

**Te damos  
la bienvenida a  
Eventum**

**la plataforma de eventos de**



*Jorman Moncho Ramirez  
Alan Estruch Gomez*

## I. Resumen Ejecutivo

Eventum es una aplicación web desarrollada con el propósito de optimizar la gestión de eventos y formaciones en Marina de Empresas. Su enfoque principal es facilitar la planificación, organización, promoción y seguimiento de una amplia gama de eventos y actividades. Esta aplicación se ha diseñado con el objetivo de mejorar la eficiencia operativa y la comunicación tanto interna como externa, proporcionando a los usuarios las herramientas necesarias para ofrecer experiencias exitosas a los asistentes.

### Descripción del Proyecto

**Objetivos del Proyecto:** Los objetivos generales de Eventum son mejorar la gestión de eventos y formaciones en Marina de Empresas, optimizando la planificación, organización, promoción y seguimiento de actividades.

**Beneficios Clave:** aporta varios beneficios a Marina de Empresas. Entre ellos se encuentran la mejora de la experiencia del usuario, la optimización de la comunicación interna y externa, y un aumento en la eficiencia operativa al simplificar la gestión de eventos y formaciones. Estos beneficios se traducen en un mayor éxito de la organización y en una experiencia más satisfactoria para los usuarios.

### Identificación de Funciones Sensibles

1. **Gestión de Datos de Usuarios:** La aplicación almacena información personal y financiera de usuarios, lo que requiere una protección rigurosa.
2. **Procesamiento de Pagos:** La seguridad en el procesamiento de pagos, incluyendo datos de tarjetas de crédito, es esencial para evitar riesgos financieros y garantizar la confianza del usuario.
3. **Acceso a Datos Sensibles:** Se deben establecer permisos adecuados para garantizar que los usuarios solo accedan a datos que les corresponden.
4. **Comunicación Interna:** La comunicación interna debe ser segura y precisa para evitar fugas de información o malentendidos.
5. **Control de Aforo:** El control de aforo es crucial para eventos; su gestión deficiente podría llevar a problemas de seguridad y comodidad.
6. **Gestión de Feedback de Asistentes:** Los comentarios de los asistentes deben tratarse con respeto y privacidad.
7. **Difusión de Eventos:** La comunicación externa debe ser cuidadosa y precisa para proteger la imagen de la organización.
8. **Segmentación de Usuarios y Personalización:** La información sobre preferencias de usuarios debe manejarse respetando la privacidad y las regulaciones de protección de datos.
9. **Diferenciación de Perfiles:** Diferentes perfiles de usuario deben tener niveles de acceso y funcionalidades específicas adecuados.

### **Permisos y Accesos**

1. Control de acceso: Garantiza que solo las personas autorizadas accedan a información confidencial.
2. Principio de Mínimo privilegio: Cada usuario y sistema accede solo a recursos y datos necesarios para sus funciones específicas.

Para lograr una gestión efectiva, hemos definido una estructura jerárquica de roles, con la posibilidad de expandirla en el futuro:

#### **Base Jerárquica Actual:**

- I. Superadministrador
- II. Administrador
- III. Usuario

#### **Estructura Jerárquica Futura:**

1. Administrador (gestión completa)
2. Moderadores (moderación y gestión de contenido)
3. Organizador/es (gestión de eventos)
4. Logística (gestión de eventos y logística)
5. Aprobador/es (validación y aprobación)
6. Ponente/s (participación en eventos)
7. Público (usuarios asistentes)

Cada rol tiene sus respectivos permisos y responsabilidades:

- Administradores: Tienen control total sobre la aplicación, incluyendo la gestión de usuarios, contenido, configuración, análisis y seguridad.
- Moderadores: Se encargan de moderar y gestionar el contenido generado por usuarios, manteniendo un ambiente seguro y ordenado.
- Organizador/es: Son responsables de crear y gestionar eventos, interactuar con los participantes y coordinar actividades logísticas.
- Logística: Gestionan eventos y recursos logísticos, incluyendo la reserva de salas y coordinación de actividades relacionadas.
- Aprobador/es: Validan y aprueban contenido, solicitudes de acceso y modificaciones importantes.
- Ponente/s: Participan en eventos, compartiendo conocimientos y interactuando con la audiencia.
- Público: Son los asistentes a eventos, interactúan con contenido público y gestionan sus propios perfiles y preferencias.

### **Flujo de Datos**

En términos generales:

1. El tráfico del navegador del usuario pasa a través de Cloudflare, que actúa como un intermediario.
2. La comunicación está encriptada en SSL desde el navegador hasta el servidor de origen (una instancia EC2 en AWS) a través de Cloudflare.
3. El certificado SSL se genera y gestiona en Cloudflare.

Cloudflare también proporciona protección contra ataques DDoS.

4. La ruta completa sería: Navegador del usuario -> Cloudflare -> Vercel (frontend) -> Cloudflare -> AWS EC2 (backend) -> AWS RDS (base de datos).

### Análisis de Riesgos

1. Autenticación: Prevenir intentos de robo de contraseñas con bloqueo de cuentas y autenticación de dos factores.
2. Phishing: Enseñar a los usuarios a identificar correos de phishing y usar herramientas de detección.
3. Cuentas Falsas: Detectar cuentas falsas y limitar la creación de múltiples cuentas por usuario.
4. Robo de Sesión: Usar tokens seguros, cifrado HTTPS, y controlar sesiones activas.
5. Inyección de SQL: Evitar ataques SQL con consultas seguras y validación de datos.
6. Acceso Administrador: Implementar control de acceso y limitar funciones de administrador a usuarios autorizados.

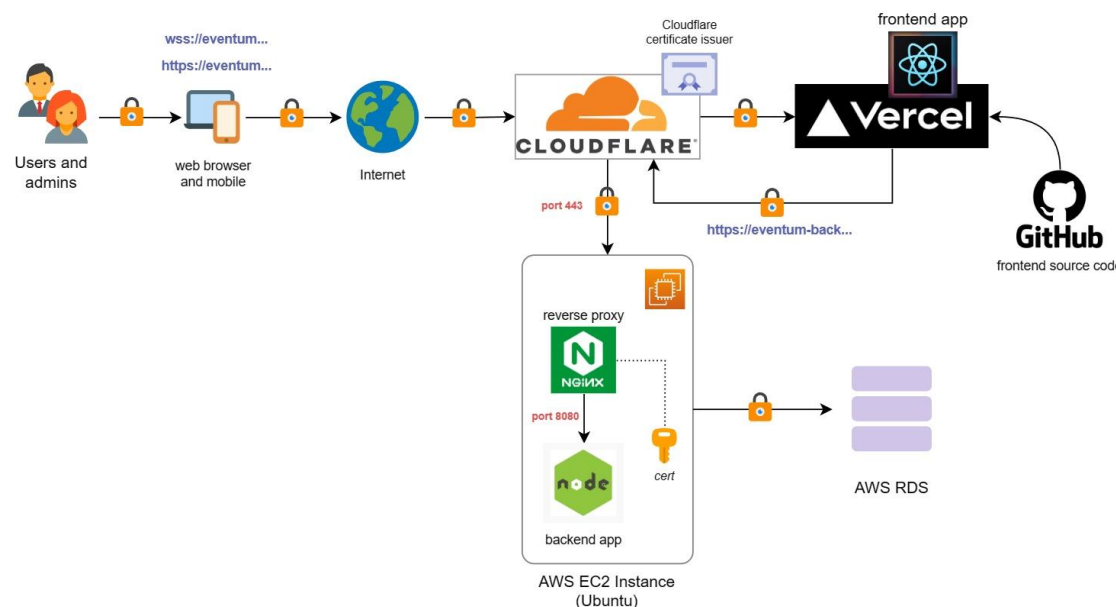
## II. Hardening de sistemas

Hardening de AWS EC2: Se han aplicado medidas de seguridad para fortalecer las instancias de EC2 en Amazon Web Services, incluyendo la restricción del acceso de red, actualizaciones regulares, y la gestión de permisos de acceso.

Hardening de AWS RDS: Se ha implementado seguridad adicional en el servicio de bases de datos de Amazon, incluyendo encriptación de datos, controles de acceso rigurosos y una política de copias de seguridad sólida.

Hardening de Vercel: Se han tomado medidas para mejorar la seguridad en la plataforma Vercel, incluyendo autenticación de dos factores, control de acceso y supervisión continua para detectar y mitigar posibles amenazas.

## III. Diseño de infraestructura



El usuario ingresa la URL en su navegador para acceder a la aplicación web.

- ✚ La solicitud del usuario primero pasa por los servidores de Cloudflare, donde se evalúa y procesa.
- ✚ Si la solicitud necesita contenido dinámico, Cloudflare la envía a los servidores de Vercel, que contienen el frontend de la aplicación, y Vercel genera la página web dinámica correspondiente.
- ✚ Después de eso, Cloudflare recibe la respuesta de Vercel y la somete a servicios adicionales de seguridad y optimización antes de enviarla de nuevo al usuario.
- ✚ Si la solicitud implica operaciones del lado del servidor, Cloudflare redirige la solicitud a los servidores de AWS EC2, donde se encuentra el backend de la aplicación. AWS EC2 procesa la solicitud y, si es necesario, interactúa con la base de datos AWS RDS para obtener datos dinámicos.
- ✚ Si se necesitan datos almacenados, el backend en AWS EC2 se comunica con la base de datos AWS RDS, que procesa las consultas y devuelve los datos solicitados al backend en EC2.
- ✚ El backend en EC2 combina los datos de la base de datos, si es necesario, con la respuesta generada previamente y la envía de vuelta a Cloudflare.
- ✚ Cloudflare recibe la respuesta final del backend en EC2 y la somete a sus servicios antes de enviarla de vuelta al navegador del usuario.
- ✚ Finalmente, el navegador del usuario recibe la respuesta final de Cloudflare, que puede incluir contenido dinámico y estático. El navegador renderiza la página web y permite al usuario interactuar con la aplicación.

#### **IV. Inventario Activos**

##### **Inventario de Herramientas Utilizadas:**

Se ha realizado un inventario de las herramientas que se han utilizado. Esto implica identificar y registrar todas las herramientas, software, hardware y recursos tecnológicos que son esenciales para el funcionamiento. Este inventario nos permite tener una visión clara de nuestros activos tecnológicos, su estado y su relevancia en nuestra operación. Además, nos ayuda a tomar decisiones informadas sobre actualizaciones, mantenimiento y adquisición de nuevas herramientas.

##### **Inventario de los Integrantes:**

También se ha llevado a cabo un inventario de nuestros integrantes del equipo. Sobre cada ordenador en el cual trabaja y su sistema operativo, su software y el antivirus que usan. Esto nos permite a llevar un seguimiento de cada uno.

#### **V. Backup**

Se ha optado por utilizar AWS Backup para gestionar sus copias de seguridad. AWS Backup es una solución confiable que le permite respaldar y proteger sus datos críticos en la nube de Amazon Web Services.

Es importante destacar que, si en el futuro la organización necesita aumentar su capacidad de almacenamiento para respaldos, esto conlleva un costo adicional. AWS ofrece escalabilidad, lo que significa que la organización puede aumentar la capacidad de respaldo según sus necesidades, pero debe estar preparada para pagar por el espacio adicional requerido.

En resumen, AWS Backup es la elección de la organización para respaldar sus datos en la nube de AWS, y debe ser consciente de que, si necesita más capacidad de almacenamiento en el futuro, esto implicará un costo adicional.

## **VI. Metodología**

Se ha optado por utilizar las metodologías ISO 27001 y OWASP Top 10 para asegurar la seguridad de su aplicación web. La ISO 27001 proporciona un enfoque integral para gestionar los riesgos de seguridad de la información en general, asegurando la protección de sus activos de datos. Por otro lado, OWASP Top 10 se enfoca en abordar las vulnerabilidades específicas más comunes en aplicaciones web, lo que permite proteger la aplicación contra las amenazas más relevantes y actuales. En conjunto, estas metodologías ayudan a la organización a desarrollar una aplicación web segura y confiable, mitigando riesgos y garantizando la integridad de los datos y la confidencialidad de la información para sus usuarios.

## **VII. Revisar los controles de seguridad**

Se ha fortalecido la seguridad de nuestra aplicación web configurando reglas en el WAF de AWS. Esto nos ayuda a detectar y bloquear amenazas en tiempo real. Sin embargo, si se necesita reglas adicionales, habrá un costo adicional. También se ha evaluado el AWS Shield Advanced para protección contra ataques DDoS avanzados, pero esto también implica costos extras. Estas medidas aumentan la seguridad, pero por el momento por falta de recursos no se han implementado todo.

## **VIII. Definir impacto técnico y de negocio**

A corto plazo, planeamos implementar CAPTCHA para mejorar la seguridad de nuestra aplicación web. Esto añadirá una capa de protección contra ataques automatizados. Sin embargo, debemos estar conscientes de que puede ralentizar ligeramente la velocidad de respuesta del servidor y requerir una configuración y gestión adicionales. Además, los costos pueden variar, especialmente si optamos por un servicio de terceros.

A largo plazo, tenemos la intención de implementar medidas de seguridad adicionales, como firewalls y protección contra ataques DDoS. Esto implicaría costos estimados mensuales de alrededor de \$250 para la base de datos, \$250 para opciones de firewall, y \$3,000 para la protección DDoS. También mantenemos un costo mensual de aproximadamente \$20 para el servidor web y \$2,400 anuales para la protección a través de Cloudflare, que ofrece seguridad adicional contra varios tipos de ataques web.

En resumen, se está tomando medidas para fortalecer la seguridad tanto a corto como a largo plazo, lo que puede implicar costos adicionales, pero es esencial para proteger nuestra aplicación web y mantener la integridad de nuestros servicios en línea.

## Precio de AWS RDS

Instancia de base de datos	989.88 USD
Almacenamiento	435.00 USD
IOPS provisionadas	1044.00 USD
<b>Total</b>	<b>2468.88 USD</b>

Esta estimación de facturación se basa en el uso bajo demanda, tal como se describe en [Precios de Amazon RDS](#). La estimación no incluye los costos de almacenamiento de copias de seguridad, operaciones de E/S (si proceden) ni transferencia de datos.

Realice una estimación de sus costos mensuales de la instancia de base de datos mediante la [Calculadora costo mensual AWS](#).

## Precio para mantener El Frontend

Most Popular

Pro

**\$20** per user / month

Everything in Hobby, plus higher limits and team features

✓

Unlimited Environments

✓

More Functions (Serverless, Edge)

✓

More Databases (KV, Postgres)

✓

More Web Analytics Events

✓

More Experimentation (Edge Config, Middleware)

+

Preview/Comment/Edit Deployments

+

Basic DDoS Mitigation

+

Email Support

Upgrade now

→

## IX. Pruebas de análisis estático de código

Se ha llevado a cabo un proceso de ejecución de pruebas utilizando herramientas de análisis estático de código con el fin de identificar posibles problemas en el código. Una vez que se detectaron estos problemas, se informó detalladamente al equipo de desarrollo full stack, el cual se encargó de abordar y solucionar cada uno de los inconvenientes identificados.

Con este trabajo se busca garantizar la calidad y la integridad de nuestro código fuente. Gracias a las herramientas de análisis estático de código nos permite realizar un análisis de nuestro proyecto en busca de vulnerabilidades, errores de programación que podrían afectar su rendimiento y seguridad.

## X. Pentesting


Se ha realizado una auditoría básica utilizando herramientas de pentesting. Este proceso implica la evaluación activa de nuestra infraestructura y sistemas para identificar posibles vulnerabilidades y puntos débiles en nuestra seguridad informática.

Esta auditoría nos permite:

- Identificar Vulnerabilidades: A través de pruebas controladas, hemos detectado posibles brechas de seguridad, como configuraciones incorrectas, deficiencias en el control de acceso o fallos en el software.
- Evaluar la Postura de Seguridad: se ha evaluado la efectividad de nuestras medidas de seguridad existentes esto permite identificar áreas que requieren mejoras.
- Prevenir Ataques: Al detectar vulnerabilidades antes de que sean explotadas por atacantes, podemos tomar medidas para prevenir ataques y proteger nuestros activos digitales.

### Resultado general:

Se ha escaneado la página en varias aplicaciones de evaluación de seguridad y nos ha dado un resultado B. Esta página califica de nivel máximo un S y de nivel mínimo una F, si pudiéramos implementar las opciones que son de pago podrías mejorar mucho este proyecto a nivel de seguridad.

 **Qualys** SSL Labs

Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > eventum-back.patgonzalez.me

**SSL Report: eventum-back.patgonzalez.me**

Assessed on: Tue, 26 Sep 2023 15:17:20 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	<a href="#">2606:4700:3033:0:0:0:ac43:baad</a> Ready	Tue, 26 Sep 2023 15:10:26 UTC Duration: 103.160 sec	<b>B</b>
2	<a href="#">2606:4700:3030:0:0:0:6815:409f</a> Ready	Tue, 26 Sep 2023 15:12:10 UTC Duration: 103.311 sec	<b>B</b>
3	<a href="#">104.21.64.159</a> Ready	Tue, 26 Sep 2023 15:13:53 UTC Duration: 104.96 sec	<b>B</b>
4	<a href="#">172.67.186.173</a> Ready	Tue, 26 Sep 2023 15:15:37 UTC Duration: 102.749 sec	<b>B</b>

SSL Report v2.2.0