

## 1.1 Glosario

Pruebas de Integración: Evaluación de la interacción entre módulos o componentes.

Pruebas de Sistema: Validación de la aplicación en su conjunto.

Pruebas de Navegabilidad: Compatibilidad del Navegador: Verificación de la funcionalidad en diferentes navegadores (Chrome, Firefox, Safari, etc.).

Adaptabilidad a Dispositivos: Comprobación de la respuesta y la visualización en dispositivos móviles y tabletas.

Pruebas de Rendimiento: Evaluación del desempeño del sistema para medir velocidad y eficiencia.

Carga: Evaluación del tiempo de carga de la página.

Estrés: Verificación de la estabilidad y rendimiento bajo carga extrema.

Volumen: Evaluación del rendimiento con grandes cantidades de datos o usuarios concurrentes.

Seguridad: Medidas implementadas para proteger un sistema o datos contra amenazas y accesos no autorizados.

Pruebas de Penetración: Identificación de posibles vulnerabilidades y brechas de seguridad.

SSL/TLS: Verificación del cifrado de datos mediante protocolos seguros.

Usabilidad: La facilidad con la que los usuarios pueden interactuar con un sistema o producto.

Accesibilidad: Comprobación de la accesibilidad para usuarios con discapacidades.

Facilidad de Uso: Evaluación de la interfaz y la experiencia del usuario.

Compatibilidad con Dispositivos de Asistencia: Verificación del soporte para tecnologías de asistencia.

Contenido: La información presente en un sistema, aplicación o página web, que puede incluir texto, imágenes, multimedia, y otros elementos.

Integridad del Contenido: Verificación de la precisión y coherencia del contenido.

Multimedia: Comprobación del correcto funcionamiento de elementos multimedia (imágenes, videos).

Formularios y Transacciones: La interacción y procesamiento de datos a través de formularios en una aplicación o sitio web, así como la realización segura y eficiente de transacciones, como envíos de datos o procesos de compra.

Validación de Formularios: Verificación de la entrada de datos.

Procesamiento de Pagos: Evaluación de la seguridad y la precisión en transacciones financieras.

Mantenimiento: Actividades planificadas y no planificadas realizadas para asegurar el funcionamiento continuo, la corrección de errores y la actualización de un sistema.

Actualizaciones: Evaluación del proceso de actualización de la página.

Registro de Errores: Implementación de un sistema para rastrear y corregir problemas.

Compatibilidad con Estándares:

Cumplimiento de Estándares Web: Verificación del cumplimiento de normativas como HTML, CSS, etc.

Documentación: Registros detallados y descripciones escritas que explican el funcionamiento, la estructura y el propósito de un sistema, aplicación o proceso.

Manuales de Usuario: Creación de manuales para los usuarios finales.

Informe de Pruebas: Documentación detallada de los resultados de las pruebas.

Cache: La caché es un espacio de almacenamiento temporal que se utiliza para acelerar el acceso a datos frecuentemente utilizados.

Base de datos: Una base de datos es un conjunto organizado de información estructurada que se puede acceder y gestionar de manera electrónica.

Password: Un password o contraseña de datos es una clave de acceso utilizada para proteger la seguridad de información confidencial.

SignIn/login: SignIn o inicio de sesión es el proceso de autenticación de usuario para acceder a un sistema o aplicación

Clic: Clic es una acción mediante la cual se presiona y suelta el botón del mouse para interactuar con un objeto o elemento en una interfaz de usuario.

Formulario web: Un formulario web es una página que permite a los usuarios enviar información a través de una serie de campos.

Archivos multimedia/digitales: Los archivos multimedia/digitales son aquellos que contienen diferentes tipos de contenido como imágenes, audio, video y texto.

Ventana Emergente: Una ventana emergente es una ventana secundaria que aparece automáticamente en una página web sin ser solicitada por el usuario.

Campos: Los campos son áreas de un formulario o base de datos destinadas a contener información específica de un usuario o un registro.

## 1.2 Requerimientos

---

Los requerimientos funcionales para la beta de [www.demoblaze.com](http://www.demoblaze.com) incluyen:

### 1.2.1 Pre-cache

---

Para reducir el tiempo de espera de los usuarios en el sitio web, se podría implementar un pre-caché de los contenidos digitales como fotos o videos. Esto se lograría mediante la realización de una operación batch diaria que permita almacenar en caché los contenidos agregados al sitio en las últimas 24 horas. Esto ayudaría a acelerar la carga de contenido y mejorar la experiencia del usuario.

### 1.2.2 Taxonomía de las URL's

---

Idealmente las URL's deberían ser:

- 1) [www.demoblaze.com](http://www.demoblaze.com) Homepage:
  - <https://www.demoblaze.com/index.html>
- 2) Home de un artículo:
  - <https://www.demoblaze.com/prod.html?idp =1>
- 3) Home de Cart:
  - <https://www.demoblaze.com/cart.html>

## Introducción:

---

El objetivo de este plan de pruebas es asegurar la calidad del sitio web de comercio electrónico que vende productos electrónicos, como laptops, smartphones y monitores. El sitio web ha sido desarrollado y está listo para ser sometido a pruebas para garantizar su funcionalidad, usabilidad, seguridad y

rendimiento. Las pruebas se llevarán a cabo para identificar cualquier defecto, error o problema que pueda impactar la satisfacción del usuario y reducir la calidad del producto.

## Objetivos:

---

Los objetivos principales del plan de pruebas son:

- Evaluar la funcionalidad del sitio web: se comprobará si el sitio web cumple con los requisitos del cliente, incluyendo la capacidad de navegar, buscar, comparar y comprar productos.
- Verificar la usabilidad del sitio web: se evaluará si el sitio web es fácil de usar y si los usuarios pueden interactuar con él sin dificultades.
- Evaluar la seguridad del sitio web: se comprobará si el sitio web es seguro y si los datos personales de los usuarios están protegidos adecuadamente.
- Evaluar el rendimiento del sitio web: se comprobará si el sitio web carga rápido, si no hay problemas de tiempo de respuesta y si se puede manejar la carga de usuarios simultáneos.

## Estrategia de pruebas:

---

La estrategia de pruebas se basará en una combinación de pruebas manuales y automatizadas para cubrir todas las áreas críticas del sitio web. Se utilizarán herramientas de prueba para automatizar las pruebas y reducir el tiempo de prueba, mientras que las pruebas manuales se utilizarán para detectar problemas de usabilidad y otros problemas que no puedan ser detectados por herramientas de prueba.

Se utilizarán los siguientes tipos de pruebas:

- Pruebas de unidad:

Para evaluar el comportamiento y la funcionalidad de cada componente del sitio web de manera aislada.

- Pruebas de integración:

Para verificar la integración y el comportamiento del sitio web completo, incluyendo las conexiones entre los diferentes componentes.

- Pruebas de sistema:

Para evaluar la funcionalidad del sitio web en su conjunto y su capacidad para manejar una carga de usuarios simultáneos.

- Pruebas de aceptación:

Para comprobar si el sitio web cumple con los requisitos del cliente y las expectativas de los usuarios.

- Pruebas de seguridad:

Para verificar la seguridad del sitio web y su capacidad para proteger los datos personales de los usuarios.

## Plan de pruebas:

---

El plan de pruebas se llevará a cabo en varias etapas, cada una de las cuales tendrá objetivos y criterios de finalización específicos. Los siguientes son los elementos clave del plan de pruebas:

- Planificación y diseño de pruebas:

En esta etapa, se definirán los objetivos de las pruebas, se identificarán los requisitos de prueba y se creará un plan de prueba detallado.

- Preparación de pruebas:

En esta etapa, se preparará el entorno de prueba y se configurarán las herramientas de prueba necesarias.

- Ejecución de pruebas:

En esta etapa, se llevarán a cabo las pruebas planificadas y se registrarán los resultados.

- Análisis de resultados:

En esta etapa, se analizarán los resultados de las pruebas para identificar y documentar los defectos, errores o problemas detectados. Cada problema se clasificará según su gravedad y se le asignará a un miembro del equipo para su corrección.

- Corrección de problemas:

En esta etapa, se corregirán los problemas identificados y se volverán a realizar las pruebas necesarias para verificar que se hayan solucionado.

- Verificación de cumplimiento:

En esta etapa, se verificará que el sitio web cumpla con todos los requisitos del cliente y las expectativas de los usuarios.

- Validación del producto:

En esta etapa, se validará que el sitio web esté listo para su lanzamiento y se presentará al cliente para su aprobación final.

## **Criterios de finalización:**

---

Se considerará que el plan de pruebas ha sido completado exitosamente si se cumplen los siguientes criterios de finalización:

- Se han completado todas las pruebas planificadas.
- Todos los problemas detectados se han documentado y se han asignado a un miembro del equipo para su corrección.
- Todos los problemas detectados han sido corregidos y se ha verificado su solución.
- Se ha verificado que el sitio web cumple con todos los requisitos del cliente y las expectativas de los usuarios.
- El cliente ha aprobado el lanzamiento del sitio web.

## **Criterios de inicio de pruebas:**

---

- Definir claramente los requisitos del sitio web, incluyendo funcionalidades, características y aspectos de seguridad.
- Contar con un diseño detallado del sitio web que incluya información sobre la estructura, funcionalidades, características e interfaces de usuario.
- Seleccionar las herramientas de prueba adecuadas para el sitio web que puedan simular un gran número de usuarios, probar la seguridad y detectar problemas de rendimiento.
- Establecer un equipo de pruebas capacitado y experimentado en pruebas de sitios web de comercio electrónico, incluyendo probadores manuales y automáticos, analistas y coordinadores de pruebas.

## Criterios de aprobación / rechazo de las pruebas:

---

- 1) Todos los casos de prueba planificados han sido ejecutados y los resultados han sido documentados.
- 2) Todos los problemas encontrados durante las pruebas han sido documentados y se les ha asignado una prioridad y un propietario para su resolución.
- 3) Los problemas críticos han sido resueltos y verificados por el equipo de pruebas antes de la entrega del producto final.
- 4) La cobertura de las pruebas ha sido adecuada en términos de funcionalidad, rendimiento y seguridad.
- 5) La calidad del software ha alcanzado el nivel requerido por el cliente y cumple con los estándares de calidad establecidos.
- 6) El equipo de pruebas ha proporcionado un informe final detallado que resume todas las pruebas realizadas, los problemas detectados y las soluciones implementadas.
- 7) El cliente ha aprobado los resultados del plan de pruebas y ha autorizado la entrega del producto final.
- 8) Si todos estos criterios se cumplen satisfactoriamente, el plan de pruebas será aprobado y se procederá con la entrega del producto final. En caso contrario, el plan de pruebas será rechazado y se deberá trabajar en la resolución de los problemas encontrados antes de la entrega del producto final.

## Entorno y configuración de las pruebas:

---

Sistema operativo: Windows 10

Navegador: Google Chrome Versión 97.0.4692.99 (64 bits)

Resolución de pantalla: 1920x1080

Conexión a internet: Conexión estable a Internet con una velocidad de descarga mínima de 10 Mbps y una velocidad de carga mínima de 5 Mbps.

## Herramientas de pruebas:

---

Se utilizarán las siguientes herramientas de pruebas para garantizar la efectividad y eficiencia de las pruebas:

- Selenium WebDriver para pruebas automáticas.
- JMeter para pruebas de carga y rendimiento.
- Postman para pruebas de API.
- El equipo de pruebas será responsable de documentar todos los problemas encontrados durante las pruebas y de asignarlos a un miembro del equipo de desarrollo para su corrección. Además, se llevará a cabo una revisión diaria del progreso de las pruebas para garantizar que se estén cumpliendo los plazos establecidos en el calendario de pruebas.

El alcance de las pruebas se enfocará en validar la funcionalidad y usabilidad del sitio web de la tienda en línea, asegurando que los procesos de búsqueda, selección y compra de productos, así como la gestión de cuentas de usuario y el proceso de pago y envío funcionen correctamente. Además, se comprobará que la integración con sistemas externos, como proveedores de pago y servicios de envío, sea efectiva y confiable. Las pruebas se realizarán en múltiples navegadores y dispositivos, asegurando la compatibilidad del sitio web con diferentes entornos y plataformas. Se prestará especial atención a los aspectos de seguridad, incluyendo la protección de datos personales y la prevención de ataques informáticos. El objetivo final es asegurar la calidad del sitio web de la tienda en línea y garantizar una experiencia de usuario satisfactoria para los clientes.

## Planificación de pruebas:

---

Para garantizar la calidad del sitio web de la tienda en línea, se ha establecido un calendario de pruebas que se llevará a cabo durante un período de cuatro semanas. El calendario incluirá las siguientes etapas de pruebas:

- Pruebas unitarias:

Se realizarán pruebas exhaustivas en cada componente del sitio web para asegurarse de que funcionen correctamente de manera individual.



Ejemplo: Se probarán los formularios de registro, los botones de agregar al carrito y las páginas de información de productos para garantizar su funcionalidad.

- Pruebas de integración:

Se probará la integración entre los diferentes componentes del sitio web para asegurarse de que trabajen juntos sin problemas.

Ejemplo: Se probará la integración entre el carrito de compras y el proceso de pago para garantizar una transición sin problemas.

- Pruebas de sistema:

Se probará el sitio web completo como un sistema para verificar su funcionalidad, seguridad y rendimiento en diferentes escenarios.

Ejemplo: Se simularán diferentes cantidades de tráfico en el sitio web para verificar su capacidad de respuesta y detectar cualquier problema de rendimiento.

- Se ha asignado a un equipo de pruebas capacitado y experimentado en pruebas de sitios web de comercio electrónico para realizar las pruebas. El equipo estará compuesto por probadores manuales y automáticos, analistas y coordinadores de pruebas.

## Ambiente de Pruebas:

---

El ambiente de pruebas se ha configurado de manera aislada del ambiente de producción para evitar cualquier impacto negativo en el sitio web de la tienda en línea. Se ha creado un ambiente de pruebas dedicado en un servidor separado y se han instalado las herramientas necesarias para la ejecución de las pruebas.

Además, se han establecido diferentes ambientes de pruebas para las pruebas unitarias, de integración y de sistema. Para las pruebas unitarias, se ha creado un ambiente de pruebas local en el equipo de cada desarrollador, donde se realizan las pruebas individuales de cada componente del sistema. Para las pruebas de integración, se ha creado un ambiente de pruebas en el servidor de integración donde se realizan las pruebas de integración entre los diferentes componentes del sistema. Finalmente, para las pruebas de sistema, se ha creado un ambiente de pruebas en el servidor de pruebas, donde se realiza la ejecución de las pruebas finales del sistema completo.

Se ha establecido un proceso de control de cambios para garantizar que todas las modificaciones realizadas en el ambiente de pruebas se realicen de manera controlada y se registren adecuadamente. Además, se ha definido un procedimiento de restauración de la base de datos de pruebas a un estado anterior para facilitar la repetición de pruebas y evitar interferencias entre diferentes pruebas.

## Gestión de incidentes:

---

Durante las pruebas, se registrarán y gestionarán todos los incidentes detectados. Los incidentes serán documentados en un sistema de seguimiento de problemas y asignados a un miembro del equipo para su resolución.

El sistema de seguimiento de problemas se actualizará regularmente para reflejar el estado actual de cada incidente. Los incidentes se clasificarán según su prioridad y gravedad para asegurar que los más críticos sean abordados primero.

Una vez que se resuelva un incidente, se realizarán pruebas adicionales para verificar que la solución fue exitosa. Si la solución es efectiva, el incidente se cerrará en el sistema de seguimiento de problemas. Si el incidente persiste o se detectan problemas adicionales, se volverá a abrir y se asignará a un miembro del equipo para su resolución.

Se proporcionará un informe final de incidentes para el cliente y el equipo de desarrollo después de que se completen las pruebas. Este informe incluirá detalles de todos los incidentes detectados, incluyendo su prioridad, gravedad y estado de resolución.

## Criterios de aceptación:

---

- Funcionalidad:

Todas las funcionalidades del sitio web deben cumplir con los requisitos del cliente y ser accesibles y utilizables para los usuarios. Se considerará que este criterio se ha cumplido si no hay problemas funcionales importantes reportados por los usuarios en un período de una semana después del lanzamiento.

- Rendimiento:

El sitio web debe ser capaz de manejar un alto volumen de tráfico sin experimentar tiempos de carga prolongados o errores. Se considerará que este criterio se ha cumplido si el sitio web mantiene un tiempo de carga promedio de menos de 3 segundos y no se experimentan errores graves bajo cargas de trabajo normales.

- Seguridad:

El sitio web debe ser resistente a ataques y proteger los datos personales y financieros de los usuarios. Se considerará que este criterio se ha cumplido si no hay brechas de seguridad significativas reportadas en un período de un mes después del lanzamiento.

- Usabilidad:

El sitio web debe ser fácil de usar y navegar para los usuarios, con una interfaz clara e intuitiva. Se considerará que este criterio se ha cumplido si no hay problemas importantes de usabilidad reportados por los usuarios en un período de una semana después del lanzamiento.

- Compatibilidad:

El sitio web debe ser compatible con diferentes navegadores, dispositivos y sistemas operativos. Se considerará que este criterio se ha cumplido si el sitio web funciona correctamente en al menos el 90% de las combinaciones de navegadores, dispositivos y sistemas operativos probados.

- Aprobación del cliente:

El cliente debe aprobar los resultados de las pruebas y estar satisfecho con la calidad del sitio web. Se considerará que este criterio se ha cumplido si el cliente emite una aprobación formal y sin reservas del sitio web después de las pruebas.

- Especificaciones adicionales:

- 1) Se debe documentar cada prueba realizada, incluyendo el resultado y cualquier problema o error detectado.
- 2) Se debe clasificar cada problema o error según su gravedad, y asignar un miembro del equipo para su corrección.
- 3) Se debe realizar una verificación final del sitio web antes de su lanzamiento, para asegurarse de que cumpla con todos los requisitos del cliente y las expectativas de los usuarios.

## Requisitos:

---

- Requisito funcional:

El sitio web debe permitir a los usuarios realizar búsquedas de productos electrónicos, como laptops, smartphones y monitores. Esto incluye la implementación de un motor de búsqueda eficiente que permita a los usuarios buscar productos por categorías, características técnicas y precios.

- Requisito funcional:

El sitio web debe permitir a los usuarios comparar productos electrónicos seleccionados. Esto implica la implementación de una funcionalidad de comparación que muestre claramente las características técnicas y precios de los productos seleccionados para facilitar la toma de decisiones de compra.

- Requisito funcional:

El sitio web debe permitir a los usuarios agregar productos electrónicos al carrito de compra y completar el proceso de compra y pago. Esto incluye la implementación de un carrito de compra funcional que permita a los usuarios agregar, editar y eliminar productos, así como ingresar la información de pago de forma segura.

- Requisito de compatibilidad:

El sitio web debe ser compatible con los principales navegadores web, como Google Chrome, Mozilla Firefox, Microsoft Edge y Safari. Esto implica que el sitio web debe ser probado y optimizado para asegurar que se muestre correctamente y funcione sin problemas en cada uno de estos navegadores.

- Requisito de usabilidad:

El sitio web debe ser fácil de usar y navegar. Esto implica la implementación de una interfaz de usuario intuitiva con etiquetas y botones claros, y un flujo de navegación lógico que facilite la búsqueda, comparación y compra de productos electrónicos.

- Requisito de diseño responsive:

El sitio web debe ser diseñado de forma responsive, es decir, debe adaptarse correctamente a diferentes dispositivos y tamaños de pantalla, incluyendo computadoras de escritorio, laptops, smartphones y tablets, tanto en modo horizontal como vertical. Esto implica que el sitio web debe ser probado

en diferentes dispositivos para asegurar su apariencia, legibilidad y funcionalidad en cada uno de ellos.

- Requisito de seguridad:

El sitio web debe cumplir con las mejores prácticas de protección de datos personales y financieros. Esto implica la implementación de encriptación de la información sensible, validación adecuada de los formularios de ingreso de datos y protección contra posibles vulnerabilidades de seguridad.

- Requisito de rendimiento:

El sitio web debe cargar rápidamente y manejar una carga de usuarios simultáneos sin problemas. Esto implica realizar pruebas de rendimiento para identificar posibles cuellos de botella en el rendimiento y proponer mejoras para asegurar una experiencia rápida y fluida para los usuarios.

- Requisito de compatibilidad con sistemas operativos y dispositivos:

El sitio web debe ser compatible con diferentes sistemas operativos y dispositivos, incluyendo Windows, macOS, iOS y Android, así como laptops, smartphones y tablets. Esto implica que el sitio web debe ser probado y optimizado para asegurar su apariencia, funcionalidad y compatibilidad en cada uno de estos sistemas operativos y dispositivos.

## Funcionalidades no cubiertas para el plan de pruebas:

---

- Búsqueda avanzada:

La búsqueda por características técnicas y precios de los productos electrónicos no será implementada en esta versión del sitio web. Por lo tanto, no se realizarán pruebas de funcionamiento y rendimiento de esta funcionalidad.

- Comparación de productos en tiempo real:

La funcionalidad de comparación de productos seleccionados en tiempo real no será implementada en esta versión del sitio web. Por lo tanto, no se realizarán pruebas de funcionamiento y rendimiento de esta funcionalidad.

- Pruebas exhaustivas en diferentes navegadores:

Debido a limitaciones de tiempo y recursos, las pruebas exhaustivas en todos los principales navegadores web,

incluyendo Google Chrome, Mozilla Firefox, Microsoft Edge y Safari, no se realizarán en esta versión del sitio web.

- Pruebas de seguridad en profundidad:

Si bien se implementarán las mejores prácticas de protección de datos personales y financieros, no se realizarán pruebas de seguridad en profundidad para identificar posibles vulnerabilidades y brechas de seguridad en esta versión del sitio web.

- Pruebas de rendimiento en carga máxima:

Debido a limitaciones de recursos y capacidad de carga, las pruebas de rendimiento en carga máxima con usuarios simultáneos no se realizarán en esta versión del sitio web.

- Integración con redes sociales:

La integración con redes sociales, como compartir productos en redes sociales o autenticación mediante redes sociales, no será implementada en esta versión del sitio web. Por lo tanto, no se realizarán pruebas de funcionamiento y rendimiento de esta funcionalidad.

- Funcionalidades de recomendación de productos:

Las funcionalidades de recomendación de productos basadas en el historial de compra o preferencias del usuario no serán implementadas en esta versión del sitio web. Por lo tanto, no se realizarán pruebas de funcionamiento y rendimiento de estas funcionalidades.

- Establecer políticas claras de confidencialidad:

La empresa debe establecer políticas claras de confidencialidad para los testers y asegurarse de que estén debidamente capacitados y comprometidos a mantener la privacidad y la confidencialidad de la información del usuario.

- Utilizar datos de prueba en un entorno controlado:

La empresa debe proporcionar un entorno de pruebas controlado para que los Testers inserten datos de prueba y así evitar que se inserten en la base de datos real. Además, se debe implementar un proceso de eliminación de datos de prueba después de que se complete la sesión de testing.

- Realizar pruebas de penetración de seguridad:

La empresa debe contratar a expertos en seguridad para realizar pruebas de penetración en la página web y abordar adecuadamente las vulnerabilidades de seguridad identificadas. Además, se deben implementar medidas de

seguridad adicionales para proteger la página web de los ataques de los hackers.

## Sign In / Sign Up

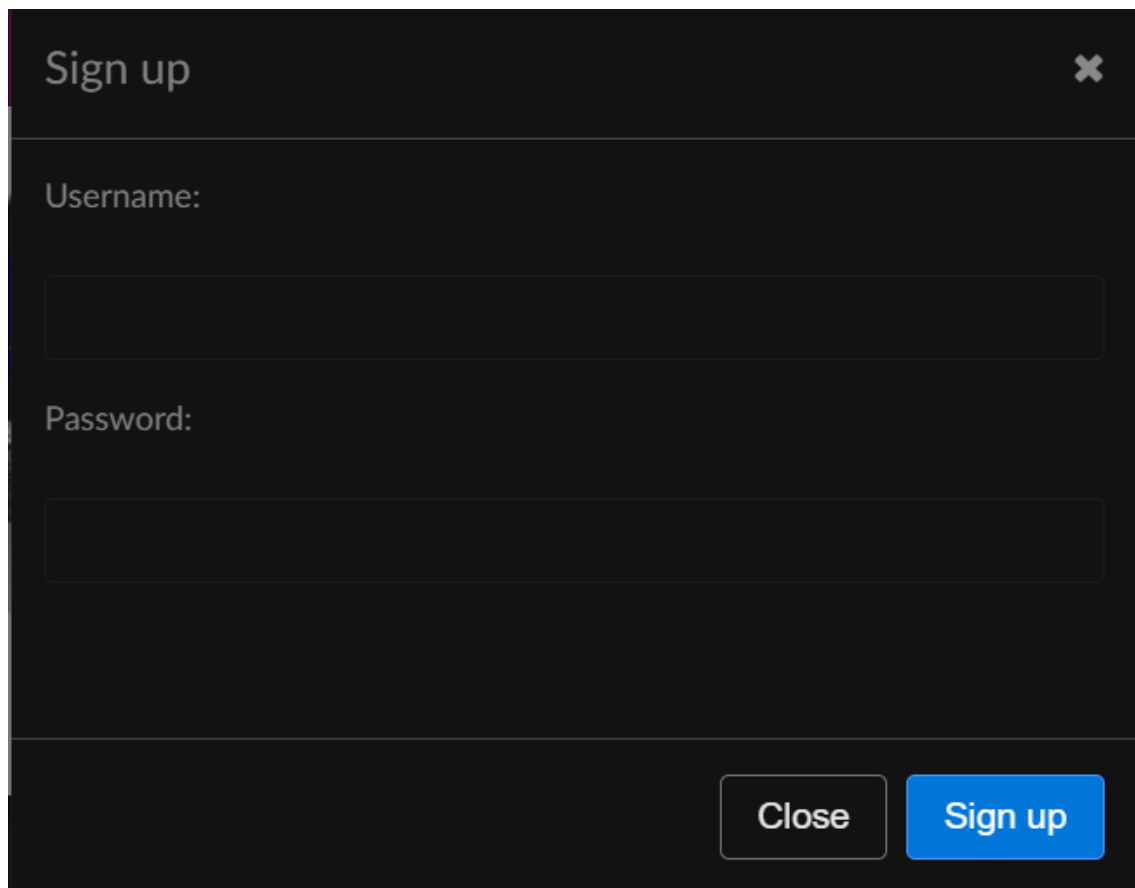
---

Sign Up / Sign In en [www.demoblaze.com](http://www.demoblaze.com) incluye:

- 1) Creación de una cuenta Demoblaze.
- 2) Formulario Pop-Up de Sign Up.
- 3) Formulario Pop-Up de Sign In.

### **Creación de una cuenta Demoblaze (Sign Up):**

Es obligatorio completar todos los campos descritos a continuación, a menos que se indique lo contrario. Cualquier campo numérico debe ser ingresado como un número entero, a menos que se especifique lo contrario. Además, se debe proporcionar una página de modificación de Cuenta Demoblaze para que los usuarios puedan actualizar su información de perfil según sea necesario. Esto permitirá una experiencia de usuario más personalizada y mejorará la calidad de los datos en el sitio web.

A dark-themed pop-up form titled "Sign up" with a close button (X) in the top right corner. The form contains two input fields: "Username:" and "Password:". At the bottom right, there are two buttons: "Close" and "Sign up".

Sign up

Username:

Password:

Close Sign up

1) Campo tipo texto "Username":

- Longitud máxima de 25 caracteres.
- Si el campo no se completa, se mostrará un mensaje de error en rojo que indique "Por favor, complete el Username".
- Se deben aplicar restricciones de validación de datos, como permitir solo letras sin espacios en blanco en este campo.
- Si se ingresa un carácter no válido el sistema no debe permitir ingresarlo y se mostrará un mensaje tipo "alert" con el mensaje: "Formato no válido".
- Se puede agregar una descripción o ayuda contextual para explicar claramente lo que se espera que los usuarios ingresen en este campo, por ejemplo, "Ingresa su Username sin espacios en blanco. Pueden ser letras y números únicamente".

2) Campo tipo "Password":

- El campo debe tener un límite máximo de 12 caracteres.
- Si el usuario no completa el campo, se debe mostrar un mensaje de error indicando "Por favor ponga una password".
- El color de la fuente del campo debe cambiar a rojo si se produce un error.
- Se puede agregar una descripción o ayuda contextual para explicar claramente lo que se espera que los usuarios ingresen en este campo, por ejemplo, "Ingresa su Password sin espacios en blanco. Pueden ser letras minúsculas y mayúsculas, números y caracteres especiales".
- Colocar una leyenda a modo de ejemplo y de recomendación de cómo debe estar compuesta una contraseña segura.

**Iniciar sesión en Demoblaze (Log In):**

Al hacer clic en el botón Log In de la barra de navegación de la Home de Demoblaze, se abrirá el siguiente Pop-Up:



Log in

Username:

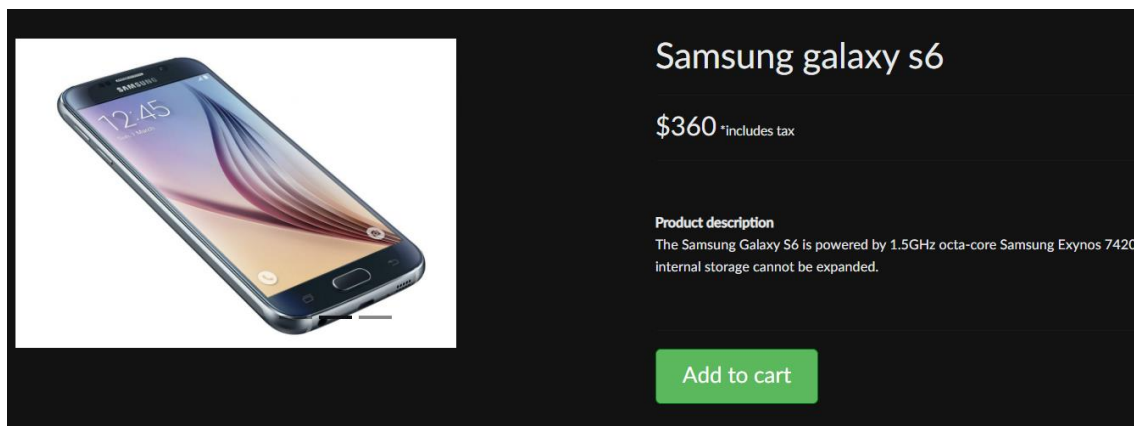
Password:

Close Log in

- 1) Una vez validado el email y el password, accederá a la página descrita en “Cómo se ve la home de cada usuario registrado” (**Out of Scope**).
- 2) Si los datos ingresados de usuario o password no son válidos, el sistema deberá:
  - Mostrar un “alert” con el mensaje de error: “User does not exist.”.
  - Limpiar los campos email y password.
  - Cambiar el color del texto a rojo para destacar el error en el campo correspondiente.
  - Al tercer intento fallido:
    - a) El sistema debe bloquear la cuenta para que no se pueda volver a ingresar hasta que lo autorice el administrador.
    - b) Se debe enviar un correo al administrador con el email del usuario, fecha y hora del momento en que se bloqueó la cuenta.
    - c) Se debe enviar un email al usuario notificándole que la cuenta está bloqueada temporalmente debido a múltiples intentos fallido a TM.
- 3) Link “Te olvidaste tu password?” (Link de re direccionamiento)(**Out of Scope**).

- a) El usuario hace clic en el enlace "Te olvidaste tu password?".
- b) El usuario ingresa su nombre, apellido y correo electrónico.
- c) El usuario hace clic en el botón "Enviar".
- d) El sistema envía un correo electrónico al correo ingresado con una clave de única vez.
- e) El correo electrónico incluye instrucciones para cambiar la contraseña en el siguiente inicio de sesión.
- f) El usuario inicia sesión en el sitio web con la clave de única vez proporcionada.
- g) El sistema requiere que el usuario cambie la contraseña en su primer inicio de sesión después de la recuperación de la contraseña.
- h) El usuario cambia la contraseña y se redirige a la página de inicio de sesión.

### **Agregar un producto al Cart:**





1. Para acceder a esta página, es necesario que el usuario seleccione un producto.
2. Se debe visualizar las características del producto en cuestión, la imagen del mismo, el nombre del producto, su precio y si incluye impuestos.
3. Deberá contar con un botón "Add to Cart".
4. Al hacer clic en el botón Add to Cart, debe mostrarse un alert con el siguiente mensaje: "Product added."

www.demoblaze.com dice

Product added

Aceptar

### Productos agregados al Cart:

Products				Total
Pic	Title	Price	x	720
	Samsung galaxy s6	360	Delete	Place Order
	Samsung galaxy s6	360	Delete	

1. Los productos deben visualizarse uno debajo del otro con sus precios unitarios en una respectiva fila.
2. Deberá contar con un totalizador en la última columna a la derecha del Cart.
3. El Total (suma de los precios unitarios de cada producto más los impuestos) debe estar visible.
4. Si se quita un producto del Cart, el campo Total debe reflejar al instante la modificación en la suma de los productos.
5. Cálculo de totales de precios de productos:

Precio unitario	IVA	Sub Total	Total
360	21	435.6	
360	21	435.6	
			871.2

6. Los cálculos de los totales debe regirse por el siguiente procedimiento matemático:
  - a. Precio unitario \* 0.21 = Sub Total.
  - b. Total = (Suma de todos los Sub Totales).

**Realizar la compra (Place Order):**

Place order

Total: 720

Name:

Country:

City:

Credit card:

Month:

Year:

Close

Purchase

### 1) Campo tipo texto "Nombre":

- Longitud máxima de 75 caracteres.
- Si el campo no se completa, se mostrará un mensaje de error en rojo que indique "Por favor, complete el/los nombre/s".
- Se deben aplicar restricciones de validación de datos, como permitir solo letras y espacios en blanco en este campo.
- Si se ingresa un carácter no válido el sistema no debe permitir ingresarlo y se mostrará un mensaje tipo "alert" con el mensaje: "Formato no válido".
- Se puede agregar una descripción o ayuda contextual para explicar claramente lo que se espera que los usuarios ingresen en este campo, por ejemplo, "Ingresa su nombre y/o nombres separados por espacios".

### 2) Campo tipo texto "Country":

- Longitud máxima de 50 caracteres:  
El campo "Country" no debe aceptar más de 50 caracteres.
- Formato alfabético:  
Solo se permiten letras y espacios en blanco en el campo "Country".
- Campo obligatorio:  
Si el campo "Country" se deja en blanco, se debe mostrar un mensaje de error en rojo que indique: "Por favor, seleccione un país".
- Validación de formato especial:  
Se deben permitir caracteres especiales específicos para países que los utilicen (por ejemplo, apóstrofes en nombres como "Côte d'Ivoire").
- Selección de lista desplegable:  
Se puede considerar implementar el campo "Country" como una lista desplegable para garantizar selecciones válidas y mejorar la experiencia del usuario.
- Autocompletado o sugerencias:  
Proporcionar sugerencias automáticas basadas en la entrada del usuario para facilitar la selección del país.
- Validación en tiempo real:

Realizar validación en tiempo real mientras el usuario completa el campo, mostrando mensajes de error instantáneos si se ingresan datos no válidos.

- Compatibilidad con múltiples idiomas:  
Asegurarse de que el campo "Country" sea sensible a diferentes idiomas y regiones, mostrando nombres de países en el idioma seleccionado por el usuario.
- Pruebas de límites:  
Verificar el comportamiento del sistema ante nombres de países largos y cortos, así como ante la inserción de espacios adicionales al principio o final del nombre.
- Validación de ingreso manual:  
Asegurarse de que los usuarios puedan ingresar manualmente el nombre de su país incluso si no está presente en la lista desplegable, pero manteniendo las restricciones de formato.

### 3) Campo tipo texto "City":

- Longitud máxima de 50 caracteres:  
El campo "Country" no debe aceptar más de 50 caracteres.
- Formato alfabético:  
Solo se permiten letras y espacios en blanco en el campo "Country".
- Campo obligatorio:  
Si el campo "Country" se deja en blanco, se debe mostrar un mensaje de error en rojo que indique: "Por favor, seleccione un país".
- Validación de formato especial:  
Se deben permitir caracteres especiales específicos para países que los utilicen (por ejemplo, apóstrofes en nombres como "Côte d'Ivoire").
- Selección de lista desplegable:  
Se puede considerar implementar el campo "Country" como una lista desplegable para garantizar selecciones válidas y mejorar la experiencia del usuario.
- Autocompletado o sugerencias:  
Proporcionar sugerencias automáticas basadas en la entrada del usuario para facilitar la selección del país.
- Validación en tiempo real:

Realizar validación en tiempo real mientras el usuario completa el campo, mostrando mensajes de error instantáneos si se ingresan datos no válidos.

- Compatibilidad con múltiples idiomas:  
Asegurarse de que el campo "Country" sea sensible a diferentes idiomas y regiones, mostrando nombres de países en el idioma seleccionado por el usuario.
- Pruebas de límites:  
Verificar el comportamiento del sistema ante nombres de países largos y cortos, así como ante la inserción de espacios adicionales al principio o final del nombre.
- Validación de ingreso manual:  
Asegurarse de que los usuarios puedan ingresar manualmente el nombre de su país incluso si no está presente en la lista desplegable, pero manteniendo las restricciones de formato.

#### 4) Campo tipo texto "Credit Card":

- Longitud válida de la tarjeta:  
El campo "Credit Card" debe aceptar el número correcto de dígitos según el tipo de tarjeta (por ejemplo, 16 dígitos para Visa y MasterCard).
- Formato numérico:  
Solo se deben permitir caracteres numéricos en el campo "Credit Card".
- Campo obligatorio:  
Si el campo "Credit Card" se deja en blanco, se debe mostrar un mensaje de error indicando que el campo es obligatorio.
- Validación de tipo de tarjeta:  
Implementar validación para determinar si el número de tarjeta coincide con un formato válido para Visa, MasterCard, American Express, etc.
- Número de tarjeta enmascarado:  
Mostrar los últimos cuatro dígitos de la tarjeta enmascarados para mayor seguridad y confirmación visual.
- Fecha de vencimiento:  
Incluir campos separados para el mes y el año de vencimiento de la tarjeta y validar que estén dentro del rango permitido.

- Campo de código de seguridad (CVV):

Incluir un campo para el código de seguridad (CVV) y validar que tenga la longitud correcta según el tipo de tarjeta.

- Alerta de seguridad:

Mostrar un mensaje de alerta si el usuario intenta ingresar una tarjeta vencida.

- Rechazo de tarjetas bloqueadas o inválidas:

Validar la tarjeta contra una lista de tarjetas bloqueadas o inválidas.

- Confirmación de datos:

Antes de enviar el formulario, proporcionar una confirmación visual de los detalles de la tarjeta ingresada para evitar errores.

- Seguridad en la transmisión:

Garantizar que la información de la tarjeta se transmita de manera segura mediante el uso de protocolos de cifrado (por ejemplo, SSL/TLS).

- Mensajes de error específicos:

Mostrar mensajes de errores claros y específicos en caso de que el número de tarjeta, la fecha de vencimiento o el código de seguridad sean incorrectos.

##### 5) Campo tipo date "Month":

- Campo obligatorio:

Si el campo "Month" se deja en blanco, se debe mostrar un mensaje de error indicando que el campo es obligatorio.

- Selección válida de mes:

El campo "Month" debe permitir solo la selección de un mes válido (1-12).

- Presentación visual:

Presentar los meses en un formato fácilmente comprensible, como una lista desplegable con nombres de meses.

- Formato numérico y/o textual:

Permitir la entrada del mes tanto en formato numérico (por ejemplo, "01" para enero) como en formato textual (por ejemplo, "Enero").



- Validación de formato de entrada:

Validar que la entrada del usuario siga el formato correcto y proporcionar mensajes de error claros si se detectan problemas.

- Control de límites:

Verificar que el campo "Month" acepte únicamente valores dentro del rango de meses válidos (1-12).

- Asociación con el año de vencimiento:

Coordinar el campo "Month" con el campo "Year" para asegurar que la fecha de vencimiento completa sea válida.

- Respetar idioma y formato local:

Mostrar los nombres de los meses en el idioma y formato local del usuario para mejorar la comprensión.

- Facilidad de uso:

Facilitar la selección del mes mediante el uso de controles intuitivos, como una lista desplegable o un selector de fechas.

- Compatibilidad con diferentes formatos de fecha:

Garantizar que el campo "Month" funcione correctamente con diferentes formatos de fecha utilizados en diferentes regiones.

- Validación en tiempo real:

Realizar validación en tiempo real mientras el usuario selecciona el mes, mostrando mensajes de error instantáneos si se elige un mes no válido.

- Mensajes de ayuda contextual:

Proporcionar mensajes de ayuda o descripciones contextuales que expliquen claramente cómo ingresar el mes y su importancia en el contexto de la tarjeta de crédito.

#### 6) Campo tipo date "Year":

- Campo obligatorio:

Si el campo "Year" se deja en blanco, se debe mostrar un mensaje de error indicando que el campo es obligatorio.

- Selección válida de año:

El campo "Year" debe permitir solo la selección de años válidos en el futuro.

- Presentación visual:

Presentar los años en un formato fácilmente comprensible, como una lista desplegable.

- Control de límites:

Verificar que el campo "Year" acepte únicamente valores dentro de un rango lógico, por ejemplo, no permitir años pasados.

- Validación de formato de entrada:

Validar que la entrada del usuario siga el formato correcto y proporcionar mensajes de error claros si se detectan problemas.

- Asociación con el mes de vencimiento:

Coordinar el campo "Year" con el campo "Month" para asegurar que la fecha de vencimiento completa sea válida.

- Facilidad de uso:

Facilitar la selección del año mediante el uso de controles intuitivos, como una lista desplegable o un selector de fechas.

- Validación en tiempo real:

Realizar validación en tiempo real mientras el usuario selecciona el año, mostrando mensajes de error instantáneos si se elige un año no válido.

- Compatibilidad con diferentes formatos de fecha:

Garantizar que el campo "Year" funcione correctamente con diferentes formatos de fecha utilizados en diferentes regiones.

- Mensajes de ayuda contextual:

Proporcionar mensajes de ayuda o descripciones contextuales que expliquen claramente cómo ingresar el año y su importancia en el contexto de la tarjeta de crédito.

- Seguridad en la transmisión:

Asegurarse de que la información del año de vencimiento se transmita de manera segura mediante el uso de protocolos de cifrado (por ejemplo, SSL/TLS).

7) Si se efectúa la compra mediante el botón "Purchase" con los datos requeridos en blanco debe mostrarse el siguiente alert:

www.demoblaze.com dice

Please fill out Name and Creditcard.

Aceptar

### **Sección de contacto (Contact):**

Al hacer clic en el botón Contact se deberá visualizar el siguiente Pop-Up:

New message



Contact Email:

Contact Name:

Message:

Close

Send message

1) Campo tipo Email "Contact Email":

- Campo obligatorio:

Si el campo "ContactEmail" se deja en blanco, se debe mostrar un mensaje de error indicando que el campo es obligatorio.

- Formato de dirección de correo electrónico:

Validar que la entrada en el campo "ContactEmail" siga un formato de dirección de correo electrónico válido.

- Longitud máxima:

Limitar la longitud del campo "ContactEmail" a un número específico de caracteres (por ejemplo, 320 caracteres, que es la longitud máxima permitida para direcciones de correo electrónico según las normas).

- Validación de dominio:

Verificar que el dominio del correo electrónico sea válido y exista.

- Validación de caracteres especiales:

Permitir caracteres especiales válidos en la parte local del correo electrónico (antes del símbolo '@') y en el dominio.

- Confirmación de dirección de correo electrónico:

Incluir un campo adicional para confirmar la dirección de correo electrónico y validar que coincida con la introducida anteriormente.

- Mensajes de error específicos:

Mostrar mensajes de error específicos en caso de que se introduzca una dirección de correo electrónico no válida o si las direcciones de correo electrónico no coinciden en el campo de confirmación.

- Autocompletado del navegador:

Desactivar la opción de autocompletado del navegador para el campo "ContactEmail" para evitar posibles errores.

- Caracteres permitidos:

Proporcionar una lista clara de los caracteres permitidos en el campo "ContactEmail".

- Enlace de ayuda:

Incluir un enlace o icono de ayuda que proporcione información sobre el formato esperado de la dirección de correo electrónico.

- Notificación de envío exitoso:

Después de enviar el formulario, mostrar una notificación visual o mensaje que confirme al usuario que la información ha sido enviada correctamente.

- Seguridad en la transmisión:

Asegurarse de que la información del correo electrónico de contacto se transmita de manera segura mediante el uso de protocolos de cifrado (por ejemplo, SSL/TLS).

## 2) Campo tipo Email "Contact Name":

- Campo obligatorio:

Si el campo "Contact Name" se deja en blanco, se debe mostrar un mensaje de error indicando que el campo es obligatorio.

- Longitud máxima:

Limitar la longitud del campo "Contact Name" a un número específico de caracteres (por ejemplo, 100 caracteres).

- Formato alfabético:

Permitir solo caracteres alfabéticos en el campo "Contact Name", evitando números u otros caracteres especiales.

- Validación de mayúsculas/minúsculas:

Aceptar tanto mayúsculas como minúsculas en el nombre y garantizar que la validación no sea sensible a mayúsculas.

- Espacios permitidos:

Permitir espacios en blanco en el nombre, para manejar nombres compuestos o con apellidos.

- Validación de caracteres especiales:

Limitar el uso de caracteres especiales en el campo, permitiendo solo aquellos que son comúnmente aceptados en nombres (por ejemplo, apóstrofes, guiones).

- Mensajes de error específicos:

Mostrar mensajes de error específicos si se introducen caracteres no permitidos o si la longitud máxima se ha superado.

- Autocompletado del navegador:

Desactivar la opción de autocompletado del navegador para el campo "Contact Name" para evitar posibles errores.

- Caracteres permitidos:

Proporcionar una lista clara de los caracteres permitidos en el campo "Contact Name".

- Enlace de ayuda:

Incluir un enlace o icono de ayuda que proporcione información sobre el formato esperado del nombre de contacto.

- Validación en tiempo real:

Realizar validación en tiempo real mientras el usuario completa el campo, mostrando mensajes de error instantáneos si se ingresan datos no válidos.

- Seguridad en la transmisión:

Asegurarse de que la información del nombre de contacto se transmita de manera segura mediante el uso de protocolos de cifrado (por ejemplo, SSL/TLS).

### 3) Campo tipo Text Área (Message):

- Campo obligatorio:

Si el campo "Message" se deja en blanco, se debe mostrar un mensaje de error indicando que el campo es obligatorio.

- Longitud máxima:

Limitar la longitud del campo "Message" a un número específico de caracteres (por ejemplo, 1000 caracteres).

- Caracteres permitidos:

Permitir una amplia variedad de caracteres en el campo "Message", incluyendo letras, números, espacios y caracteres especiales comunes.

- Validación de formato de entrada:

Validar que la entrada del usuario en el campo "Message" no contenga formato inseguro o código malicioso.

- Mensajes de error específicos:

Mostrar mensajes de error específicos si se ingresan caracteres no permitidos o si la longitud máxima se ha superado.

- Autocompletado del navegador:

Desactivar la opción de autocompletado del navegador para el campo "Message" para evitar posibles errores.

- Seguridad en la transmisión:

Asegurarse de que la información del mensaje se transmita de manera segura mediante el uso de protocolos de cifrado (por ejemplo, SSL/TLS).

- Permitir saltos de línea:

Permitir saltos de línea en el campo "Message" para que los usuarios puedan formatear su mensaje de manera legible.

- Control de spam:

Implementar medidas para prevenir el envío automático de mensajes spam, como un sistema de captcha o validación adicional.

- Validación en tiempo real:

Realizar validación en tiempo real mientras el usuario completa el campo, mostrando mensajes de error instantáneos si se ingresan datos no válidos.

- Caracteres permitidos:

Proporcionar una lista clara de los caracteres permitidos en el campo "Message".

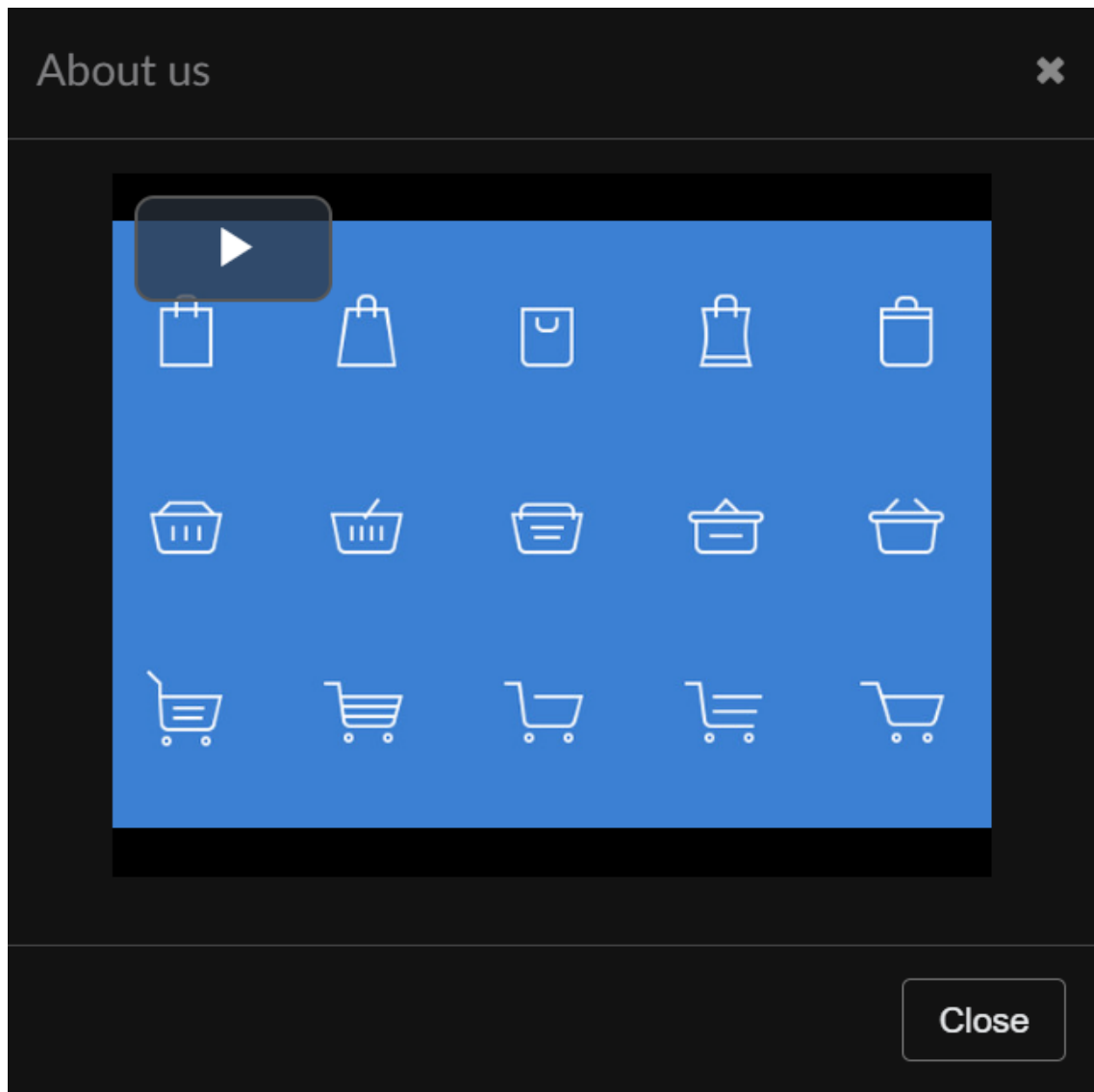
- Almacenamiento seguro:

Garantizar que los mensajes se almacenen de manera segura en la base de datos, protegiendo la privacidad y confidencialidad de la información.

- Si se envía el mensaje dejando los campos requeridos en blanco desde el botón "Send message", se debe mostrar un alert con el siguiente mensaje: "Los campos requeridos son obligatorios" y se debe marcar en rojo la fuente de los campos obligatorios.

### **Sección acerca de nosotros (About Us):**

Al hacer clic en el botón About us de la barra de navegación se debe mostrar un Pop-Up de la siguiente manera:



**Proyecto:** Sitio web de Ecommerce “Demoblaze.com”

**Fecha:** [ 18/11/2023 ]

**Tester:** [ Fabricio García ]