



UTL

Universidad
Tecnológica
de León
Ser, saber, hacer

PROYECTO PARA EMPRESA

“GORILLA CAPS”

UNIVERSIDAD TECNOLÓGICA DE LEÓN

GRUPO:

IDGS-1002

AUTORES:

ALBA ARGUELLO SERGIO ARTURO
BARRON RICO ADRIANA
ORTEGA LIZAMA JUAN DANIEL DE JESÚS
QUIROZ RAMIREZ YAHIR BERNARDO

INDICE

| | |
|--|----|
| 1. DESARROLLO DE LA ARQUITECTURA DE LA INFORMACIÓN | 3 |
| 1.1. DEFINICIÓN DE OBJETIVOS DEL PROYECTO..... | 3 |
| 1.1.1 Objetivo general..... | 3 |
| 1.1.2 Objetivos metodológicos..... | 3 |
| 1.1.3 Alcance..... | 3 |
| 1.2 DEFINICIÓN DE AUDIENCIA | 4 |
| 1.3 DEFINICIÓN DE CONTENIDOS DEL PROYECTO | 4 |
| 1.4. DEFINICIÓN DE LA ESTRUCTURA DEL PROYECTO | 5 |
| 1.5. DEFINICIÓN DE LOS SISTEMAS DE NAVEGACIÓN..... | 7 |
| 1.6. DEFINICIÓN DEL DISEÑO VISUAL DEL PROYECTO | 8 |
| 2.REQUERIMIENTOS DEL PROYECTO | 9 |
| REQUERIMIENTOS FUNCIONALES | 9 |
| REQUERIMIENTOS NO FUNCIONALES..... | 10 |
| REQUERIMIENTOS DE SEGURIDAD | 11 |
| 3.EVALUACIÓN DE RIESGOS | 12 |
| FASE 1: DEFINE OBJETIVOS..... | 12 |
| FASE 2: DEFINE EL ENFOQUE TÉCNICO | 13 |
| FASE 3 DESCOMPOSICIÓN DE LA APLICACIÓN | 15 |
| FASE 4: ANÁLISIS DE AMENAZAS..... | 15 |
| 4. DESARROLLO DE DIAGRAMAS UML | 20 |
| 4.1 DIAGRAMA DE CLASES. | 20 |
| 4.2. DIAGRAMAS DE CASOS DE USO. | 21 |
| 4.3. DIAGRAMAS DE CASOS DE ABUSO..... | 29 |
| 4.4. DIAGRAMA DE SECUENCIA. | 38 |
| 5. DIAGRAMA DE BASE DE DATOS..... | 39 |
| 5.1. DIAGRAMA ER | 39 |
| 5.2. DIAGRAMA RELACIONAL | 40 |

1. DESARROLLO DE LA ARQUITECTURA DE LA INFORMACIÓN.

1.1. DEFINICIÓN DE OBJETIVOS DEL PROYECTO.

1.1.1 Objetivo general

Implementar un sistema de gestión integral para la empresa Gorilla Caps, que incluya un apartado de ventas de productos, con el fin de que se aumente la eficiencia operativa, se optimicen los procesos de negocio, con ello aumente la satisfacción del cliente y se potencialicen las ventas.

1.1.2 Objetivos metodológicos

1.1.2.1 Seleccionar un sistema de gestión de procesos integrado que se ajuste a las necesidades y requerimientos de la empresa y que sea fácil de usar por el personal.

1.1.2.2 Implementar un sistema automatizado de gestión de pedidos que permita el seguimiento en tiempo real, reduzca los tiempos de envío, disminuya los errores en la entrega de productos y aumente la satisfacción del cliente.

1.1.2.3 Integrar un sistema de gestión financiera que permita el seguimiento de cuentas por cobrar y pagar, mejore la liquidez y facilite la planificación y control de los gastos.

1.1.2.4 Implementar un sistema de seguimiento preciso del inventario que permita identificar la cantidad y ubicación exacta de cada producto, con el fin de mejorar el control sobre las existencias y evitar errores en la toma de decisiones sobre los niveles de inventario.

1.1.3 Alcance

El alcance de este proyecto está delimitado principalmente en desarrollar una aplicación web con tres tipos de usuarios: cliente, empleado y administrador. La implementación de un módulo de autenticación de usuarios, creación de un catálogo de productos (gorras) y carrito de compras para los clientes. Además, la gestión de pedidos y ventas para los empleados. Integración de un sistema de gestión financiera y seguimiento del inventario para el administrador y la interconexión de los módulos para un flujo de información continuo. Finalmente, los requerimientos, base de datos y sistema funcional se entregarán en un periodo de 4 semanas.

1.2 DEFINICIÓN DE AUDIENCIA

Gorilla Caps se dedica a la elaboración y ventas de gorras de visera curva (Trucker Hat). Por lo que para la empresa tiene un publico en general, hombres y mujeres de 7 años en adelante.

1.3 DEFINICIÓN DE CONTENIDOS DEL PROYECTO

Al manejarse el sistema mediante una aplicación web, se van a tener tres tipos de usuario que serían el cliente, empleado y administrador. El usuario de cliente será el único que tenga acceso desde la aplicación móvil. Cada usuario contará con diferentes contenidos a los que podrá acceder:

Cliente:

- Vista sección informativa (visión, misión, ubicación, etc.)
- Página de contactos
- Inicio de sesión
- Catálogo de productos (gorras)
- Carrito de compras
- Catálogo de trazabilidad de la entrega o estatus de pedido de los productos

Empleado:

- Vista sección informativa (visión, misión, ubicación, etc.)
- Inicio de Sesión
- Pedidos
- Compras

Administrador:

- Vista sección informativa (visión, misión, ubicación, etc.)
- Inicio de Sesión
- Finanzas
- Dashboard
- Usuarios
- Proveedores
- Ventas
- Productos
- Compras (al proveedor)
- Inventario (materia prima)

1.4. DEFINICIÓN DE LA ESTRUCTURA DEL PROYECTO

➤ AUTENTICACIÓN DE USUARIOS O LOGIN:

La aplicación debe contar con una pantalla de inicio de sesión donde se debe permitir el ingreso al sistema a través de un inicio de sesión con usuario y contraseña, con la finalidad de restringir el acceso a las diferentes funciones y secciones de la aplicación según el rol o perfil de cada uno de los usuarios. La información almacenada en este módulo incluiría los datos de registro de cada usuario como su nombre y contraseña cifrada para garantizar la seguridad.

Por otra parte, la aplicación contará con tres perfiles de usuarios, los cuales tendrán los siguientes roles y privilegios:

- Administrador:

- Tendrá acceso a todos los módulos que componen el sistema, siendo estos: inicio de sesión, módulo de finanzas, módulo de dashboard, módulo de usuarios, módulo de proveedores, módulo de ventas, módulo de productos, módulo de compras (al proveedor), módulo de inventario (materia prima).

- Empleado:

- Tendrá acceso a inicio de sesión, al módulo de ventas y de pedidos.

- Cliente:

- Llevará a cabo el proceso de compra del producto, podrá ver la página informativa de la empresa, el inicio de sesión, el catálogo de productos y el carrito de compras.

➤ INVENTARIO (MATERIA PRIMA)

El módulo de inventario de materia prima se centrará en la administración de los recursos necesarios para la fabricación de las gorras, tales como la tela, hilo de costura, etc. Este módulo permitirá al administrador y empleado verificar y mantener el inventario actualizado para garantizar que se disponga de los recursos necesarios en todo momento.

➤ CATÁLOGO DE PRODUCTOS (GORRAS)

El módulo de catálogo de productos mostrará una galería de las gorras que están disponibles para la venta y que los clientes podrán adquirir. Este módulo permitirá a

los usuarios ver detalles de los productos, como la descripción, el precio y las imágenes.

➤ MÓDULO DE COMPRAS

El módulo de compras permitirá al administrador y empleado manejar las compras de materias primas a los proveedores y llevar un control de lo que se compra, cuánto se compra y el costo de dichos materiales.

➤ MÓDULO DE USUARIOS

El módulo de usuarios permitirá al administrador gestionar los permisos de los usuarios, incluyendo la creación y eliminación de cuentas de usuario y la asignación de permisos.

➤ MÓDULO DE PROVEEDORES

El módulo de proveedores permitirá al administrador registrar a los proveedores y llevar el control de estos, incluyendo sus datos de contacto y el tipo de material que se les está surtiendo.

➤ MÓDULO DE VENTAS

El módulo de ventas se utilizará para gestionar el proceso de venta de los productos. Este módulo permitirá al administrador y empleado gestionar las ventas y verificar las transacciones exitosas.

➤ MÓDULO DE PEDIDOS

El módulo de pedidos permitirá al cliente visualizar sus pedidos recientes, cancelar el producto que no le termine de gustar y realizar la compra definitiva de sus productos.

➤ MÓDULO DE FINANZAS

El módulo de finanzas se utilizará para gestionar las finanzas de la empresa, incluyendo la contabilidad, el total de ventas al mes. Solo el administrador tendrá acceso a ver esta información.

➤ MÓDULO DE DASHBOARD

El módulo de dashboard permitirá al administrador ver información relevante de manera gráfica para que sea más fácil su comprensión.

Cada módulo del proyecto será independiente, pero estará interconectado con los demás, lo que permitirá un flujo continuo de información y comunicación. Esta estructura modular facilitará la gestión del proyecto y permitirá una mayor flexibilidad en caso de cambios o actualizaciones futura.

1.5. DEFINICIÓN DE LOS SISTEMAS DE NAVEGACIÓN.

Barra de menú: en la parte superior de la interfaz de usuario, se puede incluir una barra de menú con opciones que los usuarios pueden seleccionar para acceder a diferentes secciones del software.


Navegación por pestañas: en algunas secciones del software, se usarán pestañas para permitir que los usuarios cambien entre diferentes páginas.

Íconos de navegación: en algunas pestañas, se pueden utilizar íconos de navegación para permitir a los usuarios cambiar entre diferentes secciones del software.


1.6. DEFINICIÓN DEL DISEÑO VISUAL DEL PROYECTO

GUÍA DE ESTILO "GORILLAS CAPS"

SÍMBOLOS




El usuario realizo correctamente la acción.




El usuario NO realizo correctamente o hubo un problema al realizar la acción.


PALETA DE COLORES




#FFFFFF




#000000




#1C3E66




#0066B2



#007A33




#FAC01A




#CF4527


BOTONES




#CF4527



#FAC01A



#0066B2



#1C3E66

FORMULARIO

INGRESAR:

Nombre:

BÚSQUEDA

Buscar:

TIPOGRAFÍA

HEADLINE 1

Roboto

This is a paragraph, shown in the Roboto

HEADLINE 2

Tino

This is a paragraph, shown in the Roboto

BOTONES

Arimo

This is a paragraph, shown in the Roboto

TABLA DE REGISTROS

| | | |
|--|--|---------|
| | | #002454 |
| | | #ACC3D3 |
| | | #FFFFFF |
| | | #ACC3D3 |

2.REQUERIMIENTOS DEL PROYECTO

REQUERIMIENTOS FUNCIONALES

| ID Requerimiento | Nombre del Requerimiento | Descripción |
|------------------|--|--|
| RF01 | Autenticación de Usuario | El sistema debe contar con un módulo de autenticación que permita a los usuarios ingresar al sistema y verificar sus credenciales antes de acceder a cualquier otra función del proyecto. El módulo debe tener tres perfiles disponibles: Administrador, Empleado y Cliente, cada uno con diferentes niveles de acceso a los diferentes módulos del proyecto. |
| RF02 | Gestión de Inventario de Materia Prima | |
| | Alta de materia prima | El sistema debe contar con un módulo de inventario de materia prima que permita al administrador dar de alta la materia prima, como nombre, cantidad, precio. |
| | Modificación de materia prima | El sistema deberá permitir modificar la información de la materia prima. |
| | Eliminación de materia prima. | La aplicación deberá dar de baja a la materia prima. |
| RF03 | Gestión de productos | |
| | Alta de productos | La aplicación permitirá el registro de los productos como el nombre, precio. |
| | Modificación de productos | La aplicación debe permitir modificar la información de los proveedores. |
| | Eliminación de productos | La aplicación podrá dar de baja a un proveedor. |
| RF04 | Gestión de ventas | El sistema debe contar con un módulo de ventas que se utilizará para gestionar el proceso de venta de los productos. Este módulo permitirá al administrador y empleado gestionar las ventas y verificar las transacciones exitosas. |
| RF05 | Gestión de usuarios | |
| | Alta de usuarios | La aplicación permitirá el registro de los usuarios para cada uno de los empleados que no tenga una credencial de acceso al sistema, esto incluiría el almacenamiento del nombre de usuario, contraseña y el estatus. |

| | | |
|-------------|-----------------------------|---|
| | Modificación de usuarios | La aplicación debe permitir modificar la información de los usuarios. |
| | Eliminación de usuarios | La aplicación podrá dar de baja los usuarios. |
| RF06 | Gestión de proveedores | |
| | Alta de proveedores | La aplicación permitirá el registro de los proveedores, donde se registrará información como nombre, dirección, teléfono, producto que surte. |
| | Modificación de proveedores | La aplicación debe permitir modificar la información de los proveedores. |
| | Eliminación de proveedores | La aplicación podrá dar de baja a un proveedor. |
| RF07 | Gestión de compras | El sistema debe contar con un módulo de compras que permita al administrador y empleado manejar las compras de materias primas a los proveedores y llevar un control de lo que se compra, cuánto se compra y el costo de dichos materiales. |
| RF08 | Gestión de pedidos | El sistema debe contar con un módulo de pedidos que permita al cliente visualizar sus pedidos recientes, cancelar el producto que no le termine de gustar y realizar la compra definitiva de sus productos. |

REQUERIMIENTOS NO FUNCIONALES

| ID Requerimiento | Nombre del Requerimiento | Descripción |
|------------------|--------------------------|---|
| RNF01 | Diseño de la interfaz | El diseño de formularios debe ser adecuado, utilizando iconografía y componentes de manera efectiva. |
| RNF02 | Usabilidad | La presentación de la aplicación debe ser atractiva y fácil de usar para cualquier usuario. |
| RNF03 | Manejo de errores | La aplicación debe ser capaz de controlar y manejar errores efectivamente para minimizar la interrupción del servicio y evitar la pérdida de datos. |
| RNF04 | Experiencia de usuario | La aplicación deberá ofrecer una experiencia de usuario agradable a través de acciones como, evitar que el usuario escriba datos de integridad referencial (campos ID), mostrar la menor cantidad de avisos posibles y Hacer un diseño que sea fácil e intuitivo de usar para el usuario. |
| RNF05 | Compatibilidad | La aplicación deberá de ser compatible en la mayoría de los navegadores. |
| RNF06 | Paleta de colores | La aplicación deberá estar sujeta a los colores que van de acuerdo con el entorno de la pizzería, como de su logo. |
| RNF07 | Accesibilidad | Se deberá tener acceso a la aplicación a través de cualquier dispositivo por medio de un navegador web. |

REQUERIMIENTOS DE SEGURIDAD

| ID Requerimiento | Nombre del Requerimiento | Descripción |
|------------------|--------------------------------|--|
| RS01 | Autenticación y Autorización | <ul style="list-style-type: none">• La aplicación deberá contar con un sistema de autenticación seguro que requiera un usuario y contraseña para acceder al sistema.• Deberá implementarse un control de acceso basado en roles y permisos para garantizar que solo los usuarios autorizados puedan acceder a la información y funcionalidades correspondientes a su perfil.• Deberá haber al menos un usuario administrador con privilegios especiales. |
| RS02 | Protección de datos personales | <ul style="list-style-type: none">• Deberá implementarse medidas de seguridad para proteger los datos personales de alumnos y colaboradores, como la encriptación de datos, restricciones de acceso, y respaldo de información.• La aplicación deberá cumplir con las leyes y regulaciones de protección de datos personales aplicables. |
| RS03 | Seguridad de la aplicación | <ul style="list-style-type: none">• La aplicación deberá estar protegida contra ataques informáticos, como inyección de código, ataques de denegación de servicio.• Deberá haber medidas de seguridad para prevenir y detectar intentos de intrusión, como la implementación de firewalls, monitoreo de logs, y sistemas de detección de intrusiones.• La aplicación deberá ser actualizada regularmente con parches y actualizaciones de seguridad. |
| RS04 | Trazabilidad y auditoría | <ul style="list-style-type: none">• La aplicación deberá tener un sistema de registro de eventos y operaciones para garantizar la trazabilidad y auditoría de las acciones realizadas por los usuarios.• Se deberá garantizar la integridad y confidencialidad de los registros de auditoría. |

3.EVALUACIÓN DE RIESGOS

FASE 1: DEFINE OBJETIVOS

| Requisitos comerciales |
|---|
| El costo total de la aplicación no debe exceder el presupuesto asignado por el cliente. |
| La aplicación debe ser desarrollada en un lenguaje de programación web. |
| La aplicación debe ser compatible con los navegadores web más utilizados. |
| La aplicación debe ser escalable para futuras actualizaciones y cambios en los requisitos. |
| La aplicación debe ser desarrollada siguiendo buenas prácticas de seguridad para garantizar la protección de los datos personales de los alumnos y colaboradores. |
| La aplicación debe cumplir con los estándares de accesibilidad web para que pueda ser utilizada por personas con discapacidades. |
| La aplicación debe ser fácil de usar y contar con una interfaz intuitiva para los usuarios finales. |

| Requisitos de la Protección de Datos |
|--|
| Cumplimiento de la normativa vigente en materia de protección de datos personales. |
| El sistema debe contar con medidas de seguridad adecuadas para proteger los datos personales de los diferentes tipos de usuario (cliente, empleado y administrador), incluyendo la confidencialidad, integridad y disponibilidad de estos. |
| Se debe obtener el consentimiento informado de los empleados y clientes para la recopilación y uso de sus datos personales. |
| Los datos personales solo se podrán utilizar para los fines específicos para los que se recopilaron y con el consentimiento de los titulares de los datos. |
| El acceso a los datos personales debe ser restringido únicamente a las personas autorizadas que requieren el acceso para cumplir con sus funciones |
| Los datos personales deben ser almacenados de forma segura y protegidos contra el acceso no autorizado, la pérdida o la destrucción. |
| Los datos personales solo se deben conservar durante el tiempo necesario para cumplir con los fines específicos para los que se recopilaron. |
| En caso de que se produzca una violación de seguridad que afecte los datos personales, se debe notificar a los titulares de los datos y a la autoridad competente. |

FASE 2: DEFINE EL ENFOQUE TÉCNICO

Detalles técnicos de la arquitectura de la información.

1.-Usuarios:

- Administrador: tiene acceso a todos los catálogos principales como inicio de sesión, finanzas, dashboard, usuarios, proveedores, ventas, productos, compras (al proveedor), inventario (materia prima).
- Empleado: tendrá acceso a inicio de sesión, al módulo de ventas y de pedidos.
- Cliente: llevará a cabo el proceso de compra del producto, podrá ver la página informativa de la empresa, el inicio de sesión, el catálogo de productos y el carrito de compras.

2.- Sección informativa:

- En esta parte se muestra la información general de la empresa, su filosofía y su ubicación.

3.-Acceso al sistema:

- La aplicación deberá contar con un control de acceso por login.
- Pantalla de inicio con el menú principal, de acuerdo con el perfil de la cuenta del usuario.

4.-Finanzas:

- Se utilizará para gestionar las finanzas de la empresa, incluyendo la contabilidad, el total de ventas al mes.
- Solo el administrador tendrá acceso a ver esta información.

5.-Dashboard:

- Permitirá al administrador ver información relevante de manera gráfica para que sea más fácil su comprensión.

6.-Usuarios:

- Permite al administrador gestionar la información sobre los demás usuarios, así como dar de baja y cambiar el tipo de usuario.

7.-Proveedores:

- Datos almacenados: nombre, dirección, teléfono, producto que surte.
- Solo el administrador puede manipular la información de los proveedores, sea dar de alta uno nuevo, modificarlo o eliminar.

8.-Ventas:

- Mostrará la información de las ventas, incluyendo la fecha y hora de la venta, el cliente que realizó la compra, la cantidad de gorras vendidas y el precio total.

9.-Productos:

- Datos almacenados: nombre, precio, materiales que va a utilizar.

10.-Compras:

- Es donde el administrador puede hacer las compras a los proveedores de los materiales.

11.-Inventario

- Permite al administrador ver que materias primas tiene en existencia, permitiéndole saber qué materia prima surtir.

Detalles de diseño

➤ Presentación de la aplicación:

- Diseño de interfaz de usuario limpio y claro.
- Uso de colores y tipografía adecuados para mejorar la legibilidad y accesibilidad.

➤ Diseño de formularios, uso de iconografía y manejo de componentes:

- Diseño de formularios que sean intuitivos y fáciles de usar.
- Uso de iconos y gráficos adecuados para ayudar al usuario a entender mejor la información.

Componentes tecnológicos

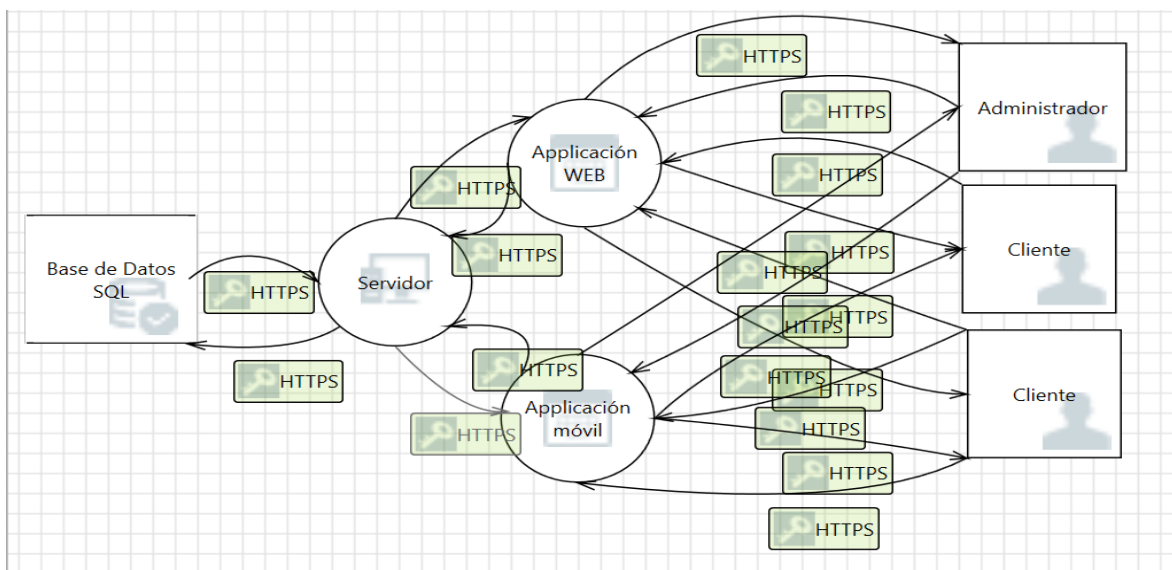
- HTML
- CSS
- React
- JavaScript
- SQL
- Bootstrap
- C#

Definición de diagramas

- Diagramas de casos de abuso
- Diagramas de casos de uso
- Diagramas de secuencia
- Diagramas de clases

FASE 3 DESCOMPOSICIÓN DE LA APLICACIÓN

Diagrama de flujos de datos



FASE 4: ANÁLISIS DE AMENAZAS

Elaborar el análisis de amenazas

Riesgo: Ataque de fuerza bruta a la autenticación de la aplicación

| | | | | | | | |
|--|--|--|----------------------------|---|-----------------------------------|---------------------|-----------------------------|
| Ataque de fuerza bruta a la autenticación de la aplicación web | | | | | | | |
| Riesgo: aplicación web | | | | | | | |
| Probabilidad | | | | | | | |
| Factores de agente de amenaza | | | | Factores de vulnerabilidad. | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión |
| 1 - No requiere habilidades técnicas | 4 - Posible recompensa | 7 - Se requiere cierto acceso o recursos | 6 - Usuarios autenticados | 1 - Prácticamente Imposible | 5 - Facil | 1 - Desconocido | 8 - Registrado sin revisión |
| Probabilidad general: | | | | 4.125 | MEDIO | | |
| Impacto técnico | | | | | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad |
| 9 - Todos los datos divulgados | 7 - Amplios datos seriamente corruptos | 0 - | 7 - Posiblemente rastreado | 1 - Menos del costo para arreglar la vulnerabilidad | 1 - Daño Mínimo | 5 - Clara violación | 3 - Un individuo |
| Impacto técnico general: | | 5.750 | MEDIO | Impacto comercial general: | | 2.500 | BAJO |
| Impacto general: | | | | 4.125 | MEDIO | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | | | |
| Impacto | ALTO | Medium | High | CRITICO | Niveles de probabilidad e impacto | | |
| | MEDIO | Low | Medium | ALTO | 0 to <3 | BAJO | |
| | BAJO | Note | Low | MEDIO | 3 to <6 | MEDIO | |
| | | BAJO | MEDIO | ALTO | 6 to 9 | ALTO | |
| Probabilidad | | | | | | | |

Riesgo: Ataque de Inyección SQL a la BD

| | | | | | | | |
|--|---|---|-----------------------------------|-----------------------------|-------------------------------|-----------------------------|---------------------------|
| Riesgo: Ataque de inyección SQL a la base de datos | | | | | | | |
| Probabilidad | | | | | | | |
| Factores de agente de amenaza | | | | Factores de vulnerabilidad. | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión |
| 3 - Algunas Habilidades técnicas | 4 - Posible recompensa | 4 - Acceso especial o recursos requeridos | 9 - Usuarios de internet anónimos | 7 - Facil | 5 - Facil | 9 - Conocimiento Publico | 3 - Registrado y revisado |
| Probabilidad general: | | | | 5.500 | MEDIO | | |
| Impacto | | | | | | | |
| Impacto técnico | | | | Impacto de negocio | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad |
| 5 - Extensos datos críticos revelados | 9 - Todos los datos totalmente corruptos. | 1 - Servicios secundarios mínimos interrumpidos | 7 - Posiblemente rastreable | 5 - | 9 - Daño de marca | 7 - Violación de alto nivel | 5 - cientos personas |
| Impacto técnico general: | | 5.500 | MEDIO | Impacto comercial general: | | 6.500 | ALTO |
| Impacto general: | | | | 6.000 | ALTO | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | | | |
| Impacto | ALTO | Medium | High | CRITICO | | | |
| | MEDIO | Low | Medium | ALTO | | | |
| | BAJO | Note | Low | MEDIO | | | |
| | | BAJO | MEDIO | ALTO | | | |
| Probabilidad | | | | | | | |
| Niveles de probabilidad e impacto | | | | | | | |
| 0 to <3 | | BAJO | | | | | |
| 3 to <6 | | MEDIO | | | | | |
| 6 to 9 | | ALTO | | | | | |

Riesgo: Ataque de denegación de servicio (DDoS) al servidor web

| | | | | | | | |
|---|---------------------------------------|--|--|---|-------------------------------|--------------------------|------------------------------------|
| Ataque de denegación de servicio (DDoS) al | | | | | | | |
| Riesgo: servidor web | | | | | | | |
| Probabilidad | | | | | | | |
| Factores de agente de amenaza | | | | Factores de vulnerabilidad. | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión |
| 9 - Habilidades en Ciberseguridad | 9 - Alta recompensa | 0 - Se requiere acceso completo o recursos caros | 2 - Desarrolladores, administradores de sistemas | 3 - Difícil | 5 - Fácil | 9 - Conocimiento Público | 1 - Detección activa en aplicación |
| Probabilidad general: | | | | 4.750 | MEDIO | | |
| Impacto técnico | | | | | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad |
| 4 - Datos críticos mínimos revelados, datos no sensibles extensos revelados | 3 - Mínimo datos seriamente corruptos | 9 - Todos los servicios completamente perdidos | 7 - Posiblemente rastreable | 7 - Efecto significativo en la ganancia anual | 9 - Daño de marca | 8 - | 5 - cientos personas |
| Impacto técnico general: | | 5.750 | MEDIO | Impacto comercial general: | | 7.250 | ALTO |
| Impacto general: | | | | 6.500 | ALTO | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | | | |
| Impacto | ALTO | Medium | High | CRITICO | | | |
| | MEDIO | Low | Medium | ALTO | | | |
| | BAJO | Note | Low | MEDIO | | | |
| | Probabilidad | | | | | | |

Riesgo: Ataque de Cross-site scripting (XSS)

| Riesgo: Ataque de Cross-site scripting (XSS) | | | | | | | |
|--|--|---|-----------------------------------|----------------------------------|-------------------------------|-----------------------------|---------------------------|
| Factores de agente de amenaza | | | | Factores de vulnerabilidad. | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión |
| 3 - Algunas Habilidades técnicas | 9 - Alta recompensa | 7 - Se requiere cierto acceso o recursos | 9 - Usuarios de internet anónimos | 6 - | 4 - | 4 - Oculto | 3 - Registrado y revisado |
| Probabilidad general: 5.625 | | | | MEDIO | | | |
| Impacto técnico | | | | Impacto de negocio | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad |
| 9 - Todos los datos divulgados | 7 - Amplios datos seriamente corruptos | 7 - Amplios servicios primarios interrumpidos | 5 - | 5 - | 9 - Daño de marca | 7 - Violación de alto nivel | 5 - cientos personas |
| Impacto técnico general: 7.000 | | ALTO | | Impacto comercial general: 6.500 | | ALTO | |
| Impacto general: 6.750 | | | | ALTO | | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | | | |
| Impacto | ALTO | Medium | High | CRITICO | | | |
| | MEDIO | Low | Medium | ALTO | | | |
| | BAJO | Note | Low | MEDIO | | | |
| | | BAJO | MEDIO | ALTO | | | |
| Probabilidad | | | | | | | |
| Niveles de probabilidad e impacto | | | | | | | |
| 0 to <3 | | BAJO | | | | | |
| 3 to <6 | | MEDIO | | | | | |
| 6 to 9 | | ALTO | | | | | |

Riesgo: Ataques de phishing a usuarios del sitio

| Riesgo: Ataques de phishing dirigidos a usuarios del sistema | | | | |
|--|---------------------------------------|---|----------------------------|---|
| | | | | Probabilidad |
| Factores de agente de amenaza | | | | Factores de vulnerabilidad |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | Facilidad para Descubrir |
| 5 - Uso Avanzado de computadoras | 4 - Posible recompensa | 9 - No se requiere acceso ni recursos | 7 - | Facilidad para la Explotación |
| | | | | Conciencia |
| | | | | Detección de Intrusión |
| | | | | 9 - Conocimiento Público |
| | | | | 3 - Registrado y revisado |
| Probabilidad general: 5.875 | | | | MEDIO |
| Impacto técnico | | | | Impacto de negocio |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | Daño Financiero |
| mínimos revelados, datos no sensibles extensos | 3 - Mínimo datos seriamente corruptos | 1 - Servicios secundarios mínimos interrumpidos | 1 - totalmente rastreable | Daño en Reputación |
| | | | | No cumplimiento |
| | | | | Violación de Privacidad |
| | | | | 1 - Menos del costo para arreglar la vulnerabilidad |
| | | | | 4 - Pérdida de cuentas importantes |
| | | | | 5 - Clara violación |
| | | | | 3 - Un individuo |
| Impacto técnico general: 2.250 | | | | Impacto comercial general: 3.250 |
| Impacto general: 2.750 | | | | BAJO |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | |
| Impacto | ALTO | Medium | High | CRITICO |
| | MEDIO | Low | Medium | ALTO |
| | BAJO | Note | Low | MEDIO |
| | | BAJO | MEDIO | ALTO |
| Probabilidad | | | | Niveles de probabilidad e impacto |
| | | | | 0 to <3 |
| | | | | 3 to <6 |
| | | | | 6 to 9 |

Riesgo: Fallas de identificación y autenticación

| Riesgo: Fallas de Identificación y Autenticación | | | | | | | | | |
|--|---|---|----------------------------|--------------|--|---|------------------------------------|---------------------|-----------------------------|
| Factores de agente de amenaza | | | | Probabilidad | | Factores de vulnerabilidad. | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | | | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión |
| 5 - Uso Avanzado de computadoras | 6 - Recompensa asegurada | 4 - Acceso especial o recursos requeridos | 4 - Usuarios de intranet | | | 2 - Complicado | 3 - Difícil | 4 - Oculto | 8 - Registrado sin revisión |
| Probabilidad general: | | | | 4.500 | | MEDIO | | | |
| Impacto técnico | | | | | | Impacto de negocio | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | | | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad |
| 5 - Extensos datos críticos revelados | 5 - Amplios datos ligeramente corruptos | 5 - Servicios primarios mínimos interrumpidos, servicios secundarios extensivos interrumpidos | 4 - Rastreado | | | 7 - Efecto significativo en la ganancia anual | 4 - Pérdida de cuentas importantes | 5 - Clara violación | 5 - cientos personas |
| Impacto técnico general: | | | | 4.750 | | MEDIO | | | |
| Impacto comercial general: | | | | 5.250 | | MEDIO | | | |
| Impacto general: | | | | 5.000 | | MEDIO | | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | | Niveles de probabilidad e impacto | | | |
| Impacto | ALTO | Medium | High | CRITICO | | 0 to <3 | BAJO | | |
| | MEDIO | Low | Medium | ALTO | | 3 to <6 | MEDIO | | |
| | BAJO | Note | Low | MEDIO | | 6 to 9 | ALTO | | |
| | | BAJO | MEDIO | ALTO | | | | | |
| Probabilidad | | | | | | | | | |

Riesgo: Componentes vulnerables y desactualizados

| Riesgo: Componentes vulnerables y desactualizados | | | | | | | | | |
|---|---|---|----------------------------|--------------|---|-------------------------------|---------------------|-------------------------|--|
| Factores de agente de amenaza | | | | Probabilidad | Factores de vulnerabilidad. | | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión | |
| 5 - Uso Avanzado de computadoras | 4 - Posible recompensa | 4 - Acceso especial o recursos requeridos | 4 - Usuarios de intranet | | 2 - Complicado | 3 - Difícil | 4 - Oculto | 9 - No Loegado | |
| Probabilidad general: | | | | 4.375 | MEDIO | | | | |
| Impacto técnico | | | | | Impacto de negocio | | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad | |
| 4 - Datos críticos mínimos revelados, datos no sensibles extensos revelados | 5 - Amplios datos ligeramente corruptos | 5 - Servicios primarios mínimos interrumpidos, servicios secundarios extensivos interrumpidos | 7 - Posiblemente rastreado | | 7 - Efecto significativo en la ganancia anual | 1 - Daño Mínimo | 5 - Clara violación | 5 - cientos personas | |
| Impacto técnico general: | | 5.250 | MEDIO | | Impacto comercial general: | | 4.500 | MEDIO | |
| Impacto general: | | | | 4.875 | MEDIO | | | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | Niveles de probabilidad e impacto | | | | |
| Impacto | ALTO | Medium | High | CRITICO | 0 to <3 BAJO | | | | |
| | MEDIO | Low | Medium | ALTO | 3 to <6 MEDIO | | | | |
| | BAJO | Note | Low | MEDIO | 6 to 9 ALTO | | | | |
| | | BAJO | MEDIO | ALTO | | | | | |
| Probabilidad | | | | | | | | | |

Riesgo: Falsificación del lado de servidor (SSRF)

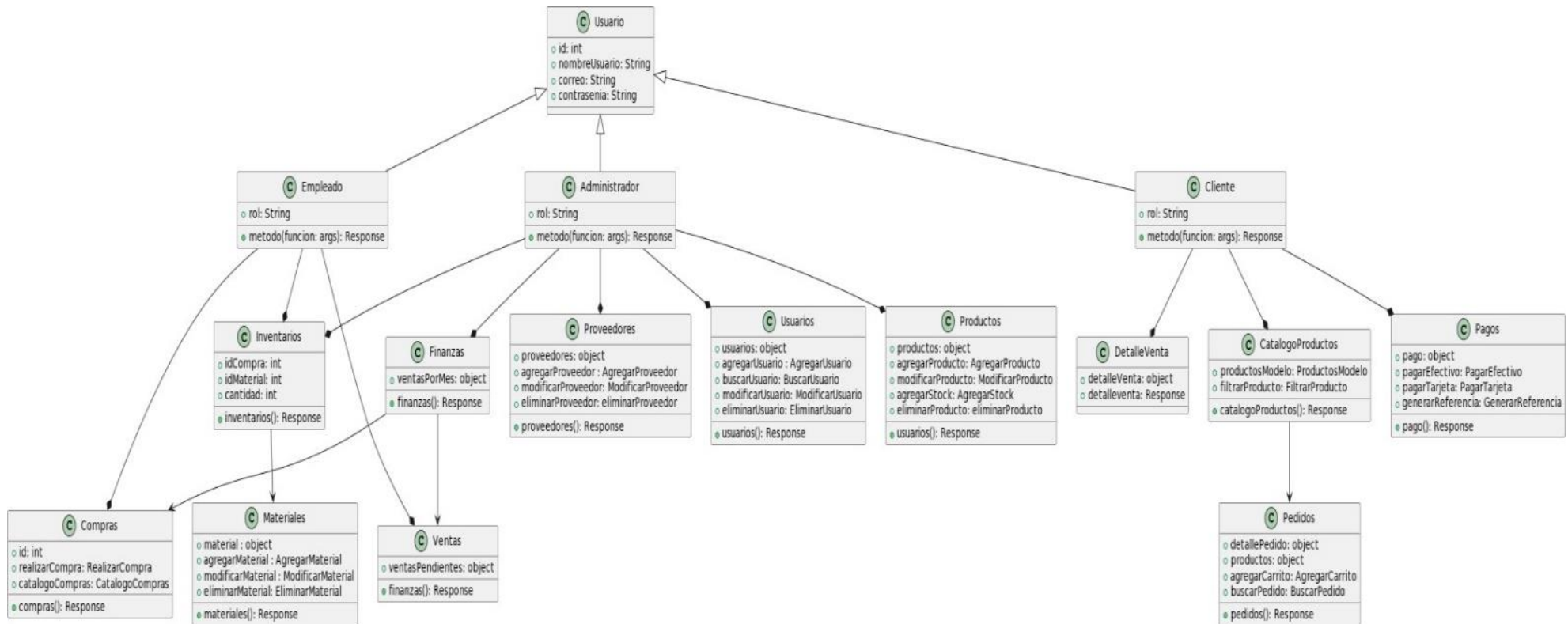
| | | | | | | | | | |
|---|---|---|----------------------------|---------|--|------------------------------------|---------------------|-----------------------------|--|
| Riesgo: Falsificación de Solicitudes del Lado del Servidor (SSRF) | | | | | | | | | |
| Probabilidad | | | | | | | | | |
| Factores de agente de amenaza | | | | | Factores de vulnerabilidad. | | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión | |
| 5 - Uso Avanzado de computadoras | 4 - Posible recompensa | 7 - Se requiere cierto acceso o recursos | 4 - Usuarios de intranet | | 3 - Difícil | 3 - Difícil | 4 - Oculto | 8 - Registrado sin revisión | |
| Probabilidad general: 4.750 | | | | | MEDIO | | | | |
| Impacto técnico | | | | | Impacto de negocio | | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad | |
| 5 - Extensos datos críticos revelados | 1 - Datos mínimos ligeramente corruptos | 5 - Servicios primarios mínimos interrumpidos, servicios secundarios extensivos interrumpidos | 7 - Posiblemente rastreado | | 3 - Efecto menor en la ganancia anual. | 4 - Pérdida de cuentas importantes | 5 - Clara violación | 5 - cientos personas | |
| Impacto técnico general: 4.500 | | | | | Impacto comercial general: 4.250 | | | | |
| Impacto general: 4.375 | | | | | MEDIO | | | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | Niveles de probabilidad e impacto | | | | |
| Impacto | ALTO | Medium | High | CRITICO | 0 to <3 | | | | |
| | MEDIO | Low | Medium | ALTO | 3 to <6 | | | | |
| | BAJO | Note | Low | MEDIO | 6 to 9 | | | | |
| | BAJO | | | | ALTO | | | | |
| Probabilidad | | | | | | | | | |

Riesgo: Fallas criptográficas

| | | | | | | | | | |
|--|---------------------------------------|--|--|--|------------------------------------|---------------------|-----------------------------|--|--|
| Riesgo: fallas criptograficas | | | | | | | | | |
| Probabilidad | | | | | | | | | |
| Factores de agente de amenaza | | | | Factores de vulnerabilidad. | | | | | |
| Nivel de habilidad | Motivo | Oportunidad | Tamaño | Facilidad para Descubrir | Facilidad para la Explotación | Conciencia | Detección de Intrusión | | |
| 3 - Algunas Habilidades técnicas | 4 - Posible recompensa | 0 - Se requiere acceso completo o recursos caros | 2 - Desarrolladores, administradores de sistemas | 7 - Facil | 5 - Facil | 6 - Ovio | 8 - Registrado sin revisión | | |
| Probabilidad general: 4.375 | | | | MEDIO | | | | | |
| Impacto técnico | | | | | | | | | |
| Pérdida de la Confidencialidad | Pérdida de Integridad | Pérdida en Disponibilidad | Pérdida en Responsabilidad | Daño Financiero | Daño en Reputación | No cumplimiento | Violación de Privacidad | | |
| 5 - Extensos datos críticos revelados | 3 - Mínimo datos seriamente corruptos | 1 - Servicios secundarios mínimos interrumpidos | 7 - Posiblemente rastreable | 3 - Efecto menor en la ganancia anual. | 4 - Pérdida de cuentas importantes | 5 - Clara violación | 5 - cientos personas | | |
| Impacto técnico general: 4.000 | | | | MEDIO | | | | | |
| Impacto general: 4.125 | | | | MEDIO | | | | | |
| Gravedad general del riesgo = Probabilidad x Impacto | | | | | | | | | |
| Impacto | ALTO | Medium | High | CRITICO | Niveles de probabilidad e impacto | | | | |
| | MEDIO | Low | Medium | ALTO | 0 to <3 BAJO | | | | |
| | BAJO | Note | Low | MEDIO | 3 to <6 MEDIO | | | | |
| | BAJO | | | | MEDIO | ALTO | 6 to 9 ALTO | | |
| Probabilidad | | | | | | | | | |

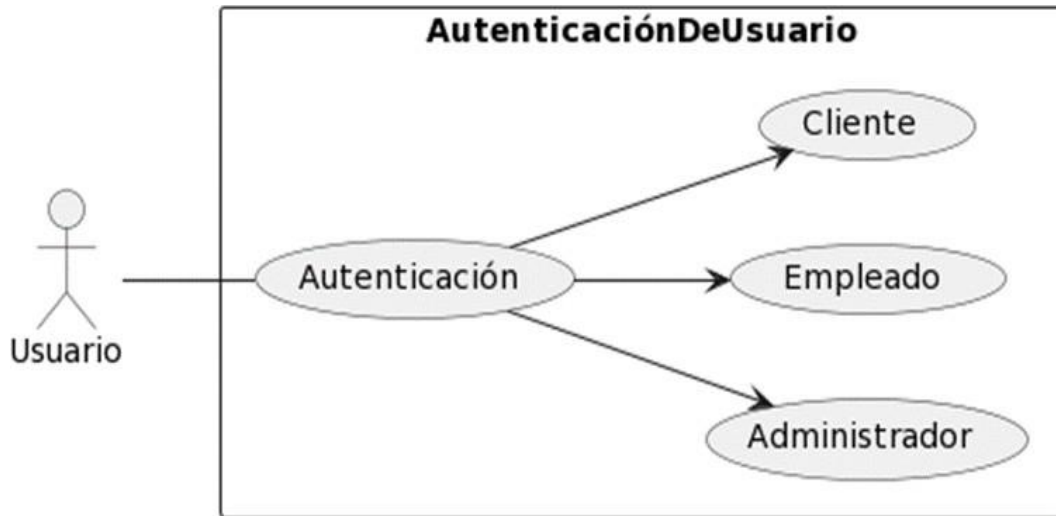
4. DESARROLLO DE DIAGRAMAS UML.

4.1 DIAGRAMA DE CLASES.



4.2. DIAGRAMAS DE CASOS DE USO.

- Módulo de autenticación de usuario



Historia de usuario del módulo:

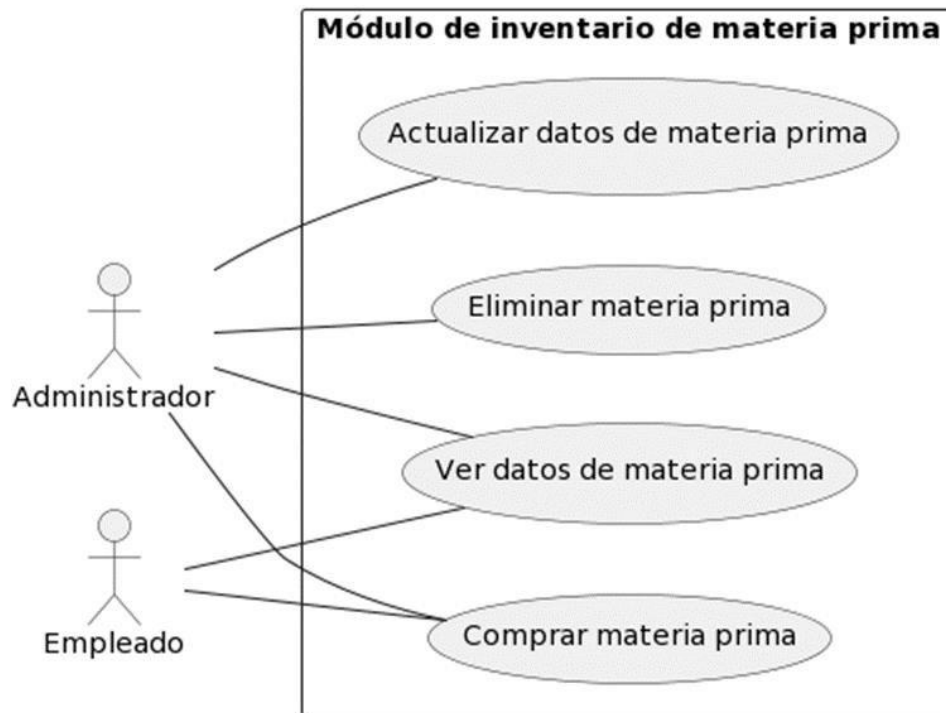
- **Título:** Implementar el módulo de autenticación de usuario

Descripción: Como usuario registrado en la plataforma, quiero poder autenticarme de manera segura y eficiente para acceder a las funciones personalizadas y proteger mi información.

Criterios de aceptación:

- En la pantalla de inicio, debe haber un formulario de inicio de sesión que permita al usuario ingresar su correo electrónico y contraseña.
- Dependiendo del tipo de usuario, se le mostrará la información a la que este autorizado para ver.
- Se debe proporcionar retroalimentación inmediata en caso de credenciales incorrectas durante el intento de inicio de sesión.
- Después de una autenticación exitosa, el usuario debe ser redirigido a su panel de control personalizado.
- La plataforma debe implementar medidas de seguridad, como el cifrado de contraseñas y la protección contra ataques de fuerza bruta.

- **Modulo inventario de materia prima**



Historia de usuario del módulo:

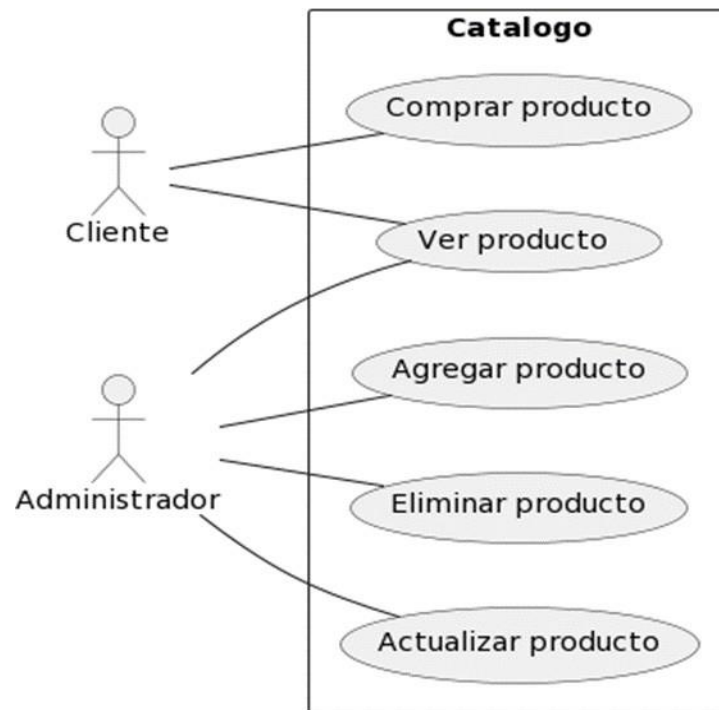
- **Título:** Desarrollar el módulo de inventario de materia prima

Descripción: El usuario que sea de tipo administrador podrá manipular todas las funciones que tenga el módulo mientras que, el usuario de tipo empleado podrá ver datos de materia prima y comprar la materia prima.

Criterios de aceptación:

- En la interfaz de materia prima, debe haber una opción clara para iniciar el proceso de compra de materia prima, los usuarios administradores y empleados deben poder seleccionar la cantidad y tipo de materia prima que desean comprar.
- Después de realizar una compra, la cantidad de materia prima en el inventario debe actualizarse correctamente, para que pueda ser visible para los usuarios administradores y empleados.
- Para la actualización y eliminación de la materia prima, solo podrá ser llevada a cabo por el usuario administrador.

- **Módulo de productos**



Historia de usuario del módulo:

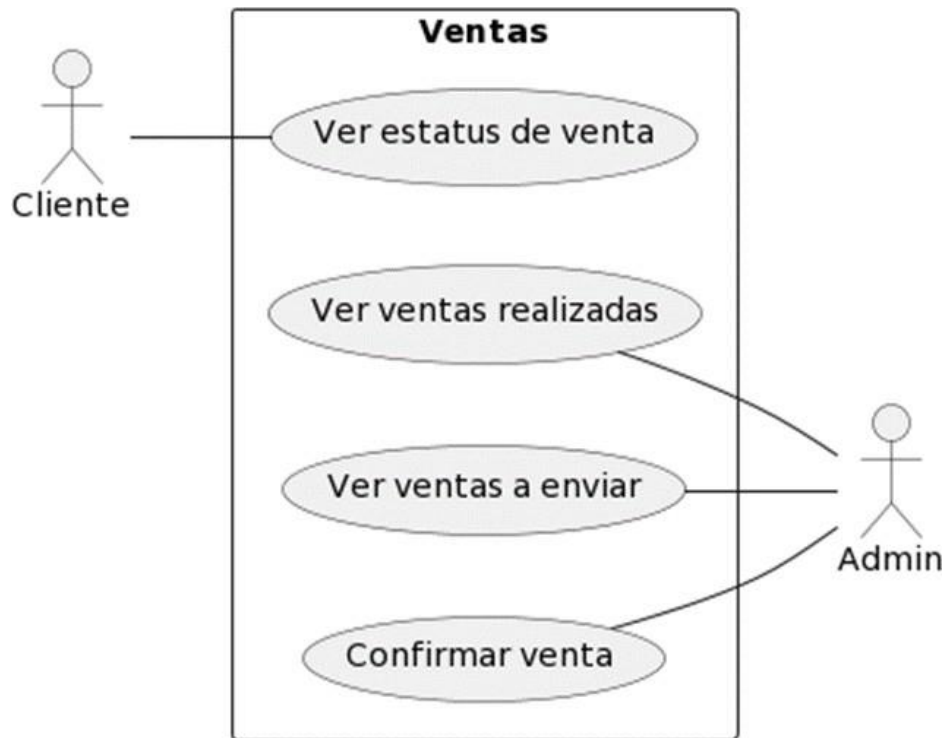
- **Título:** Desarrollar el módulo de productos.

Descripción: Se verán involucrados los usuarios de tipo administrador y cliente, el cliente por su parte podrá ver y comprar el producto, mientras que el administrador podrá agregar, eliminar, actualizar y ver el producto.

Criterios de aceptación:

- En la interfaz de administración, existe un formulario claro y accesible para registrar un nuevo producto.
- El formulario solicita la información esencial, incluyendo nombre, descripción, precio y cantidad inicial.
- En la interfaz de administración, hay una opción evidente para editar los datos de un producto existente.
- En la interfaz de administración, existe una opción clara para eliminar un producto del inventario.
- Existe una sección clara en la interfaz de usuario destinada a mostrar el catálogo de productos.

- **Módulo de ventas**



Historia de usuario del módulo:

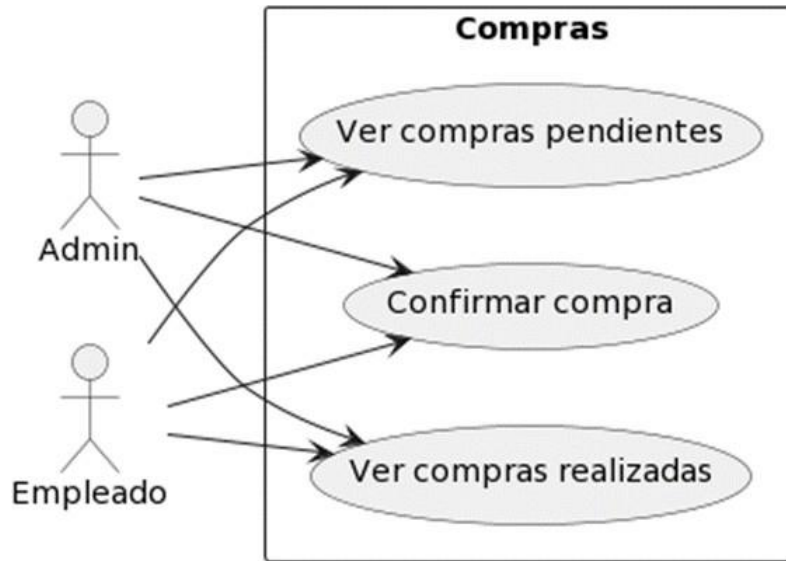
- **Título:** Desarrollar el módulo de ventas.

Descripción: Se verán involucrados los usuarios de tipo administrador y cliente, el cliente podrá ver el estatus de la venta para ver si su pedido a sido enviado, entregado o esta en camino, mientras que el administrador podrá ver las ventas realizadas, las ventas pendientes y confirmar las ventas.

Criterios de aceptación:

- Existe una sección clara en la interfaz del cliente para poder el estatus de la venta del pedido que realizo.
- El usuario administrador puede ver el historial de las ventas realizadas, así como la información relevante.
- Existe una interfaz para el usuario administrador que le permite poder ver las ventas por enviar y también le permite confirmas las ventas para cambiar el estatus de las ventas.

- **Módulo de compras**



Historia de usuario del módulo:

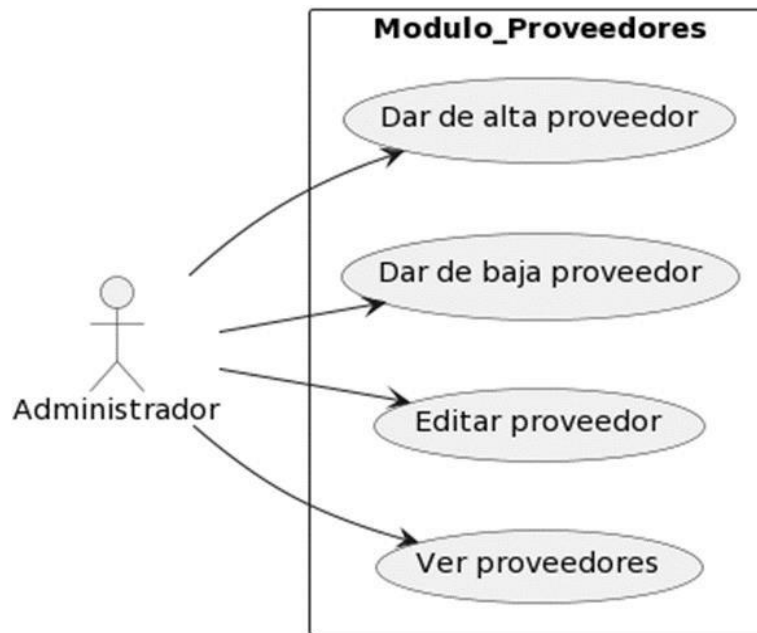
- **Título:** Desarrollar el módulo de compras

Descripción: Se verán involucrados los usuarios de tipo administrador y empleado, ambos usuarios pueden tener acceso a ver las compras pendientes, confirmación de compras y ver las compras realizadas.

Criterios de aceptación:

- Existe una interfaz de usuario que permita a los usuarios involucrados ver las compras pendientes.
- Existe una interfaz que permita con un botón confirmar las compras que han realizado los clientes, esto para que la orden pueda ser procesada.
- Existe una interfaz que permita ver las compras realizadas, esto para ver que pedidos se han realizado.

- **Módulo de proveedores**



Historia de usuario del módulo:

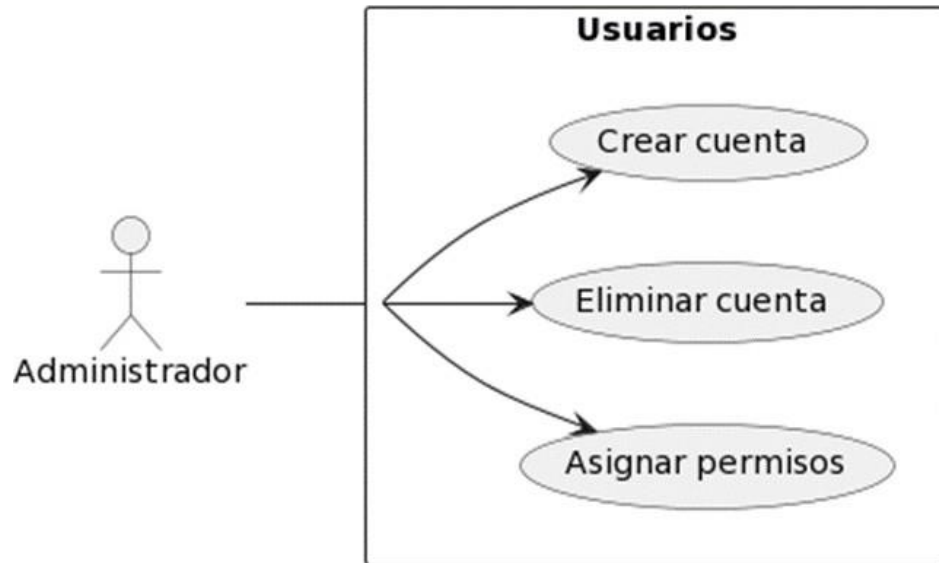
- **Título:** Desarrollar el módulo de proveedores

Descripción: Se verá involucrado el usuario administrador, este será el único que pueda acceder a toda la información de los proveedores igual que a la funcionalidad necesaria del módulo.

Criterios de aceptación:

- Existe una interfaz de usuario que permite al administrador dar de alta a un proveedor, ingresando datos como nombre, rfc, dirección, entre otros.
- En la misma interfaz debe permitir al administrador eliminar al proveedor.
- Debe permitir editar la información del proveedor existente.
- Además, debe ver la información del proveedor.

- **Módulo de usuarios**



Historia de usuario del módulo:

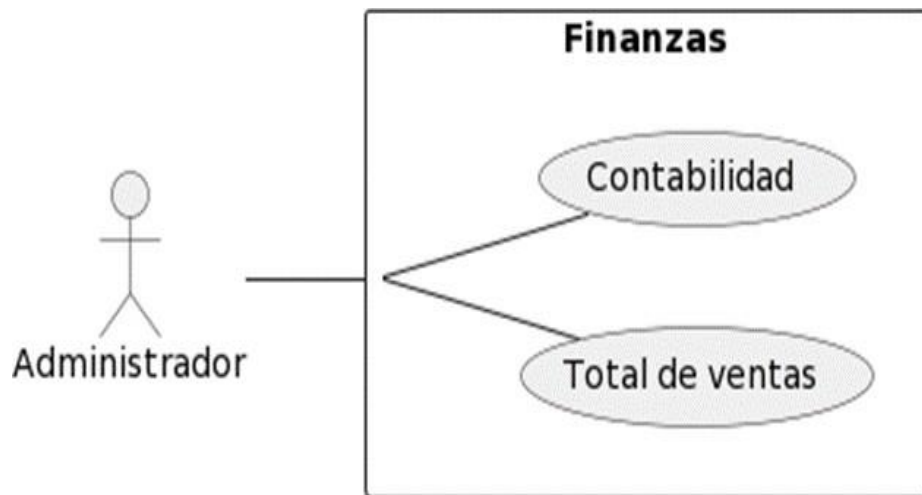
- **Título:** Desarrollar el módulo de usuarios

Descripción: Se verá involucrado el usuario administrador, este será el único que pueda acceder a toda la información de los usuarios, así como asignarle permisos a cada tipo de usuario.

Criterios de aceptación:

- Existirá una interfaz de usuario que permita al administrador crear una cuenta para un usuario que sea empleado.
- Además, podrá eliminar la cuenta del usuario si así lo desea.
- Finalmente podrá asignar los permisos para que el nuevo usuario pueda moverse dentro del sistema.

- **Módulo de finanzas**



Historia de usuario del módulo:

- **Título:** Desarrollar el módulo de finanzas

Descripción: Se verá involucrado el usuario administrador, este será el único que pueda acceder a toda la información del módulo, como lo son la contabilidad y el total de ventas.

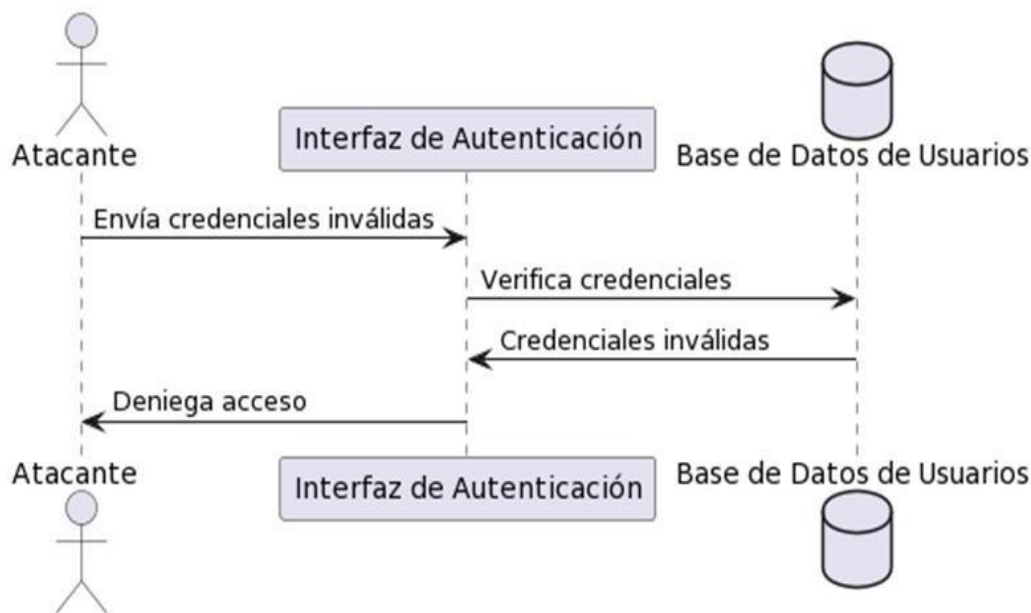
Criterios de aceptación:

- Existe una interfaz de finanzas donde el administrador podrá ver la contabilidad de las ventas.
- Además, podrá ver el total de las ventas gráficamente.

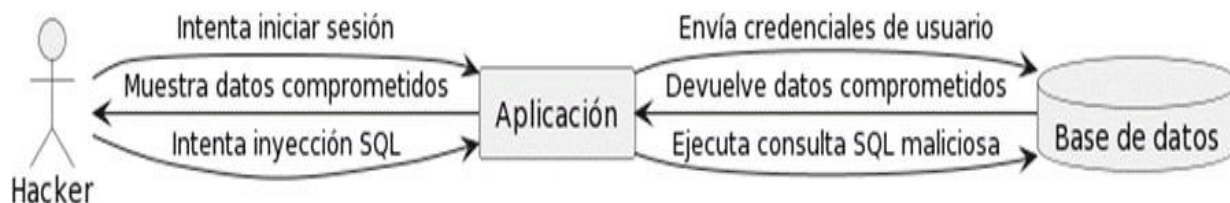
4.3. DIAGRAMAS DE CASOS DE ABUSO.

| Detalles de CA01: Ataque de fuerza bruta a la autenticación de la aplicación | |
|--|---|
| ID caso de abuso: | CA01 |
| Daño: | <ul style="list-style-type: none"> El atacante podría acceder a información confidencial de los usuarios, como sus contraseñas, nombres de usuario, direcciones de correo electrónico, entre otros datos personales. También podría comprometer la seguridad de la aplicación, causando daños a la reputación de la empresa y la pérdida de confianza de los usuarios. |
| Rangos de privilegios: | <ul style="list-style-type: none"> El atacante podría intentar acceder a la cuenta de usuario con los permisos más altos en la aplicación, como el administrador o el superusuario, para obtener acceso completo al sistema. También podría intentar obtener acceso a cuentas de usuarios con privilegios más bajos, como los usuarios regulares, para realizar actividades maliciosas en nombre de ellos |
| Descripción (interacción): | <ul style="list-style-type: none"> El atacante recopila información sobre la autenticación de la aplicación y los posibles nombres de usuario. El atacante utiliza herramientas automatizadas para intentar iniciar sesión en la aplicación utilizando una lista de posibles contraseñas o generando contraseñas aleatorias. Si el ataque es exitoso, el atacante obtiene acceso a la cuenta del usuario y a la información asociada con ella. |

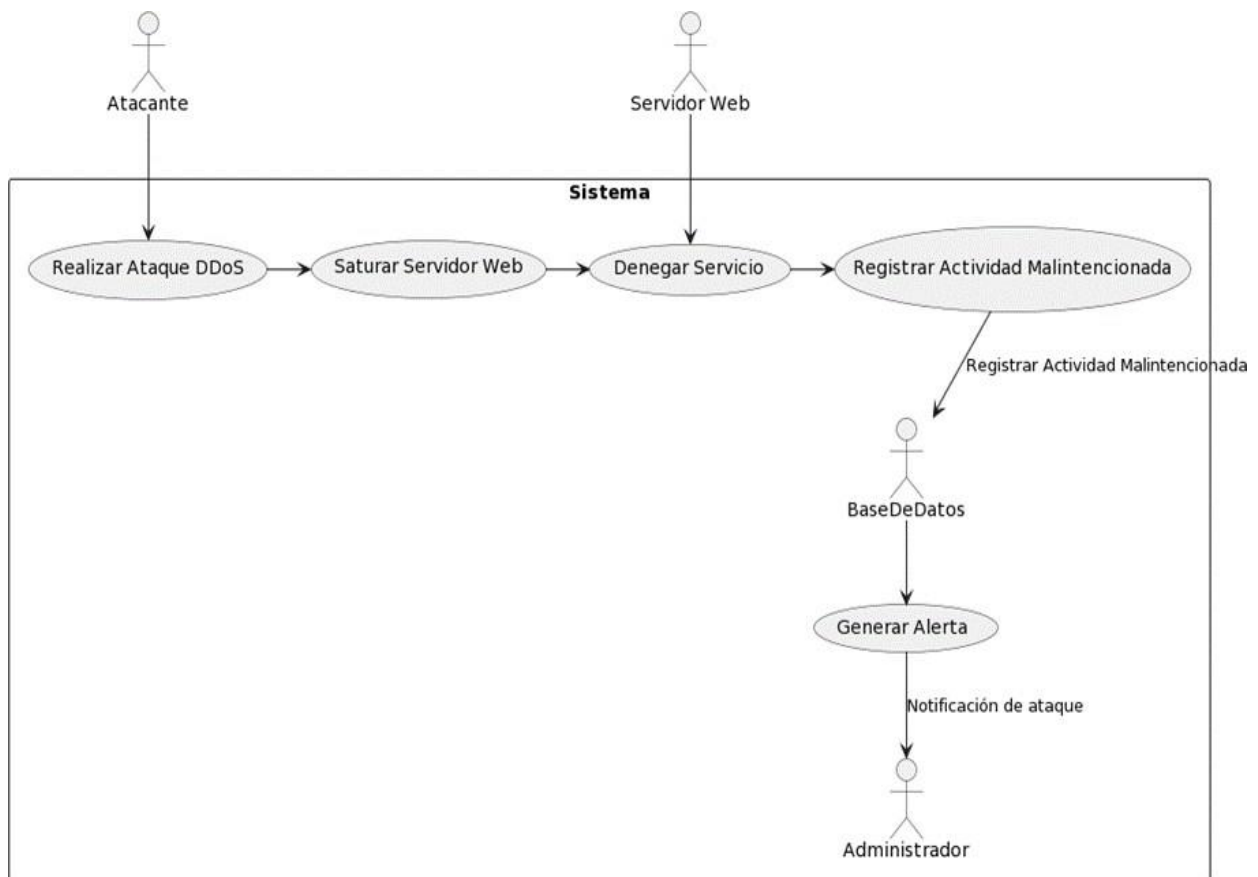
Caso de Abuso - Ataque de Fuerza Bruta a la Autenticación de la Aplicación



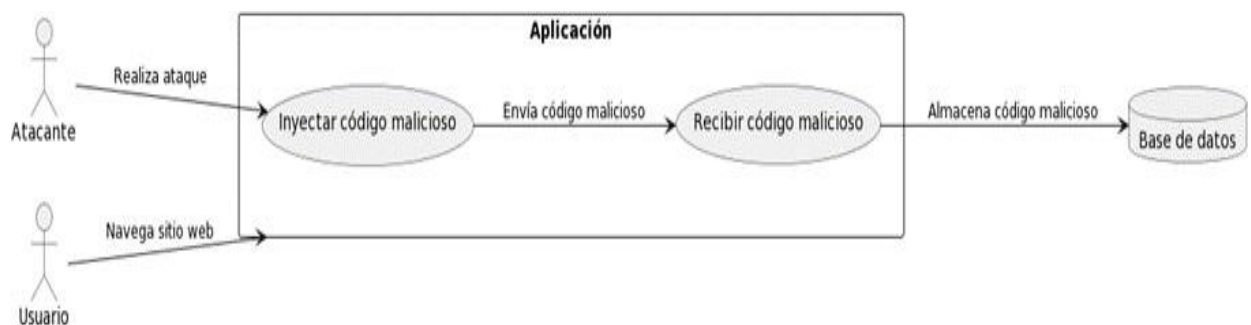
| Detalles de CA02: Ataque de inyección SQL a BD | |
|--|---|
| ID caso de abuso: | CA02 |
| Daño: | <ul style="list-style-type: none"> • Pérdida de información confidencial. • Modificación o eliminación de información importante para la empresa o los usuarios. • Pérdida de confianza de los usuarios en la aplicación web. • Daño a la reputación de la empresa. • Posibles consecuencias legales por causa del robo de información. |
| Rangos de privilegios: | <ul style="list-style-type: none"> • El atacante puede tener cualquier nivel de acceso a la aplicación web. • En función de los permisos de la cuenta comprometida, el atacante podría obtener acceso a información confidencial y/o realizar modificaciones o eliminaciones en la BD, ya que puede acceder al sistema con el rol de administrador y tener acceso a todos los privilegios de la aplicación. |
| Descripción (interacción) | <ul style="list-style-type: none"> • El atacante intenta ingresar datos maliciosos en campos de entrada de la aplicación web, buscando explotar vulnerabilidades en el código que permitan la inyección de código SQL en las consultas a la BD. • Si el ataque es exitoso, el código SQL malicioso puede ser ejecutado por la BD, permitiendo al atacante acceder a información confidencial o realizar modificaciones o eliminaciones en la BD. • Dependiendo de los objetivos del atacante, puede repetir el proceso varias veces, utilizando diferentes técnicas y estrategias para intentar comprometer la seguridad de la aplicación web y la BD. |



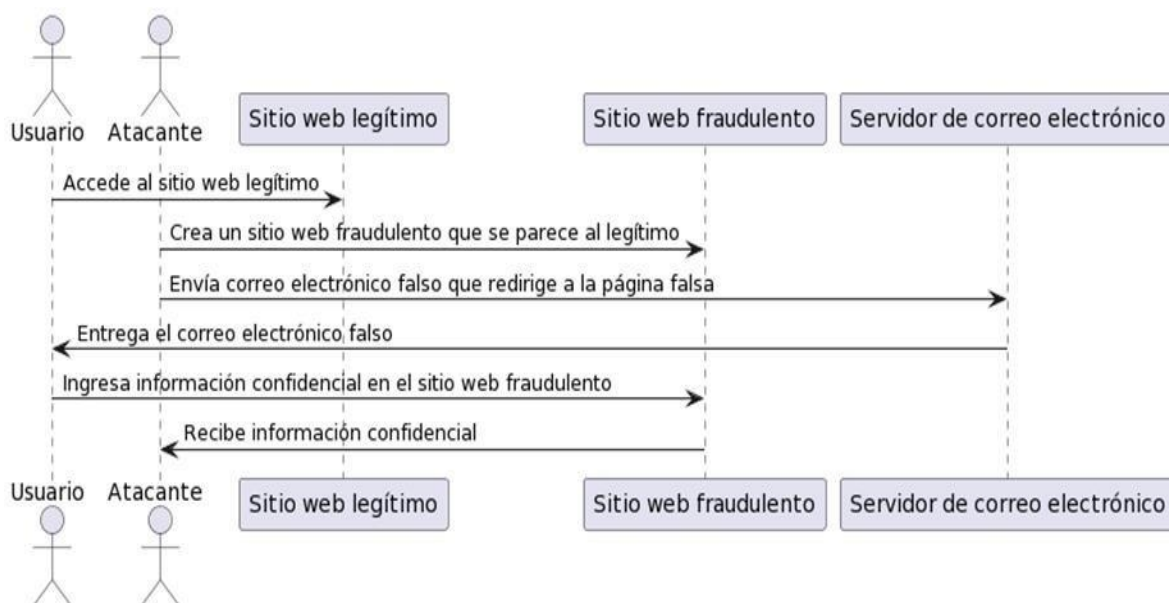
| Detalles de CA03: Ataque de denegación de servicio (DDoS) al servidor web | |
|---|--|
| ID caso de abuso: | CA03 |
| Daño: | <ul style="list-style-type: none"> La denegación del servicio puede causar pérdidas financieras y dañar la reputación de la organización, además de interrumpir el acceso a servicios y recursos vitales para la operación de la organización. |
| Rangos de privilegios: | <ul style="list-style-type: none"> El atacante no necesita tener ningún tipo de privilegio dentro del sistema o la red para realizar el ataque de denegación de servicio. |
| Descripción (interacción) | <ul style="list-style-type: none"> El atacante realiza una investigación del servidor web y sus vulnerabilidades para determinar el mejor método de ataque. El atacante utiliza una herramienta de ataque DDoS para inundar el servidor web con una gran cantidad de tráfico falso o solicitudes maliciosas. El servidor web se satura y deja de responder a las solicitudes legítimas de los usuarios, causando una denegación del servicio. |



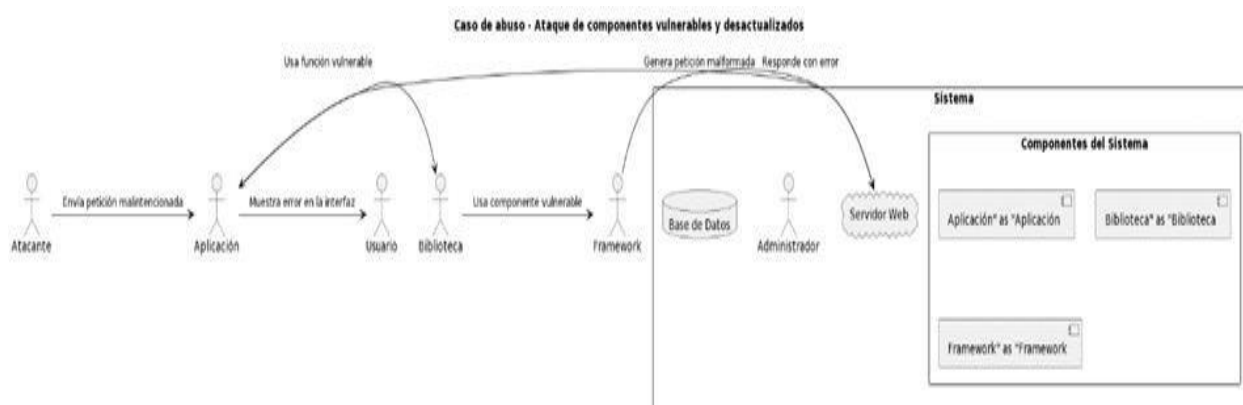
| Detalles de CA04: Ataque de Cross-site scripting (XSS) | |
|--|--|
| ID caso de abuso: | CA04 |
| Daño: | <ul style="list-style-type: none"> • Pérdida de información confidencial del usuario. • Posible compromiso de la cuenta del usuario. • Daño a la reputación de la aplicación web. |
| Rangos de privilegios: | <ul style="list-style-type: none"> • El ataque de Cross-site scripting no requiere ningún tipo de autenticación o nivel de privilegio específico para llevarse a cabo, ya que se basa en la explotación de vulnerabilidades de la aplicación web. Sin embargo, una vez que el ataque se ha llevado acabo con éxito, el alcance del daño dependerá del nivel de privilegios del usuario cuya cuenta ha sido comprometida |
| Descripción (interacción) | <ul style="list-style-type: none"> • El atacante identifica una página vulnerable de la aplicación web que no filtraadecuadamente los datos de entrada. • El atacante inserta código malicioso, como JavaScript, en los campos de entrada de la página, utilizando técnicas de inyección de código. • Cuando un usuario legítimo accede a la página web, el código malicioso se ejecutaen su navegador sin su conocimiento ni consentimiento. |



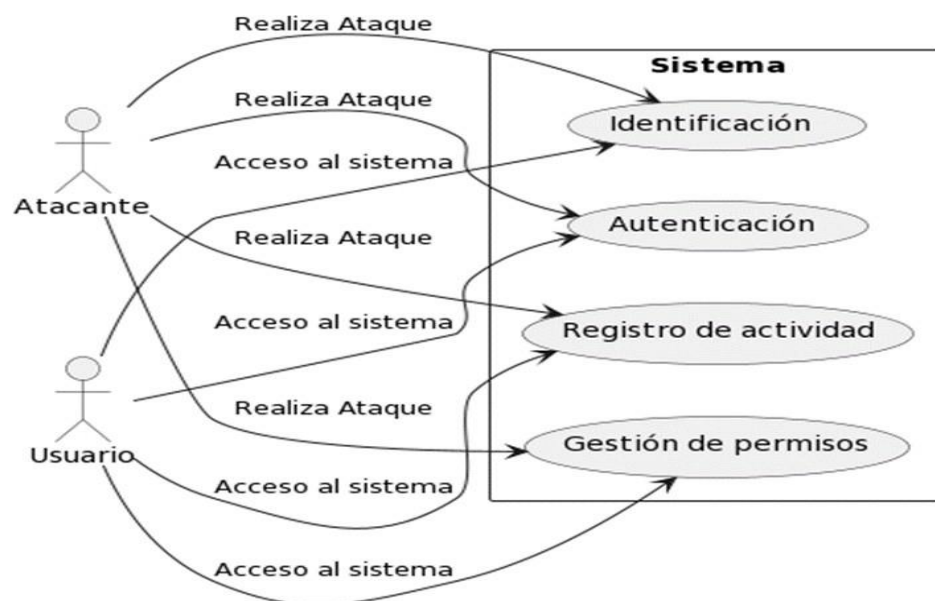
| Detalles de CA05: Ataques mediante Phishing | |
|---|---|
| ID caso de abuso: | CA05 |
| Daño: | <ul style="list-style-type: none"> El daño de un ataque de phishing puede variar desde el acceso no autorizado a cuentas hasta la pérdida de información personal o financiera. El ataque también puede servir como una puerta de entrada para ataques más avanzados, como la instalación de malware. El daño puede ser desde moderado hasta crítico. |
| Rangos de privilegios: | <ul style="list-style-type: none"> El atacante no necesitará acceso directo al sistema o aplicación, ya que el ataque se realiza a través de engaños a los usuarios. El rango de privilegio dependerá de las credenciales que se obtengan. Si se obtienen credenciales de administrador, el daño puede ser mayor. |
| Descripción (interacción) | <ul style="list-style-type: none"> Si el atacante obtiene las credenciales de un usuario con privilegios elevados, puede utilizarlas para acceder a otros sistemas o aplicaciones dentro de la misma organización. El atacante puede utilizar las credenciales obtenidas para manipular datos en la aplicación o sistema objetivo. |



| Detalles de CA06: Componentes vulnerables y desactualizados | |
|---|--|
| ID caso de abuso: | CA06 |
| Daño: | <ul style="list-style-type: none"> El daño de utilizar componentes desactualizados y vulnerables puede variar desde la exposición de datos hasta la ejecución remota de código. El daño puede ser desde moderado hasta crítico. |
| Rangos de privilegios: | <ul style="list-style-type: none"> El atacante no necesitará acceso directo al sistema o aplicación, ya que el ataque se realiza a través de la explotación de vulnerabilidades en los componentes utilizados por la aplicación. El rango de privilegio dependerá de las vulnerabilidades que se exploren. Si se explota una vulnerabilidad que permite la ejecución de código como usuario root, el daño puede ser mayor. |
| Descripción (interacción) | <ul style="list-style-type: none"> Si el atacante explota una vulnerabilidad que le permite ejecutar código con privilegios elevados, puede utilizar esta ventaja para obtener acceso a otros sistemas o aplicaciones en la misma red. Una vez que el atacante ha obtenido acceso a la aplicación o sistema objetivo, puede realizar varias iteraciones de abuso para extraer información confidencial. |

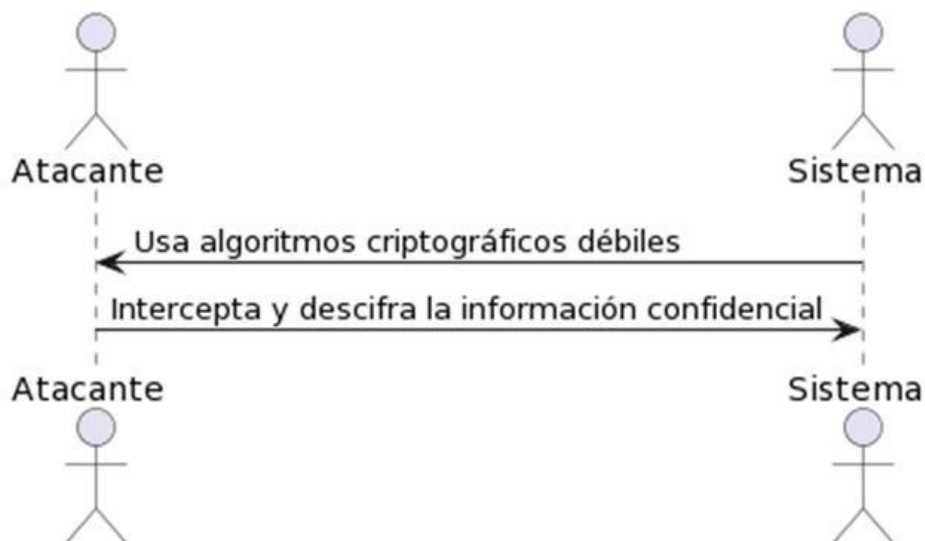


| Detalles de CA07: Fallas de identificación y autenticación | |
|--|--|
| ID caso de abuso: | CA07 |
| Daño: | <ul style="list-style-type: none"> • Si las fallas de identificación y autenticación permiten a los atacantes acceder al sistema con credenciales no válidas o falsificadas, podrán acceder a información confidencial o realizar actividades maliciosas en el sistema. • Los atacantes pueden aprovechar las fallas de identificación y autenticación para acceder a información personal de los usuarios, como calificaciones, contraseñas y otra información confidencial |
| Rangos de privilegios: | <ul style="list-style-type: none"> • Las fallas de identificación y autenticación pueden permitir a los atacantes obtener acceso a cuentas con mayores privilegios de los que deberían tener, lo que les permite realizar actividades maliciosas y acceder a información crítica del sistema. |
| Descripción (interacción) | <ul style="list-style-type: none"> • Las fallas de identificación y autenticación también pueden ser explotadas por los atacantes para realizar una iteración de abuso (también conocida como ataque de fuerza bruta o ataque de diccionario). Este tipo de ataque se realiza mediante el uso de herramientas automatizadas que intentan adivinar o crackear contraseñas débiles o fáciles de adivinar para obtener acceso no autorizado al sistema. |

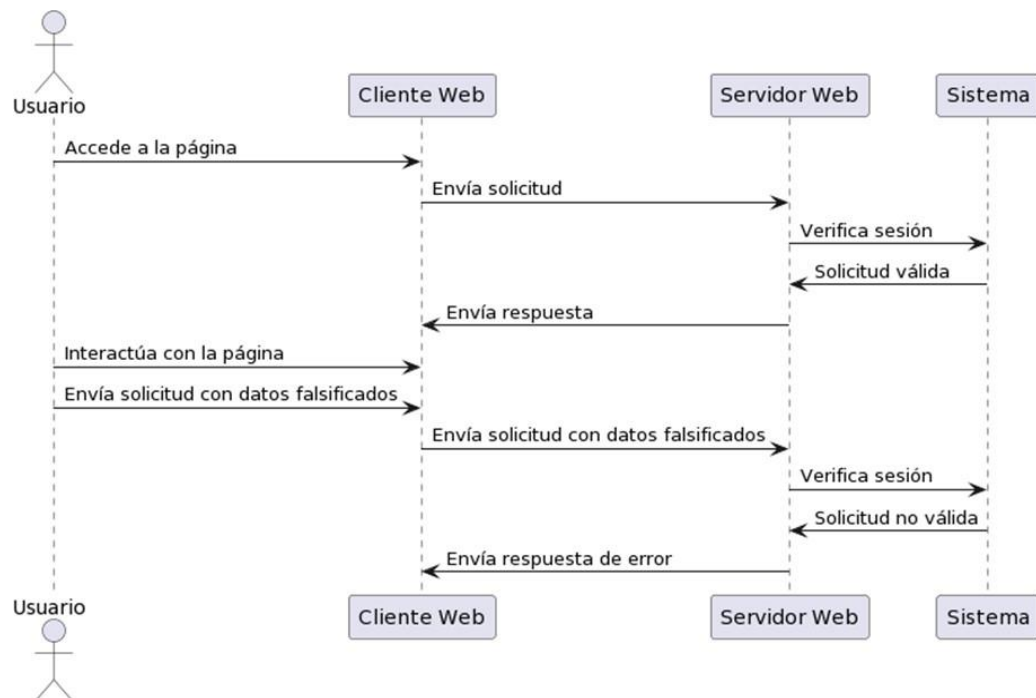


| Detalles de CA08: Fallas Criptográficas | |
|---|---|
| ID caso de abuso: | CA08 |
| Daño: | <ul style="list-style-type: none"> Pueden permitir que los atacantes obtengan acceso no autorizado a datos confidenciales, como información financiera, contraseñas del personal. Esto puede poner en peligro la privacidad y la seguridad de los individuos y organizaciones. También podría saturar el sistema mandando solicitudes al servidor, haciendo que este sea más lento al momento de enviar las peticiones o incluso denegar el servicio de este. |
| Rangos de privilegios: | <ul style="list-style-type: none"> pueden permitir a los atacantes suplantar la identidad de una entidad legítima y acceder a sistemas o información a los que no tienen derecho. Esto puede permitirles realizar actividades maliciosas, como robar datos o realizar transacciones fraudulentas |
| Descripción (interacción) | <ul style="list-style-type: none"> La iteración de abuso de fallas criptográficas puede ser especialmente peligrosa si se utiliza en combinación con otras técnicas de hacking, como la ingeniería social o la explotación de vulnerabilidades de software. |

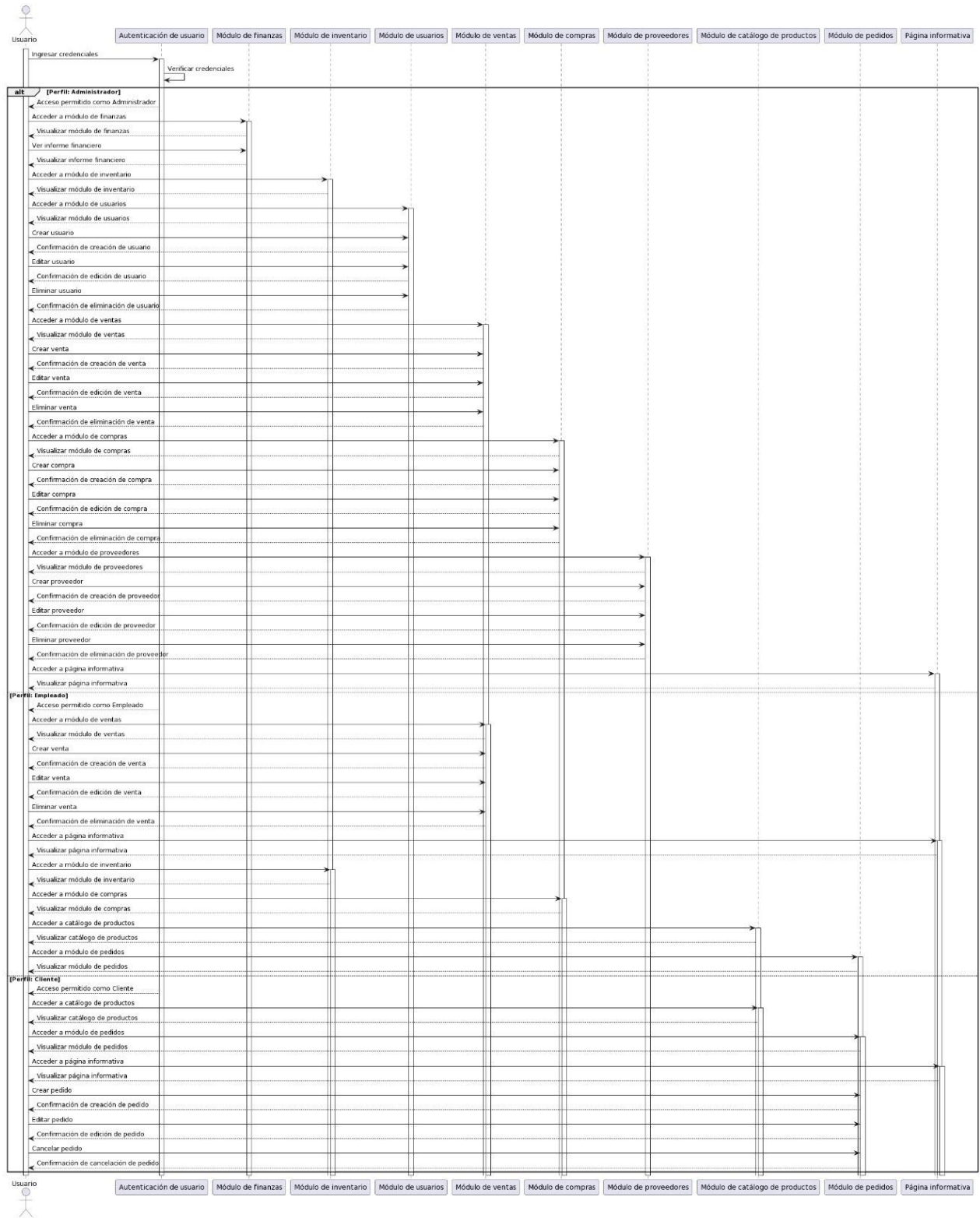
Caso de abuso: Ataque de Fallas Criptográficas



| Detalles de CA09: Falsificación de solicitudes del lado del servidor | |
|--|---|
| ID caso de abuso: | CA09 |
| Daño: | <ul style="list-style-type: none"> • El atacante podría acceder a información confidencial de los usuarios, así como sus • contraseñas, usuario, correo electrónico entre otros datos personales. • También podría saturar el sistema mandando solicitudes al servidor, haciendo que este sea más lento al momento de enviar las peticiones o incluso denegar el servicio de este. • Podría enviar scripts para realizar diferentes actividades o acceder a los diferentes niveles de la aplicación web para si robar información sensible de los usuarios. |
| Rangos de privilegios: | <ul style="list-style-type: none"> • El atacante podría intentar acceder a la cuenta de usuario con los permisos más altos, como un usuario administrador para tener acceso completo a la aplicación. |
| Descripción (interacción) | <ul style="list-style-type: none"> • Un atacante crea una página web malintencionada que contiene un formulario o un enlace que apunta a un sitio web legítimo. Este formulario o enlace realiza una acción en el sitio web legítimo que el atacante desea realizar en nombre del usuario, como cambiar la contraseña o hacer una transferencia de fondos. |

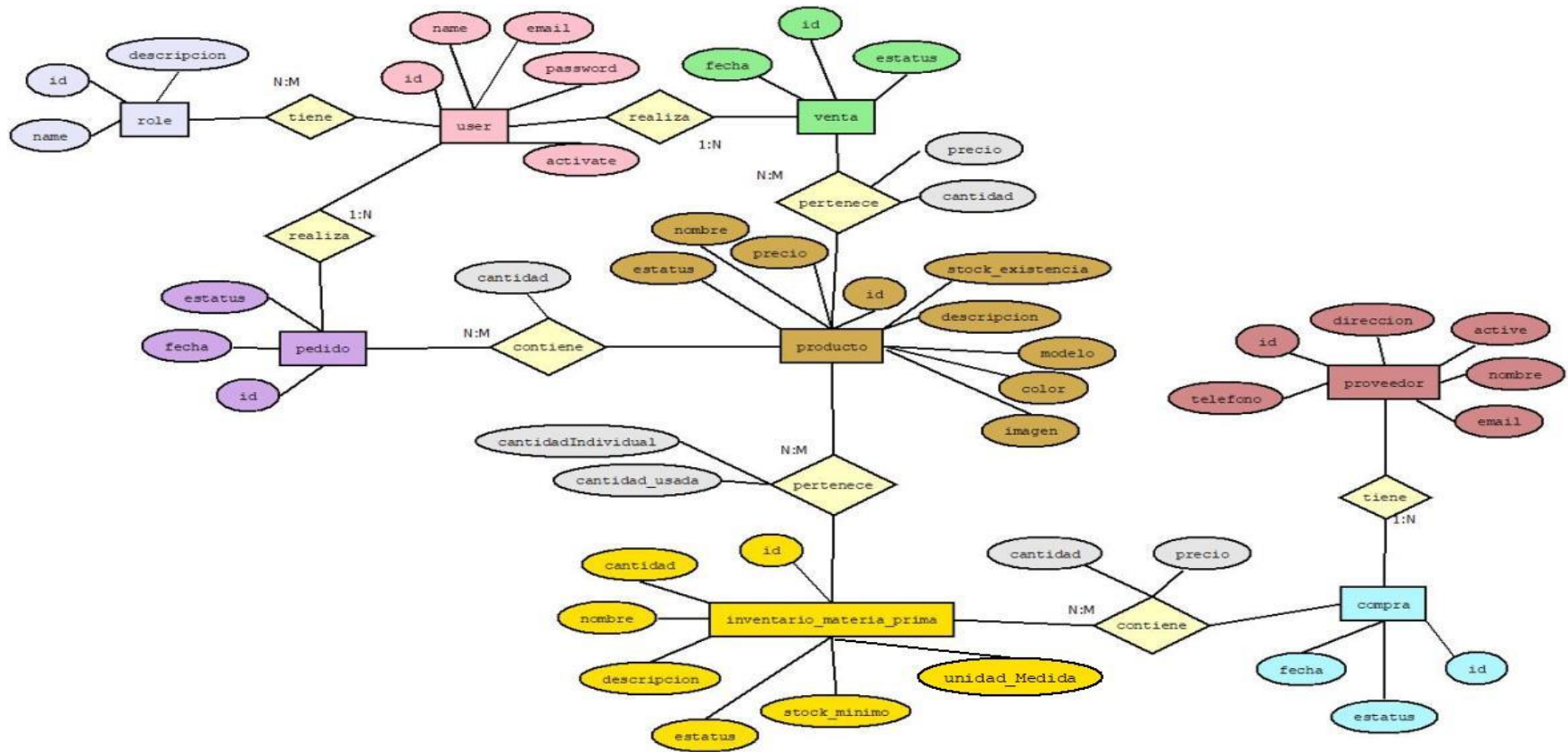


4.4. DIAGRAMA DE SECUENCIA.



5. DIAGRAMA DE BASE DE DATOS

5.1. DIAGRAMA ER



5.2. DIAGRAMA RELACIONAL

