].[accidentes]    Script Date: 29/10/2024 3:45:23 p. m. ******/

SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

CREATE TABLE [dbo].[accidentes](

        [id] [int] IDENTITY(1,1) NOT NULL,

        [empleado_id] [int] NOT NULL,

        [fecha_accidente] [datetime] NOT NULL,

        [causa] [nvarchar](255) NOT NULL,

        [parte_afectada] [nvarchar](50) NOT NULL,

        [fractura_id] [int] NULL,

        [registrado_por] [int] NOT NULL,
```

```
	[fecha_creacion] [datetime] NOT NULL,

	[creado_por] [int] NULL,

PRIMARY KEY CLUSTERED

(

	[id] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY]

GO

/****** Object:  Table [dbo].[Capacitaciones]    Script Date: 29/10/2024 3:45:23 p. m. ******/

SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

CREATE TABLE [dbo].[Capacitaciones](

	[capacitacion_id] [int] IDENTITY(1,1) NOT NULL,

	[titulo] [nvarchar](100) NOT NULL,

	[descripcion] [nvarchar](255) NULL,

	[fecha_inicio] [datetime] NOT NULL,

	[fecha_fin] [datetime] NOT NULL,

	[usuario_registro] [int] NOT NULL,

	[fecha_creacion] [datetime] NOT NULL,

	[creado_por] [int] NULL,

PRIMARY KEY CLUSTERED

(
```

```
	[capacitacion_id] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY]

GO

/****** Object:  Table [dbo].[Capacitaciones_Empleados]    Script Date: 29/10/2024 3:45:23
p. m. ******/

SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

CREATE TABLE [dbo].[Capacitaciones_Empleados](

	[id] [int] IDENTITY(1,1) NOT NULL,

	[empleado_id] [int] NOT NULL,

	[capacitacion_id] [int] NOT NULL,

	[fecha_asistencia] [datetime] NOT NULL,

	[progreso] [decimal](5, 2) NOT NULL,

PRIMARY KEY CLUSTERED

(

	[id] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY]

GO

/****** Object:  Table [dbo].[empleados]    Script Date: 29/10/2024 3:45:23 p. m. ******/
```

```
SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

CREATE TABLE [dbo].[empleados](

        [empleado_id] [int] IDENTITY(1,1) NOT NULL,

        [nombre] [nvarchar](50) NOT NULL,

        [apellido] [nvarchar](50) NOT NULL,

        [email] [nvarchar](100) NOT NULL,

        [telefono] [nvarchar](15) NULL,

        [cargo] [nvarchar](50) NULL,

        [fecha_nacimiento] [datetime] NULL,

        [imagen] [varbinary](max) NULL,

        [estado_civil] [nvarchar](20) NULL,

        [contacto_emergencia_nombre] [nvarchar](50) NULL,

        [contacto_emergencia_telefono] [nvarchar](15) NULL,

        [documento_identidad] [nvarchar](20) NOT NULL,

        [EPS] [nvarchar](50) NULL,

        [ARL] [nvarchar](50) NULL,

        [usuario_registro_id] [int] NOT NULL,

        [fecha_creacion] [datetime] NOT NULL,

        [creado_por] [int] NULL,

PRIMARY KEY CLUSTERED

(

        [empleado_id] ASC
```

```
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY],

UNIQUE NONCLUSTERED

(

        [email] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

GO

/****** Object:  Table [dbo].[Fracturas]    Script Date: 29/10/2024 3:45:23 p. m. ******/

SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

CREATE TABLE [dbo].[Fracturas](

        [id] [int] IDENTITY(1,1) NOT NULL,

        [parte_cuerpo_id] [int] NOT NULL,

        [tipo_fractura] [nvarchar](100) NOT NULL,

        [descripcion] [nvarchar](255) NULL,

        [fecha_creacion] [datetime] NOT NULL,

        [creado_por] [int] NULL,

PRIMARY KEY CLUSTERED

(

        [id] ASC
```

```
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY]

GO

/****** Object:  Table [dbo].[Incapacidades]    Script Date: 29/10/2024 3:45:23 p. m. ******/

SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

CREATE TABLE [dbo].[Incapacidades](

        [id] [int] IDENTITY(1,1) NOT NULL,

        [accidente_id] [int] NOT NULL,

        [fractura_id] [int] NULL,

        [dias_incapacidad] [int] NOT NULL,

        [fecha_inicio] [datetime] NOT NULL,

        [fecha_fin] [datetime] NOT NULL,

        [fecha_creacion] [datetime] NOT NULL,

        [creado_por] [int] NULL,

PRIMARY KEY CLUSTERED

(

        [id] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY]

GO
```

```
/****** Object:  Table [dbo].[PartesCuerpo]    Script Date: 29/10/2024 3:45:23 p. m. ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[PartesCuerpo](
	[id] [int] IDENTITY(1,1) NOT NULL,
	[nombre] [nvarchar](100) NOT NULL,
	[fecha_creacion] [datetime] NOT NULL,
	[creado_por] [int] NULL,
PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[TiposUsuario]    Script Date: 29/10/2024 3:45:23 p. m. ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[TiposUsuario](
	[tipo_usuario_id] [int] IDENTITY(1,1) NOT NULL,
	[nombre] [nvarchar](50) NOT NULL,
```

```
	[descripcion] [nvarchar](255) NULL,
	[fecha_creacion] [datetime] NOT NULL,
	[creado_por] [int] NOT NULL,
PRIMARY KEY CLUSTERED
(
	[tipo_usuario_id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[usuarios]    Script Date: 29/10/2024 3:45:23 p. m. ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[usuarios](
	[id] [int] IDENTITY(1,1) NOT NULL,
	[nombre] [nvarchar](50) NOT NULL,
	[apellido] [nvarchar](50) NOT NULL,
	[email] [nvarchar](100) NOT NULL,
	[telefono] [nvarchar](15) NULL,
	[contrasena] [nvarchar](255) NOT NULL,
	[confirmar_contrasena] [nvarchar](255) NOT NULL,
	[tipo_usuario_id] [int] NOT NULL,
	[fecha_creacion] [datetime] NOT NULL,
```

```
	[creado_por] [int] NULL,

PRIMARY KEY CLUSTERED

(

	[id] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY],

UNIQUE NONCLUSTERED

(

	[email] ASC

)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF)
ON [PRIMARY]

) ON [PRIMARY]

GO

ALTER TABLE [dbo].[accidentes] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[Capacitaciones] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[Capacitaciones_Empleados] ADD  DEFAULT (getdate()) FOR [fecha_asistencia]

GO

ALTER TABLE [dbo].[empleados] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[Fracturas] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[Incapacidades] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO
```

```
ALTER TABLE [dbo].[PartesCuerpo] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[TiposUsuario] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[usuarios] ADD  DEFAULT (getdate()) FOR [fecha_creacion]

GO

ALTER TABLE [dbo].[accidentes]  WITH CHECK ADD FOREIGN KEY([empleado_id])

REFERENCES [dbo].[empleados] ([empleado_id])

GO

ALTER TABLE [dbo].[accidentes]  WITH CHECK ADD FOREIGN KEY([fractura_id])

REFERENCES [dbo].[Fracturas] ([id])

GO

ALTER TABLE [dbo].[accidentes]  WITH CHECK ADD FOREIGN KEY([registrado_por])

REFERENCES [dbo].[usuarios] ([id])

GO

ALTER TABLE [dbo].[Capacitaciones]  WITH CHECK ADD FOREIGN KEY([usuario_registro])

REFERENCES [dbo].[usuarios] ([id])

GO

ALTER TABLE [dbo].[Capacitaciones_Empleados]  WITH CHECK ADD FOREIGN
KEY([capacitacion_id])

REFERENCES [dbo].[Capacitaciones] ([capacitacion_id])

GO

ALTER TABLE [dbo].[Capacitaciones_Empleados]  WITH CHECK ADD FOREIGN KEY([empleado_id])

REFERENCES [dbo].[empleados] ([empleado_id])

GO

ALTER TABLE [dbo].[empleados]  WITH CHECK ADD FOREIGN KEY([usuario_registro_id])
```

```
REFERENCES [dbo].[usuarios] ([id])

GO

ALTER TABLE [dbo].[Fracturas]  WITH CHECK ADD FOREIGN KEY([parte_cuerpo_id])

REFERENCES [dbo].[PartesCuerpo] ([id])

GO

ALTER TABLE [dbo].[Incapacidades]  WITH CHECK ADD FOREIGN KEY([accidente_id])

REFERENCES [dbo].[accidentes] ([id])

GO

ALTER TABLE [dbo].[Incapacidades]  WITH CHECK ADD FOREIGN KEY([fractura_id])

REFERENCES [dbo].[Fracturas] ([id])

GO

ALTER TABLE [dbo].[usuarios]  WITH CHECK ADD FOREIGN KEY([tipo_usuario_id])

REFERENCES [dbo].[TiposUsuario] ([tipo_usuario_id])

GO

ALTER TABLE [dbo].[Capacitaciones_Empleados]  WITH CHECK ADD CHECK  (([progreso]>=(0) AND
[progreso]<=(100)))

GO
```

3.4 Descripción Casos de uso

Código	01
Nombre	Ingresar usuario
Descripción	Permite al usuario ingresar al sistema de la empresa, el cual es autenticado y autorizado para la utilización de este.
Actores	Administrador
Precondición	El Administrador debe tener una cuenta por defecto con su respectiva contraseña y nombre de usuario
Flujo normal	1. Ingresar al sistema nombre de usuario 2. Ingresar al sistema contraseña 3. El sistema Valida los datos 4. El sistema Guarda al usuario 5. Presiona el botón de inicio de Sesión 6. Ingresar a la interfaz de usuario
Excepciones	7. Excepción 3) 3.1 Datos no validos 3.2 Ya existe usuario 6. Volver al 1)

Tabla 18 Login

Código	02
Nombre	Gestión de eventos
Descripción	Realizar la gestión de los eventos presentados por parte de los trabajadores de la empresa.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema.
Flujo normal	1. Consultar al empleado. 2. Gestionar datos del evento. 3. El sistema valida los datos 4. El sistema guarda los cambios.
Excepciones	5. Excepción 1) 1.1 Datos no validos 1.2 No existen eventos del empleado. 6. Volver al 1)

Tabla 19 Gestión Eventos

Código	03
Nombre	Gestionar Diagnostico
Descripción	Realizar la gestión de los diagnósticos de cada evento presentado por parte de los trabajadores de la empresa.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado y sus respectivos eventos.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Gestionar diagnóstico. 4. El sistema valida los datos 5. El sistema guarda los cambios.
Excepciones	6. Excepción 1) 1.1 Datos no validos 7. Excepción 2) 2.1 No existen eventos del empleado.

Tabla 20 Gestionar Diagnostico

Código	04
Nombre	Gestionar factores de riesgo.
Descripción	Realizar la gestión de los factores de riesgo por cada diagnóstico de un evento.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado y sus respectivos eventos.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Consultar Diagnostico. 4. Gestionar factores de riesgo. 5. El sistema valida los datos 6. El sistema guarda los cambios.
Excepciones	7. Excepción 1) 1.1 Datos no validos 8. Excepción 2) 2.1 No existen eventos del empleado. 9. Excepción 3) 3.1 No existen diagnósticos.

Tabla 21Gestionar Factores de Riesgos

Código	05
Nombre	Gestionar alta médica.
Descripción	Realizar gestión de la alta médica de un empleado.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado y sus respectivos eventos.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Gestionar alta médica. 4. El sistema valida los datos 5. El sistema guarda los cambios.
Excepciones	6. Excepción 1) 1.1 Datos no validos 7. Excepción 2) 2.1 No existen eventos del empleado.

Tabla 22 Gestionar alta médica.

Código	06
Nombre	Gestionar recomendaciones.
Descripción	Realizar la gestión de las recomendaciones médicas de los eventos presentados por los empleados.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado y sus respectivos eventos.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Gestionar recomendaciones. 4. El sistema valida los datos 5. El sistema guarda los cambios.
Excepciones	6. Excepción 1) 1.1 Datos no validos 7. Excepción 2) 2.1 No existen eventos del empleado.

Tabla 23 Gestionar recomendaciones.

Código	07
Nombre	Gestionar restricciones.
Descripción	Realizar la gestión de las restricciones médicas de los eventos presentados por los empleados.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado y sus respectivos eventos.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Gestionar restricciones. 4. El sistema valida los datos 5. El sistema guarda los cambios.
Excepciones	6. Excepción 1) 1.1 Datos no validos 7. Excepción 2) 2.1 No existen eventos del empleado.

Tabla 24 Gestionar restricciones.

Código	08
Nombre	Gestionar seguimiento.
Descripción	Realizar la gestión de los seguimientos de las recomendaciones y/o restricciones médicas de los eventos de un empleado.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado, un evento y sus respectivas recomendaciones y/o restricciones médicas.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Consultar recomendaciones y restricciones. 4. Gestionar seguimiento. 5. El sistema valida los datos 6. El sistema guarda los cambios.
Excepciones	7. Excepción 1) 1.1 Datos no validos 8. Excepción 2) 2.1 No existen eventos del empleado. 9. Excepción 3) 3.1 No existen recomendaciones y restricciones.

Tabla 25 Gestionar Seguimiento

Código	09
Nombre	Gestionar reubicación.
Descripción	Realizar la gestión de las reubicaciones de acuerdo con las recomendaciones y/o restricciones médicas de los eventos de un empleado.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado, un evento y sus respectivas recomendaciones y/o restricciones médicas.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Consultar recomendaciones y restricciones. 4. Gestionar reubicación 5. El sistema valida los datos 6. El sistema guarda los cambios.
Excepciones	7. Excepción 1) 1.1 Datos no validos 8. Excepción 2) 2.1 No existen eventos del empleado. 9. Excepción 3) 3.1 No existen recomendaciones y restricciones.

Tabla 26 Gestionar Reubicación

Código	10
Nombre	Gestionar Incapacidad.
Descripción	Realizar la gestión de la incapacidad de acuerdo las órdenes médicas para los respectivos eventos de un empleado.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado, un evento y sus respectivas recomendaciones y/o restricciones médicas.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Gestionar incapacidad. 4. El sistema valida los datos 5. El sistema guarda los cambios.
Excepciones	6. Excepción 1) 1.1 Datos no validos 8. Excepción 2) 2.1 No existen eventos del empleado.

Tabla 27 Gestionar Incapacidad.

Código	11
Nombre	Gestionar Evaluación.
Descripción	Realizar la gestión de la evaluación realizada por entidades externas.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado, un evento y sus respectivas recomendaciones y/o restricciones médicas.
Flujo normal	1. Consultar al empleado. 2. Consultar datos del evento. 3. Gestionar evaluación. 4. El sistema valida los datos 5. El sistema guarda los cambios.
Excepciones	6. Excepción 1) 1.1 Datos no validos 8. Excepción 2) 2.1 No existen eventos del empleado.

Tabla 28 Gestionar Evaluación.

Código	12
Nombre	Gestionar Reportes
Descripción	Permite al Salubrista consultar de manera general y especifica la información del estado actual de los empleados referente a los eventos generados por accidentes laborales.
Actores	Analista de seguridad y salud en el trabajo.
Precondición	El analista de seguridad y salud en el trabajo debe estar autenticado en el sistema, y además tiene que existir el empleado, un evento y sus respectivas recomendaciones y/o restricciones médicas.
Flujo normal	1. Consultar reporte general. 2. Consultar datos de todos los empleados. 3. El sistema muestra los datos
Excepciones	4. Excepción 1) 1.1 Datos no validos 8. Excepción 2) 2.1 No existen eventos de los empleados. 9. Excepción 3) 3.1 No existen eventos del empleado específico.

Tabla 29 Gestionar Reportes

3.5 Diagramas

3.5.1 Diagramas de Casos de Uso

Figura 10 Login

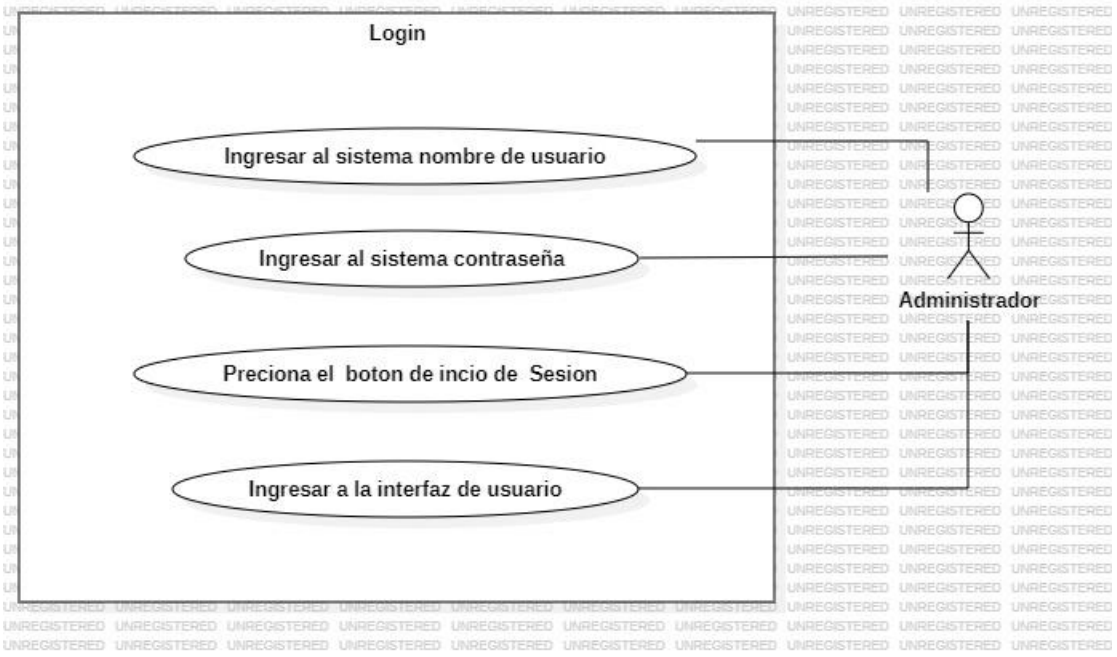


Figura Gestión de Eventos

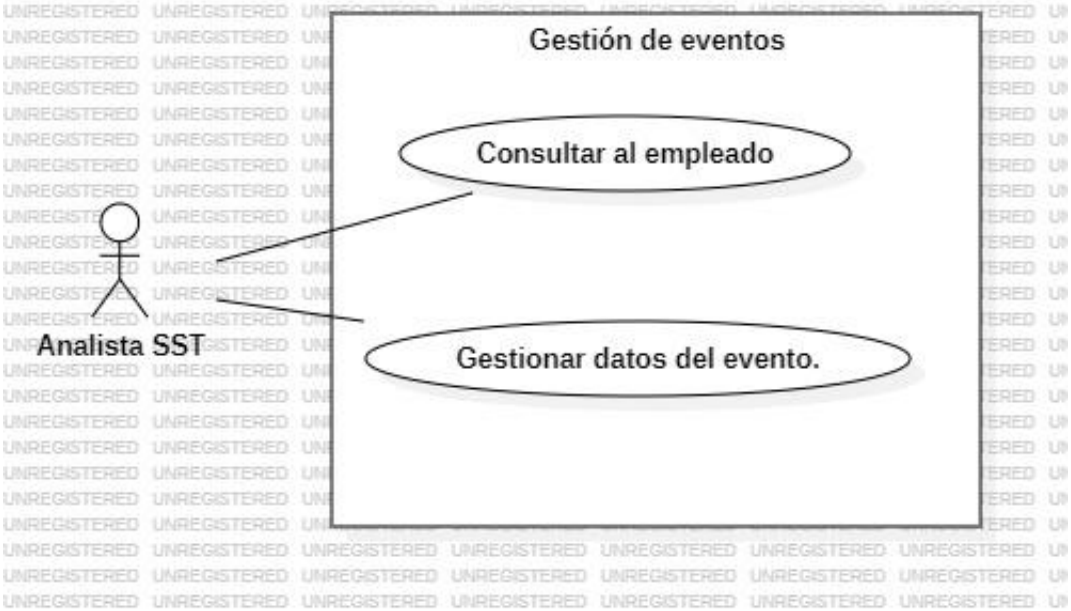


Figura 11 Gestión de diagnostico

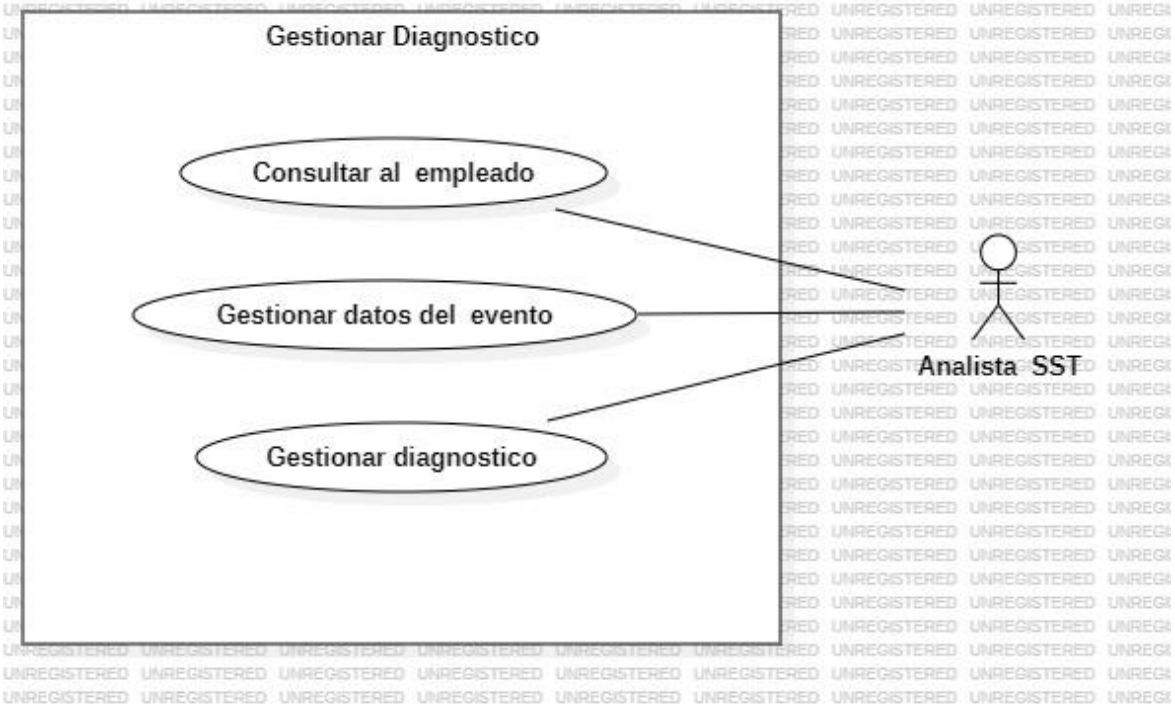


Figura 12 Gestión Factor de Riesgo

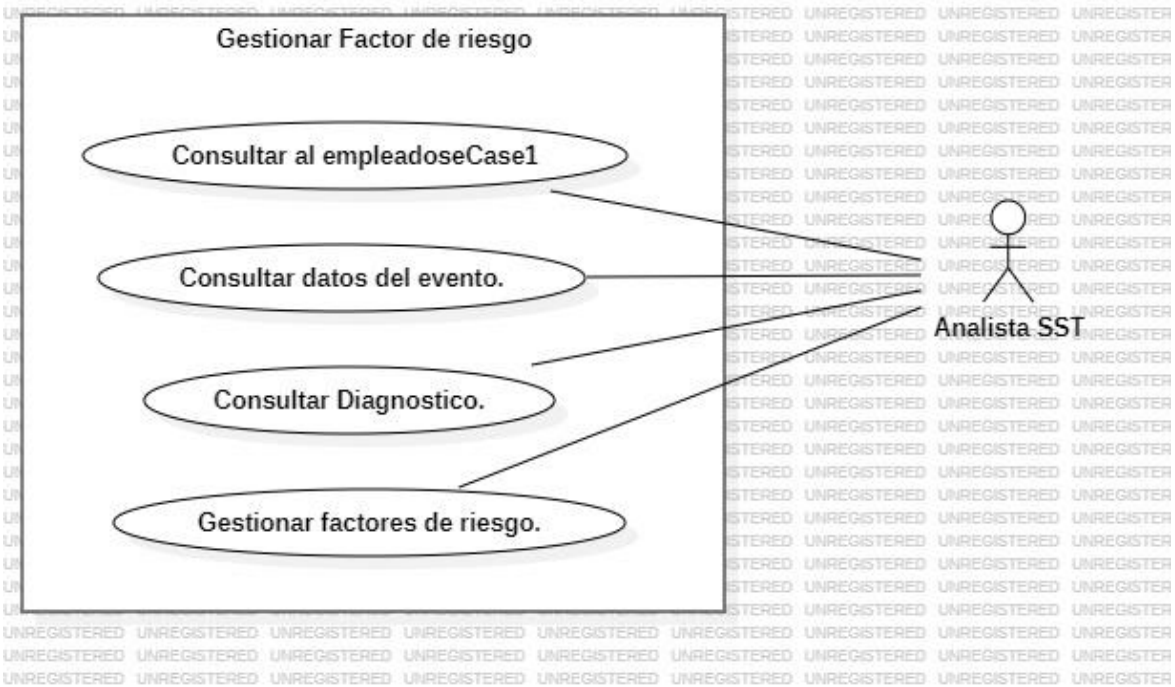


Figura 13 Gestionar alta médica

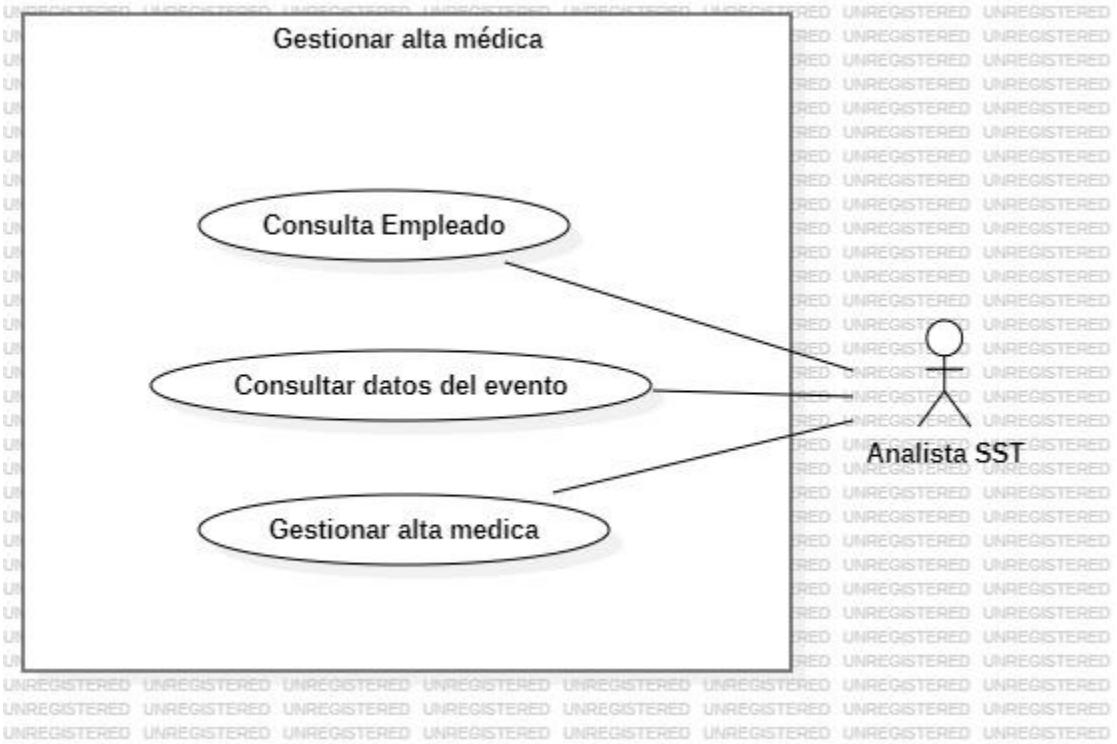


Figura 14 Gestionar recomendaciones

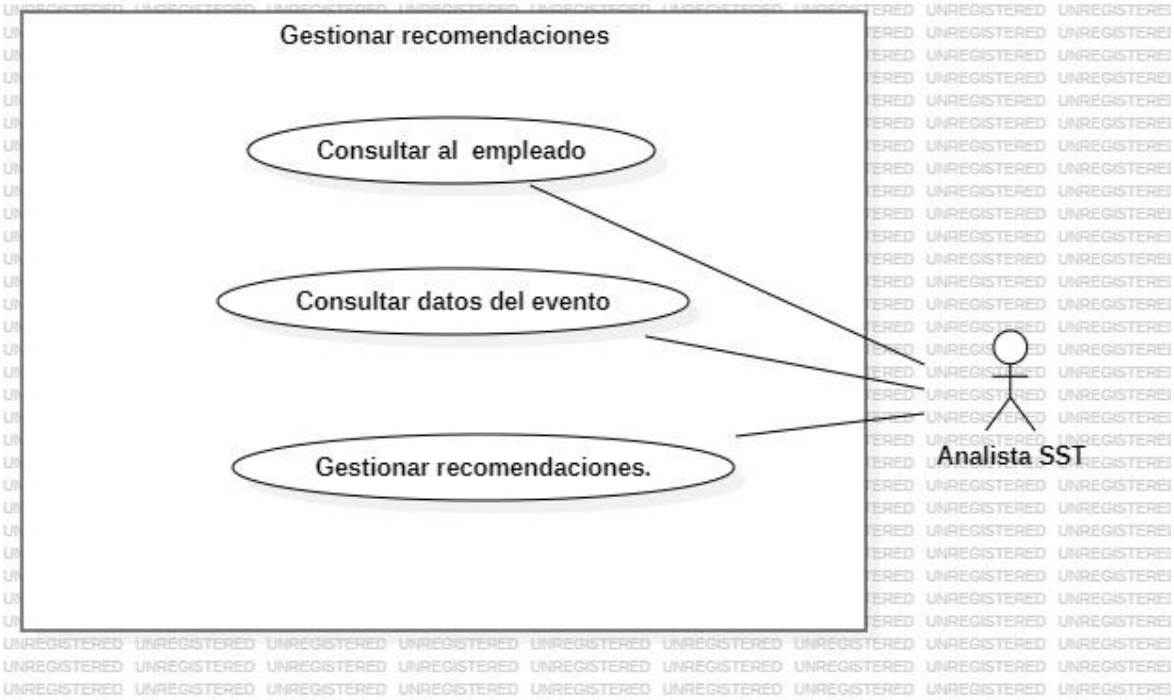
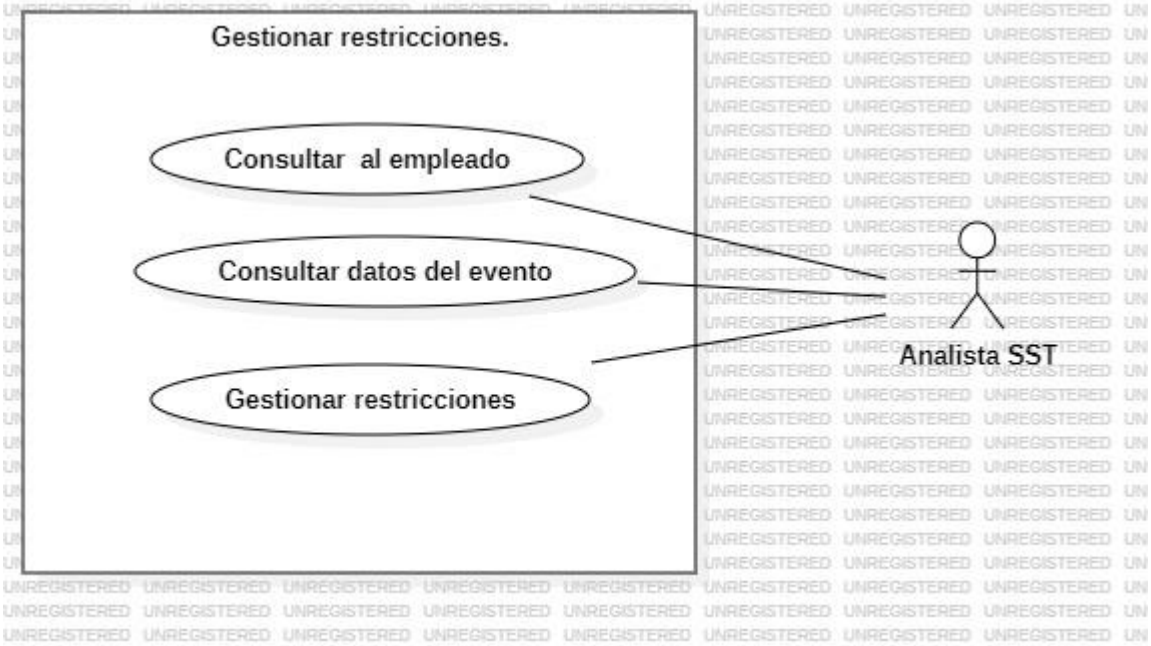


Figura 15 Gestionar restricciones



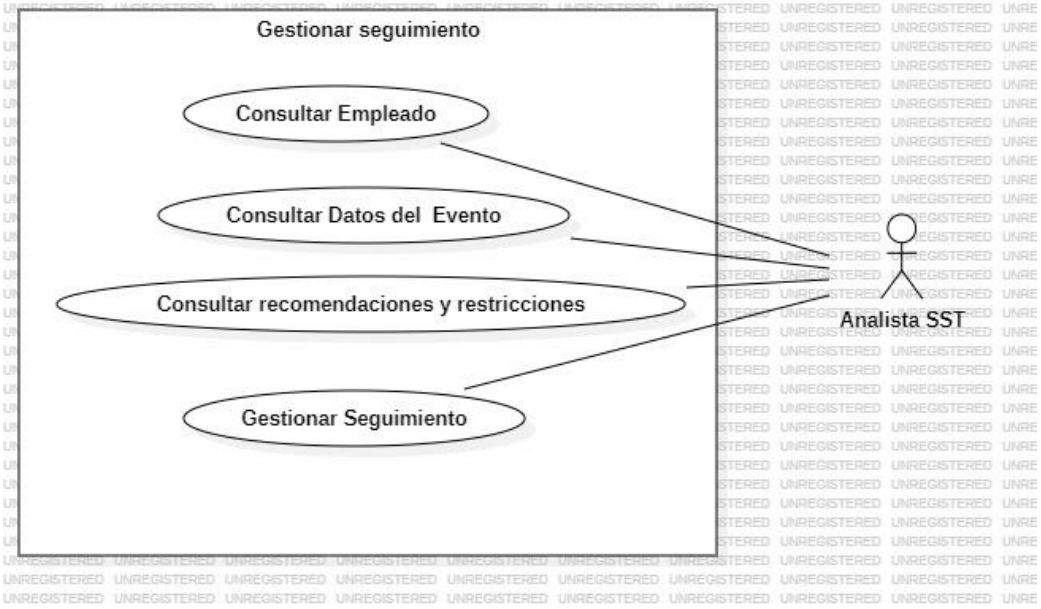


Figura 16 Gestionar Seguimiento

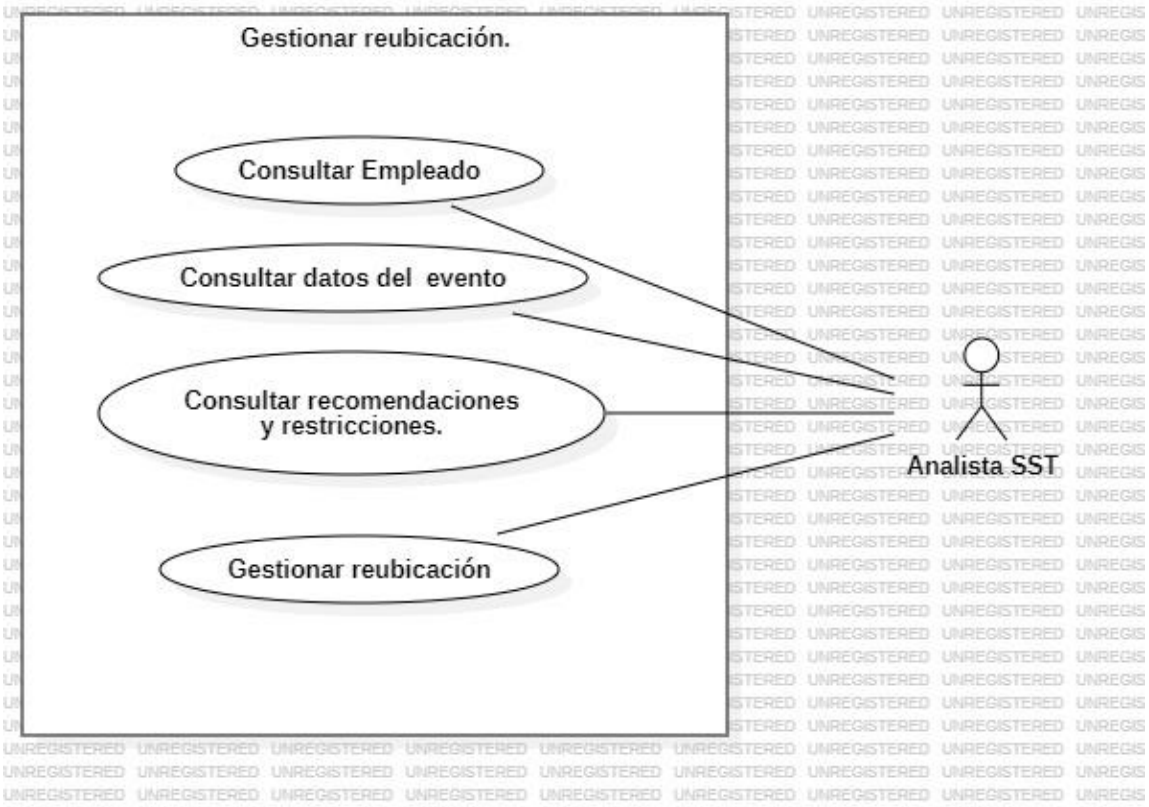


Figura 17 Gestionar reubicación

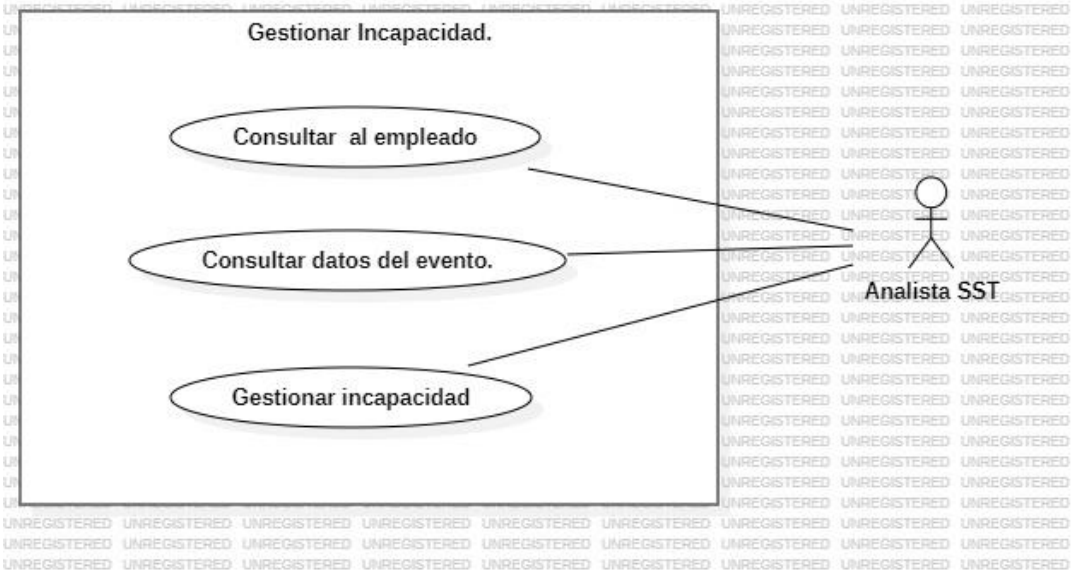


Figura 18 Gestionar Incapacidad.

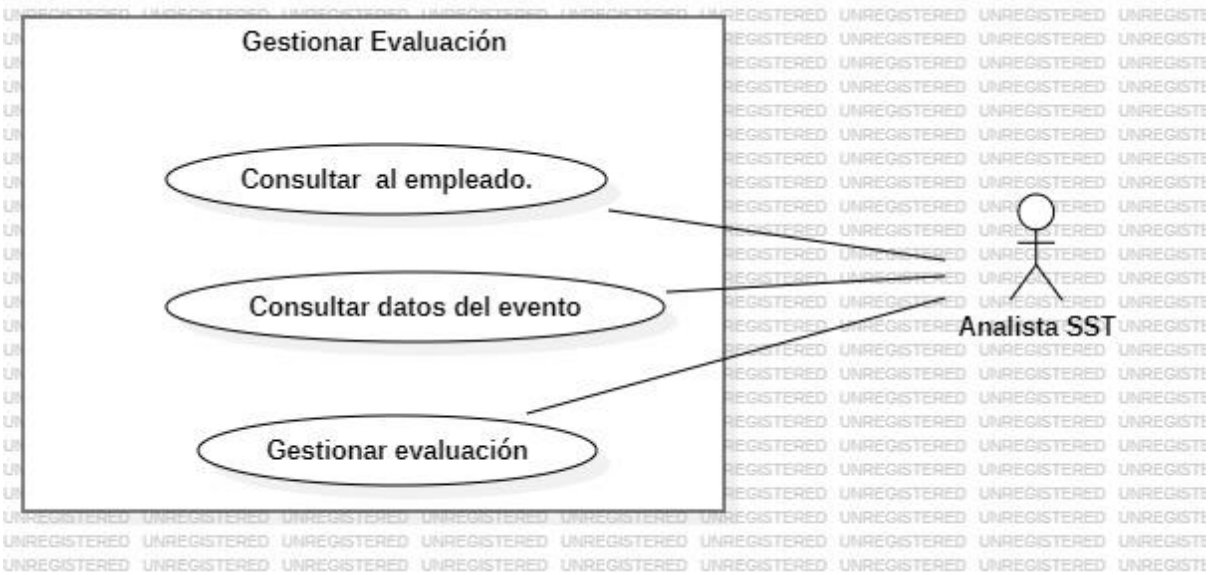


Figura 19 Gestionar Evaluación.

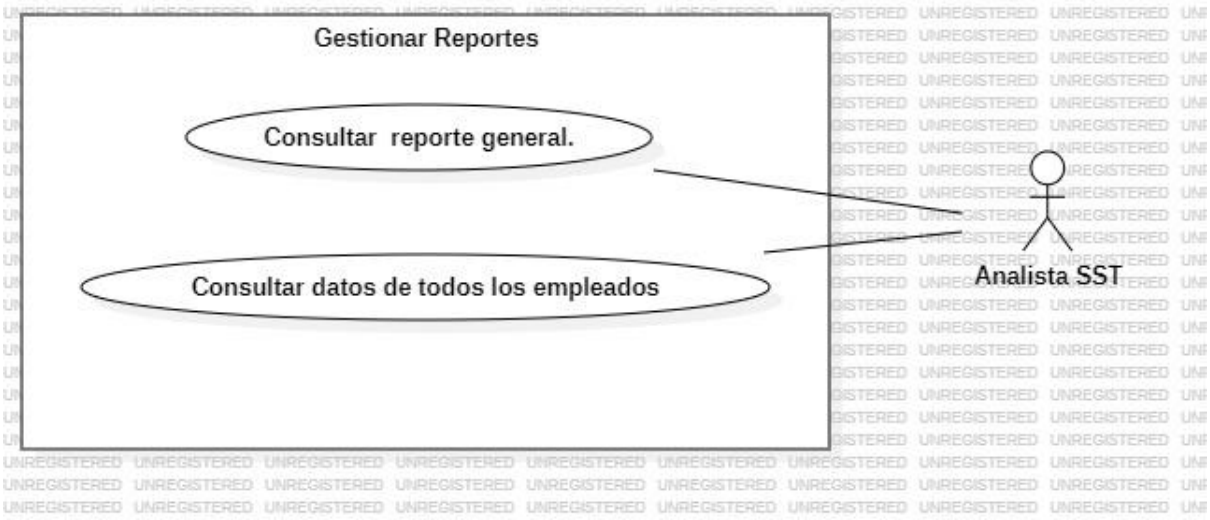


Figura 20 Gestionar Reportes

3.5.2 Diagrama de Clases

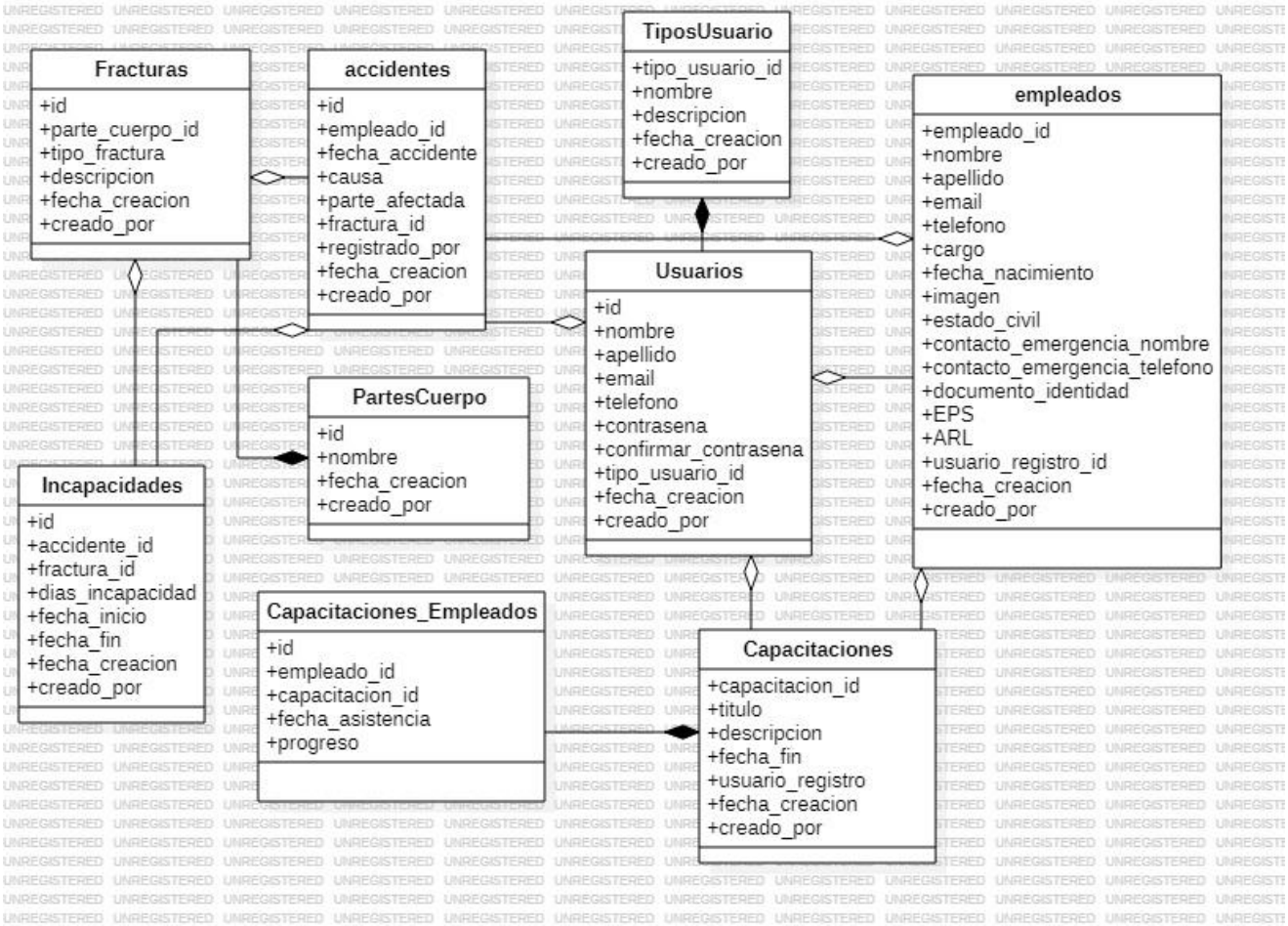


Figura 21 Diagrama de Clases

3.5.3 Diagrama Base de Datos

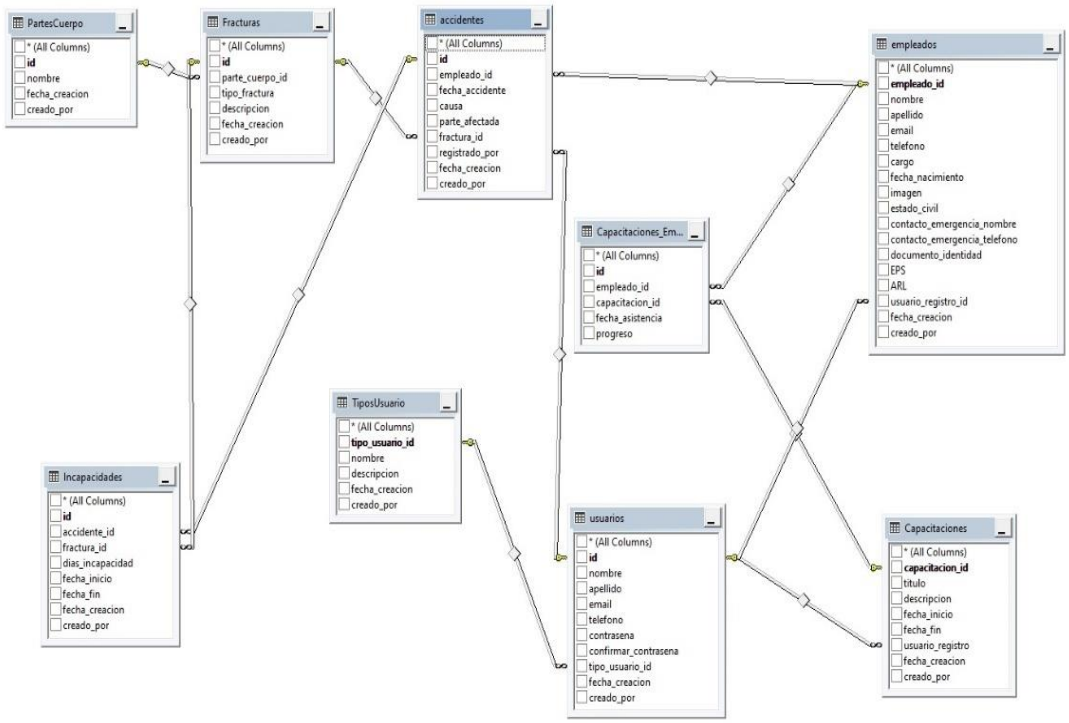
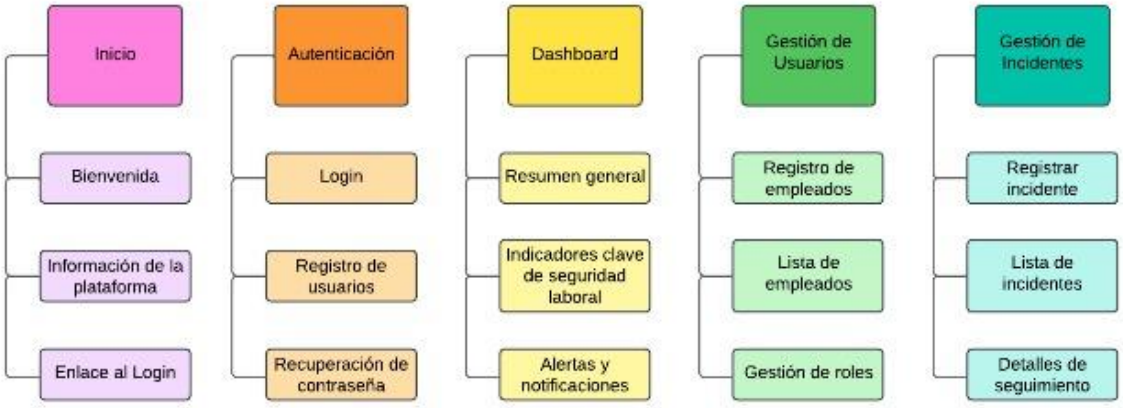
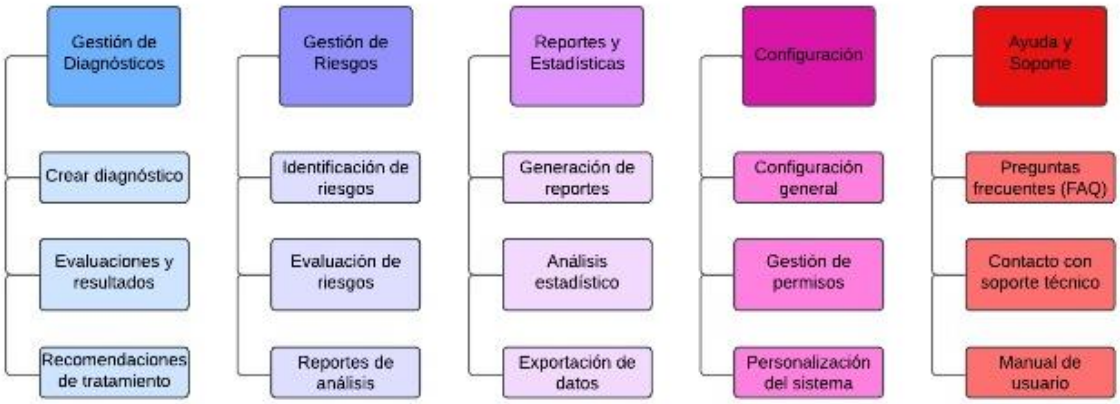


Figura 22 Diagrama Base de Datos

3.5.4 Diagrama de procesos

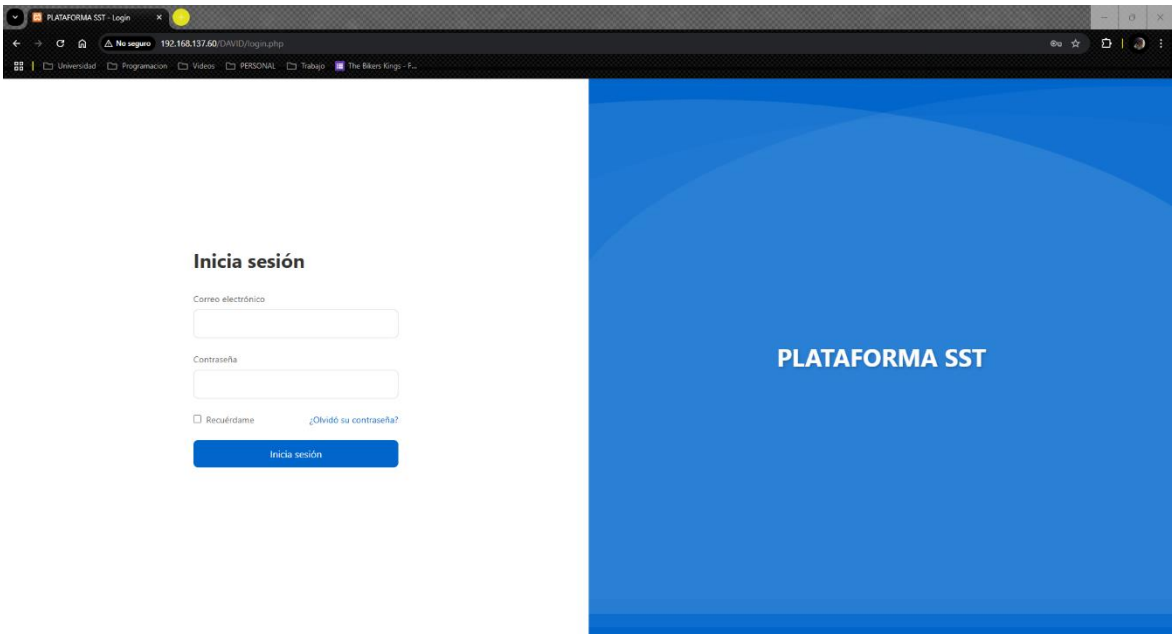
Figura 23 Diagrama de Procesos




Gestión de Diagnósticos
Crear diagnóstico
Evaluaciones y resultados
Recomendaciones de tratamiento
Gestión de Riesgos
Identificación de riesgos
Evaluación de riesgos
Reportes de análisis
Reportes y Estadísticas
Generación de reportes
Análisis estadístico
Exportación de datos
Configuración
Configuración general
Gestión de permisos
Personalización del sistema
Ayuda y Soporte
Preguntas frecuentes (FAQ)
Contacto con soporte técnico
Manual de usuario

3.6 Vista Del Software

Figura 24 Login



Login : inicio de Sesión del aplicativo

Figura 25 Interfaz de inicio

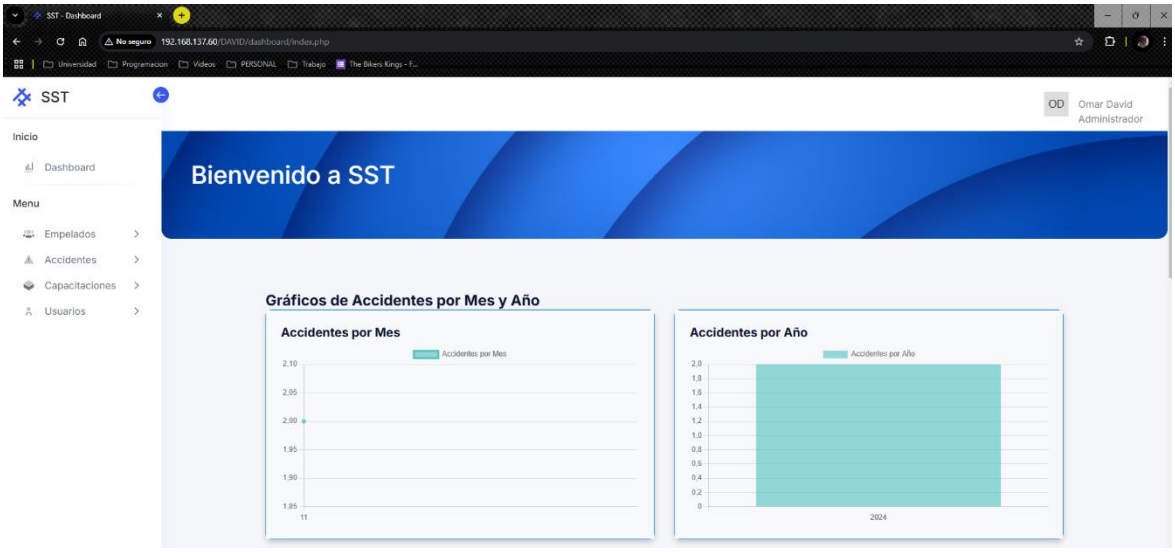
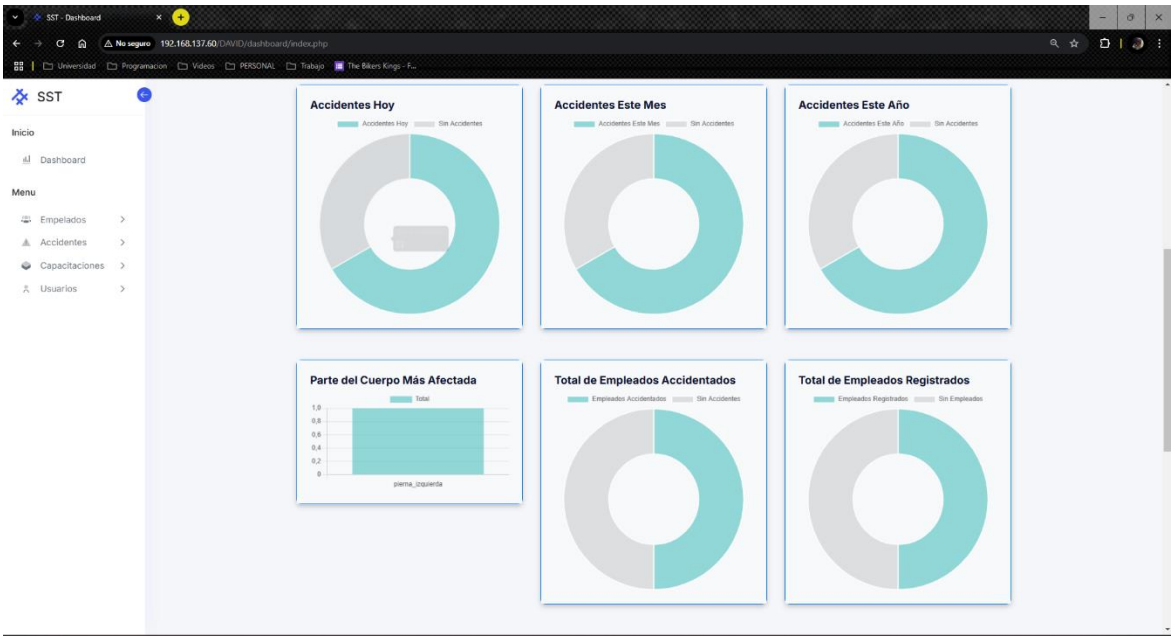
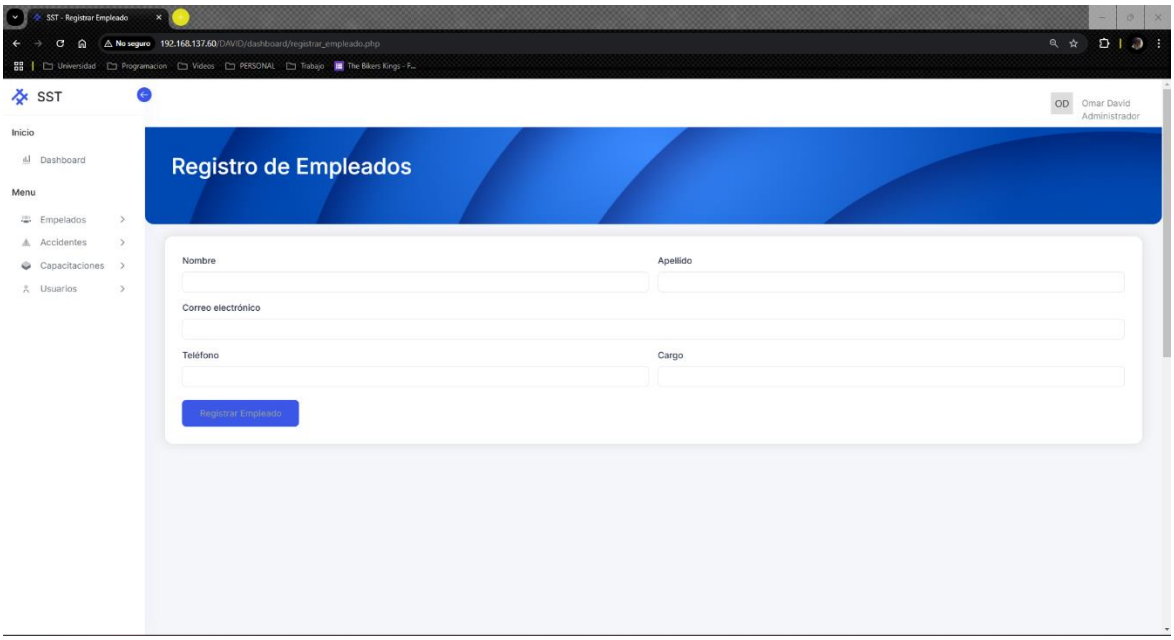


Figura 26 Dashboard



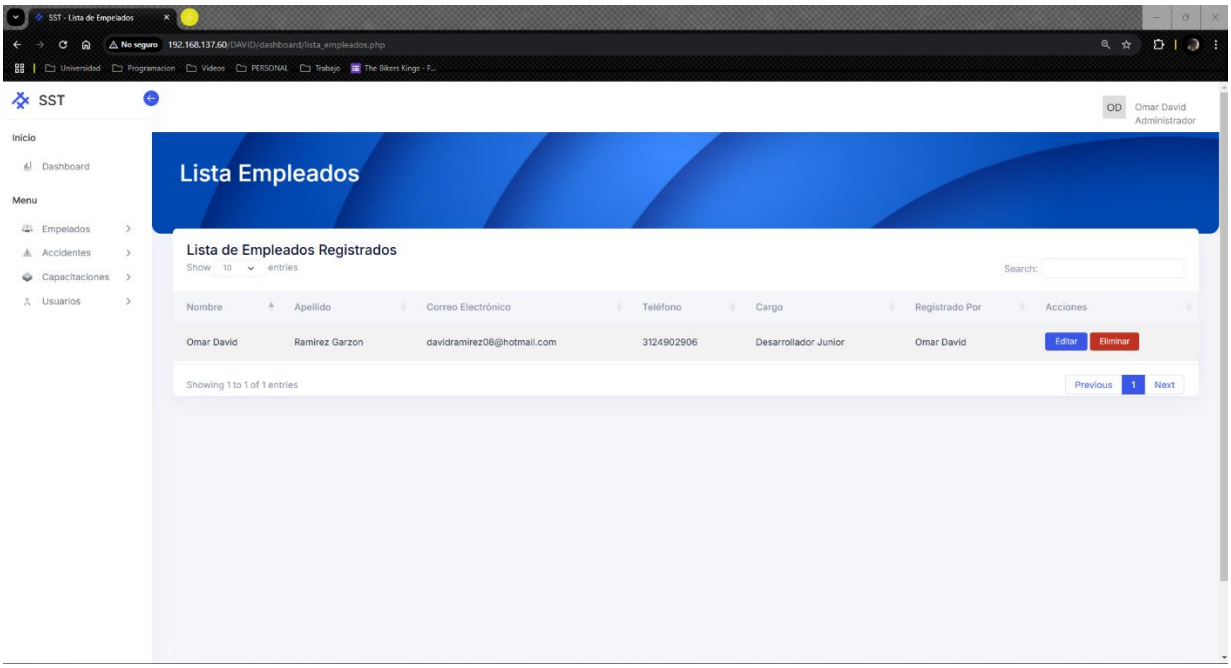
Dashboard: página principal con reportadores e indicadores de incidencias.

Figura 27 Registro de Empleados



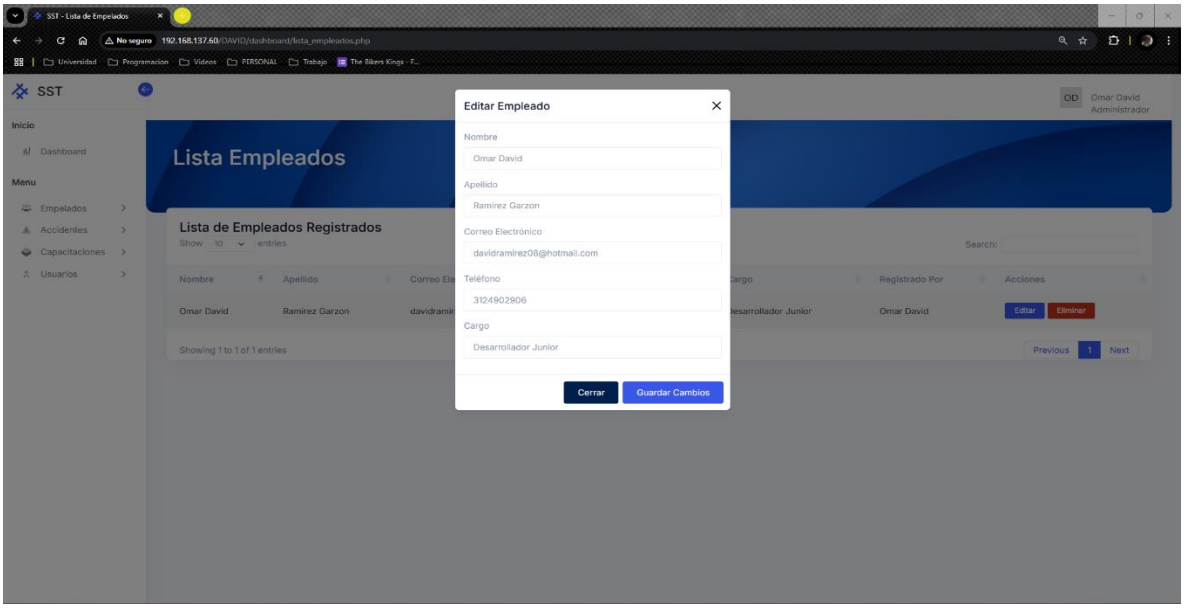
Registro de Empleados: Página con un formulario para registrar empleados, incluyendo campos para datos personales.

Figura 28 Lista de Empleados



Lista de Empleados: Página que muestra la información de los empleados, incluyendo la cantidad total de empleados y una barra de búsqueda para facilitar la localización de registros específicos.

Figura 29 Editar Empleados



Lista Editar Empleado: Función para poder editar los empleados de la compañía

Figura 29 Registrar Accidente

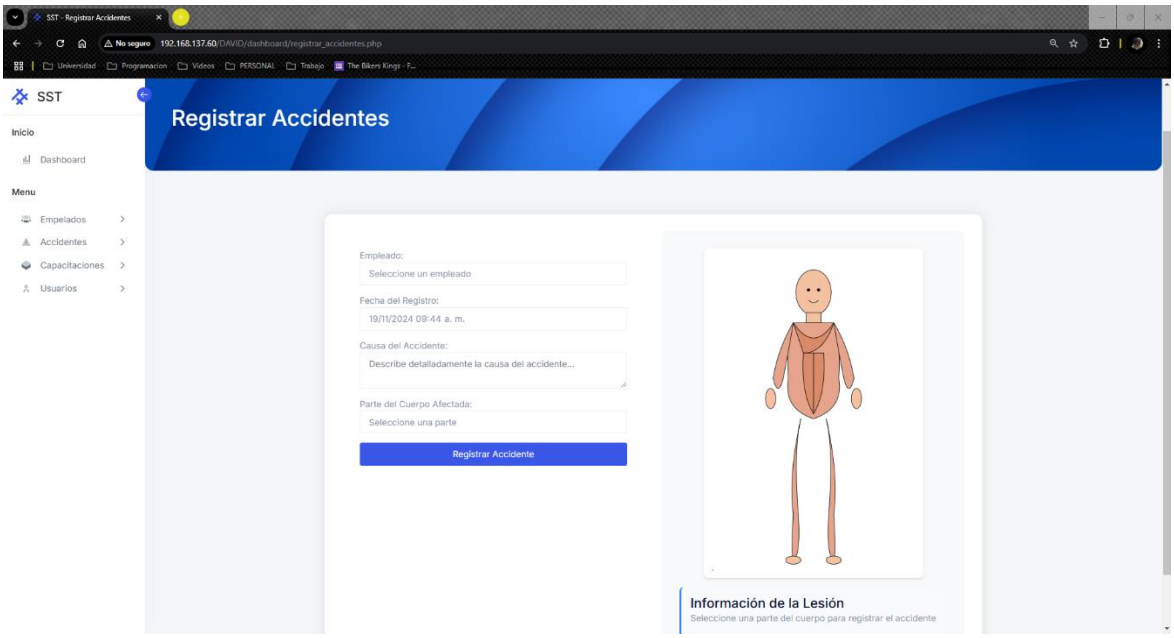
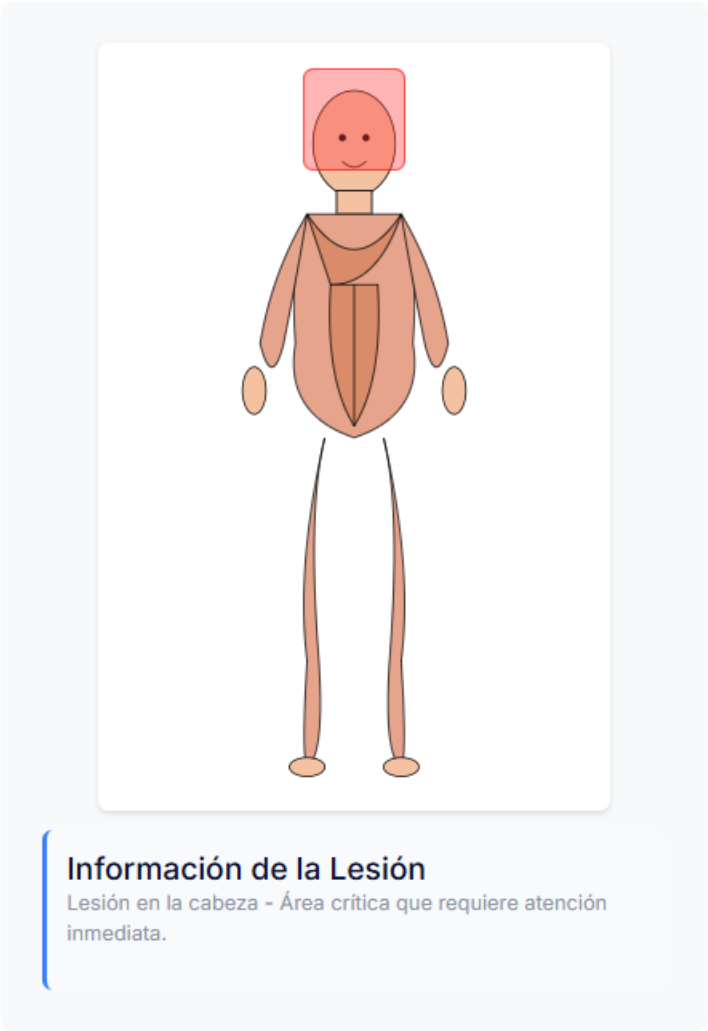
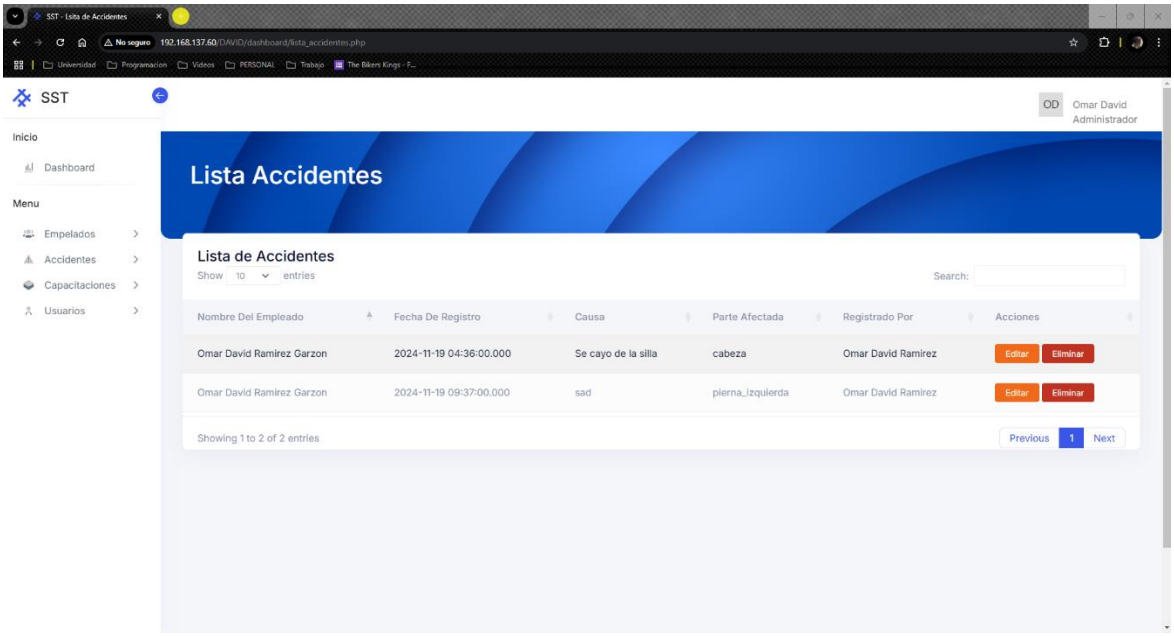


Figura 30 Registrar Accidente



Registrar Accidente: Página para registrar un accidente, donde al seleccionar la zona afectada, se resalta en una imagen del cuerpo humano la parte correspondiente, permitiendo una identificación visual clara de la lesión.

Figura 31 Lista de Accidentes



Lista de Accidentes: Página que muestra un listado de los accidentes reportados, incluyendo información sobre el empleado involucrado, la fecha de registro y la parte del cuerpo afectada.

Figura 32 Capacitaciones

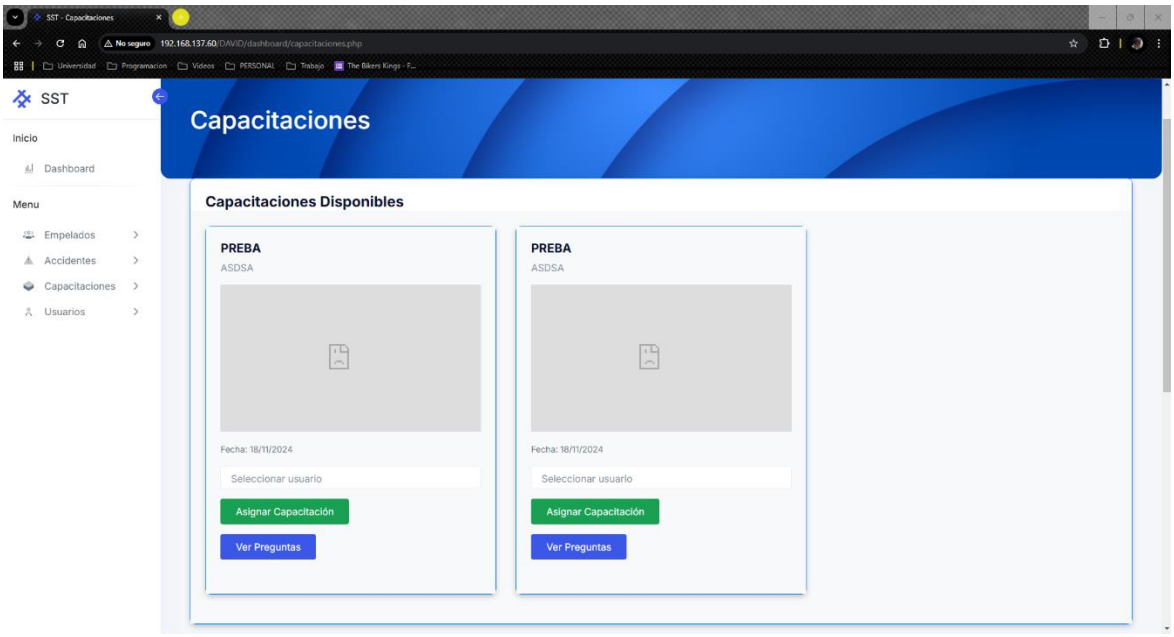
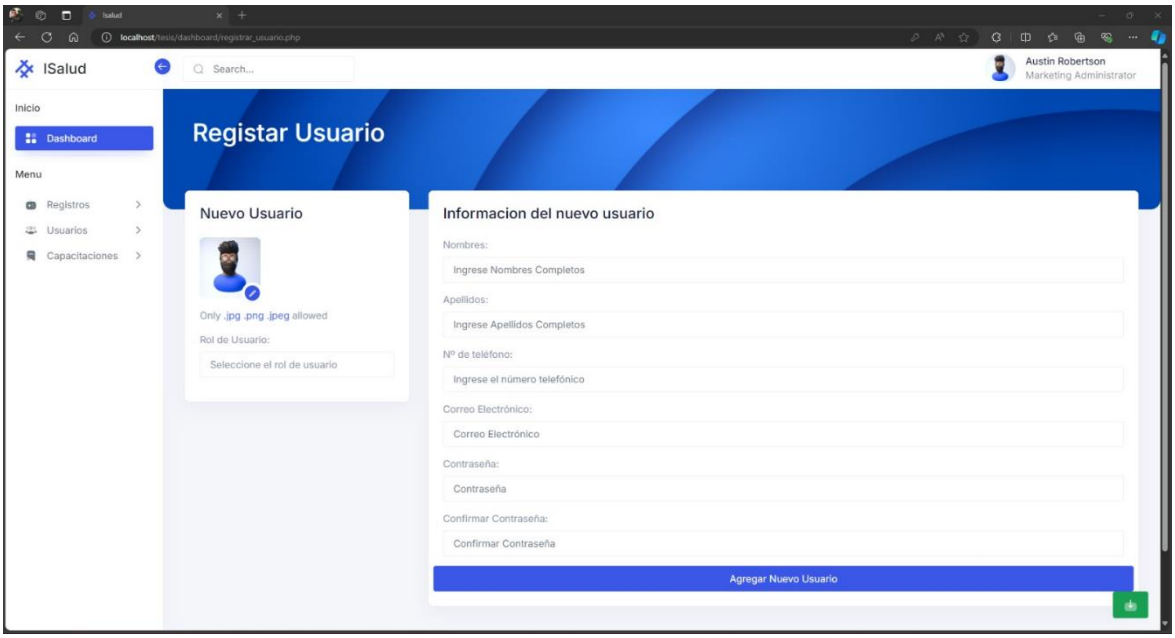


Figura 33 Registro de Usuarios



Registro de Usuarios: Página para registrar nuevos usuarios, donde se asignará un rol específico, y con este rol se establecerán los permisos de navegación dentro del sistema.

Conclusiones

El programa de salud y seguridad en el trabajo se ha consolidado como una herramienta clave para garantizar la protección de la salud y el bienestar de los empleados. Además de reducir los riesgos laborales, este tipo de iniciativas contribuyen a crear un entorno más seguro y saludable, lo que no solo beneficia a los trabajadores, sino que también impulsa la productividad en la empresa. Al establecer medidas preventivas y fomentar una cultura de seguridad, las organizaciones logran disminuir incidentes, optimizar el desempeño y fortalecer el compromiso de su equipo, generando un impacto positivo tanto en el ámbito laboral como en los resultados generales.

La prevención es un elemento clave para reducir accidentes y enfermedades laborales, siendo esencial para el bienestar de los empleados y el buen desempeño de las empresas. Acciones como capacitaciones constantes, inspecciones periódicas de seguridad y la implementación de protocolos de emergencia resultan fundamentales para minimizar riesgos y fomentar una cultura de responsabilidad dentro de las organizaciones.

En el caso de empresas con alta demanda de personal, estas medidas adquieren una importancia aún mayor, ya que contribuyen a mantener la productividad sin comprometer la seguridad de los trabajadores. Además, es imprescindible abordar la salud integral de los empleados, incorporando iniciativas que no solo se enfoquen en la seguridad física, sino también en el bienestar emocional y mental. Entre estas acciones se pueden incluir programas para gestionar el estrés, actividades que promuevan la salud emocional y revisiones médicas regulares.

Al priorizar la prevención y el cuidado integral, las empresas no solo cumplen con sus obligaciones legales, sino que también crean un entorno laboral más saludable y positivo. Esto, a su vez, fortalece la motivación, la lealtad y el compromiso de los trabajadores, factores determinantes para garantizar el éxito sostenible en cualquier sector.

Bibliografía

Aguirre Caracheo, E. (2014). *Metodología del desarrollo para sistemas de información basados en web*. https://ri-ng.uaq.mx/handle/123456789/4805

Castillo , Y. A. (2015). *Plan de Seguridad y Salud Ocupacional*. https://www.monografias.com/trabajos104/plan-seguridad-y-salud-ocupacional/plan-seguridad-y-salud-ocupacional

CORZO ROMÁN, J. M., OTERO DAJUD, E. R., GAVIRIA MUÑOZ, S., RODRÍGUEZ CAMARGO., J. A., SANTOS CALDERÓN, J. M., ARCE ZAPATA., G., MUÑOZ MUÑOZ, N. J., & PARDO RUEDA, R. (30 de Septiembre de 2024). *LEY 1562 DE 2012*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1562_2012.html#:~:text=ART%C3%8DCULO%203o.,una%20invalidez%20o%20la%20muerte.

Gov.Co. (2024). *ACCIDENTE DE TRABAJO*. https://www.sdp.gov.co/transparencia/informacion-interes/glosario/accidente-de-trabajo

Jiménez, M. M. (2022). *Vulnerabilidades que afectan la seguridad de la información*. Opirani: https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

Kosasi, S. (2016). *Researchgate*. https://www.researchgate.net/figure/fig2_322156784

SC Training . (2024). *Explore everything you can do with SC Training (formerly EdApp)*. https://training.safetyculture.com/features/

Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá. (26 de 10 de 2024). *Decreto 1377 de 2013 Nivel Nacional*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

Sommerville, I. (2011). *Ingenieria de Software*.

U de Cataluña. (2024). *Seguridad informática: La importancia y lo que debe saber.* Seguridad informática: La importancia y lo que debe saber: https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber

360learning. (2024). *The first comprehensive learning platform*. https://360learning.com/

Aguirre Caracheo, E. (2014). *Metodología del desarrollo para sistemas de información basados en web*. https://ri-ng.uaq.mx/handle/123456789/4805

Alonso, C. (2015). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Ávila Velandia, G. (2021). *Diseño del SG-SST para la empresa Tecnipanasonic Ltda., como estrategia para prevención de enfermedades y accidentes laborales, y la promoción de la salud*. https://hdl.handle.net/10656/13975

Castilla Salazar, A., & Paredes Daza, A. S. (2021). *Planificación de un sistema de gestión de seguridad y salud en el trabajo de acuerdo con el Decreto 1072 de 2015 en la Empresa Calzado Anyelme SAS ubicada en la Ciudad de Cúcuta, Norte de Santander*. https://hdl.handle.net/10656/13581

Club REM . (2024). *Programa de Gestion de Prevencion de Riesgos Laborales PrevGes 2.0. GRATIS*. https://www.clubrem.es/prevges.htm

Cority . (2023). *award-winning EHS software and OHS software*. https://www.cority.com/

DQS Colombia. (2024). *¿Qué es un sistema de gestión?* https://www.dqsglobal.com/es-co/aprenda/centro-de-conocimientos-dqs/que-es-un-sistema-de-gestion

EcoOnline. (2024). *Your complete safety and sustainability solution*. https://www.ecoonline.com/

Evaluando ERP. (2024). *Sistema de gestión ¿Qué es? ¿Cuántos tipos hay?* https://www.evaluandoerp.com/sistema-de-gestion/sistema-erp/que-es-un-sistema-de-gestion/#:~:text=Un%20sistema%20de%20gesti%C3%B3n%20es,laboral%20m%C3%A1s%20eficiente%20y%20sostenible.

Gov.co. (2021). *Sistema de Gestión de Seguridad y Salud en el Trabajo*. https://www.minambiente.gov.co/planeacion-y-seguimiento/sistema-de-gestion-de-seguridad-y-salud-en-el-trabajo/

Gov.co. (2024). *Enfermedad laboral*. https://www.minsalud.gov.co/proteccionsocial/RiesgosLaborales/paginas/enfermedad-laboral.aspx

Gov.co. (2024). *Decreto 472 de 2015 Nivel Nacional*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=61117

Gov.co. (2024). *Riesgos laborales / salud y ámbito laboral*. https://www.minsalud.gov.co/proteccionsocial/RiesgosLaborales/paginas/afiliacion-sistema-general-riesgos-laborales.aspx

Gov.co. (2024). *Sistema Integral de Información SISPRO*. https://www.minsalud.gov.co/proteccionsocial/Paginas/SistemaIntegraldeInformaci%C3%B3nSISPRO.aspx

Gov.co. (s.f.). *Resolución Conjunta 1016 de 1989 Ministerio del Trabajo*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5412

HSE Software. (2024). *Normatividad en Seguridad y Salud en el Trabajo Colombia*. https://hse.software/seguridad-y-salud-en-el-trabajo/normatividad-en-seguridad-y-salud-en-el-trabajo-colombia/

Intelex. (2024). *global EHS & Quality management software solutions*. https://www.intelex.com/

Isotools.us. (2024). *Normativa en Seguridad y Salud en el trabajo en Colombia*. https://co.isotools.us/normativa-en-seguridad-y-salud-en-el-trabajo-en-colombia/

Kaspersky Lab. (2020). *¿Qué es la ciberseguridad?* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOorG935qZEl-jFCOOtUp9mPE-aih6UiRfFAKG9jDo7DARcEfK22L

Ministerio del Trabajo, R. (2024). *Decreto 1072 de 2015*. Por el cual se adiciona la Sección 2 del Capítulo 5, del Libro 2, Parte 2, al Decreto 1072 de 2015, Único reglamentario del Sector Trabajo, por medio de la cual se adopta la Política Pública de Fomento e Implementación del Teletrabajo de que trata la Ley: https://www.mintrabajo.gov.co/web/guest/normatividad/participe-en-la-construccion-de-normatividad?inheritRedirect=true

Moodle LMS . (2024). *Desbloquee el poder de la IA para sus cursos*. https://moodle.org/?lang=es

Nexussafety.net. (2021). *Nexus safety*. https://nexussafety.net/

OpenWebinars S.L. (2022). *Arquitectura de software: Qué es y qué tipos existen*. https://openwebinars.net/blog/arquitectura-de-software-que-es-y-que-tipos-existen/

Pressman, R. (2010). *Ingenieria del Software. Un Enfoque Practico .* McGraw-Hill.

Pymes On Line . (2020). *SG SST - Pymes On Line Su Aliado Estratégico en Tecnología*. https://pymesonline.co/sg-sst/

Qualys. (2024). *Enterprise cyber risk & security platform.* https://www.qualys.com/

Revollo Trujillo , C. (2024). *Análisis de riesgos ocupacionales en el desplazamiento del personal de salud*. https://dspace.ucacue.edu.ec/handle/ucacue/17723

Sap.com. (2024). *SAP Environment, Health, and Safety Management*. https://www.sap.com/latinamerica/products/scm/ehs-management-health-safety.html

Secretaría Jurídica Distrital. (26 de 10 de 2024). *Ley 1581 de 2012 Congreso de la República de Colombia*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Secretaría Jurídica Distrital. (26 de 10 de 2024). *Ley 1581 de 2012 Congreso de la República de Colombia*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá. (26 de 10 de 2024). *Decreto 886 de 2014 Nivel Nacional*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338

Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá. (26 de 10 de 2024). *Ley 1928 de 2018 Congreso de la República de Colombia*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=147939&dt=S

Setraria juridica distrital . (22 de 10 de 2024). *Resolución 1111 de 2017 Ministerio del Trabajo*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=72623

Silva Vasconsellos, S. (2023). *Gestión de la Seguridad y Salud Laboral en las pequeñas y medianas empresas (PYMES) del sector de la construcción en Paraguay*. http://hdl.handle.net/2117/384588

Sistema de Gestión de Seguridad y Salud en el Trabajo-Ministerio de Trabajo . (2024). GOV.CO: https://www.mintrabajo.gov.co/relaciones-laborales/riesgos-laborales/sistema-de-gestion-de-seguridad-y-salud-en-el-trabajo

TalentLMS. (2024). *Cloud LMS software*. https://es.talentlms.com/

UNIVERSITAT CARLEMANY . (2023). *Qué es la seguridad informática: principios, tipos, ejemplos y más*. https://acortar.link/sIKa3B

W&B Asset Studio. (2022). *Diseño de software: fases y modelos*. https://www.wbassetstudio.com/blog/diseno-de-software-fases-y-modelos/