

RBAC y Sistema de Solicitudes Técnicas como Estrategias de Seguridad y Eficiencia en Plataformas de Comercio Electrónico Multidominio

Yamarie Ruiz Serrano
Maestría en Ciencias de Computadoras
Mentor: Nelliud D. Torres Batista, DBA
Universidad Politécnica de Puerto Rico
Graduate Project EXPO, Febrero 2026

Abstracto — *El crecimiento de las plataformas de comercio electrónico ha incrementado la necesidad de contar con sistemas seguros y eficientes capaces de manejar múltiples dominios y un alto volumen de usuarios. Este trabajo presenta el diseño de un modelo integrado que combina un esquema de Control de Acceso Basado en Roles (RBAC) con un sistema de solicitudes técnicas orientado a la gestión de incidentes en entornos de comercio electrónico multidominio. Se adopta un enfoque de diseño aplicado basado en el análisis de requerimientos y la definición de una arquitectura modular, con el fin de proponer una solución escalable y alineada con principios de protección de datos y trazabilidad operativa. La integración de ambos mecanismos permite fortalecer la separación de privilegios y mejorar la comunicación entre usuarios y equipos de soporte, estableciendo flujos de trabajo formales que contribuyen a una gestión más eficiente y confiable de la plataforma.*

Palabras Claves — *Comercio Electrónico, Control de Acceso Basado en Roles, Seguridad de la Información, Sistemas de Solicitudes Técnicas.*

INTRODUCCIÓN

El comercio electrónico se ha convertido en una parte central de la economía digital, permitiendo a organizaciones de distintos tamaños ofrecer sus servicios a través de múltiples dominios y plataformas [1]. Este crecimiento ha aumentado la complejidad de los sistemas especialmente en la forma en que se gestionan los accesos y se atienden los incidentes técnicos.

En plataformas de comercio electrónico multidominio participan diferentes tipos de usuarios como clientes, personal administrativo de los dominios y administradores globales del sistema. Cada uno de estos perfiles necesita acceder a

funciones específicas del sistema. Cuando no existe un modelo claro para definir estos accesos incrementa el riesgo de accesos no autorizados y fallas operativas que pueden provocar incidentes de seguridad [2] [3].

De manera similar la atención de fallas y solicitudes técnicas requiere un proceso organizado, sin un sistema formal que permita registrar y dar seguimiento a los incidentes resulta difícil mantener la continuidad del servicio y documentar los eventos que afectan las operaciones diarias de la plataforma [1] [3].

Ante esta situación, este trabajo presenta el diseño de un modelo que integra tres componentes principales: un esquema de Control de Acceso Basado en Roles (RBAC) para los dominios gestionados, un esquema RBAC independiente para los administradores del sistema y un sistema de solicitudes técnicas para la gestión de solicitudes de soporte. El objetivo es proponer una arquitectura fácil de entender y aplicar que ayude a mejorar la seguridad y la eficiencia operativa en plataformas de comercio electrónico multidominio, manteniendo un equilibrio entre control de accesos y facilidad de gestión.

MARCO CONCEPTUAL Y REVISIÓN DE LITERATURA

El diseño de plataformas de comercio electrónico seguras y eficientes ha sido abordado desde múltiples perspectivas en la literatura académica y técnica. Entre los enfoques más relevantes se encuentran los modelos de control de acceso orientados a la protección de datos y los sistemas de gestión de soporte técnico, los cuales contribuyen a la optimización de los procesos operativos mediante la estructuración del manejo de solicitudes a través de arquitecturas modulares y

roles definidos que permiten crear, priorizar, asignar, actualizar y cerrar solicitudes de manera eficiente y con bajo costo de rendimiento, lo que agiliza la gestión, el seguimiento y la evolución del proceso de soporte [4]. Estos mecanismos responden a necesidades que se complementan dentro de los ecosistemas digitales en los que la seguridad y la continuidad del servicio se consideran elementos fundamentales.

Control de Acceso Basado en Roles en Comercio Electrónico

El Control de Acceso Basado en Roles se define como un modelo de autorización en el que los privilegios se asignan a roles en lugar de a usuarios individuales, permitiendo que los permisos se gestionen de manera centralizada y estructurada [2]. Este enfoque facilita la administración de sistemas complejos al establecer una relación clara entre funciones organizacionales y capacidades técnicas dentro de la plataforma.

En el contexto de este trabajo el modelo RBAC se aplica en dos niveles diferenciados. El primer nivel corresponde a los dominios de comercio electrónico, donde el personal operativo accede únicamente a las funciones asociadas a su rol dentro de cada dominio. El segundo nivel corresponde a los administradores del sistema, quienes cuentan con un esquema RBAC independiente que les permite gestionar entidades, permisos y configuraciones de forma global.

Diversos estudios destacan la relevancia de RBAC como mecanismo para reducir vulnerabilidades en entornos digitales. En arquitecturas de comercio electrónico la asignación de permisos permite limitar la exposición de componentes y asegurar que los usuarios interactúen únicamente con los recursos necesarios para desempeñar sus funciones [2] [3]. Este principio de separación de privilegios contribuye a minimizar el impacto de posibles incidentes de seguridad y a fortalecer la protección de la información sensible. En entornos de comercio electrónico basados en la nube, esta protección se vincula directamente con el cumplimiento de marcos regulatorios como el

Reglamento General de Protección de Datos (GDPR) y la *California Consumer Privacy Act* (CCPA), los cuales establecen requisitos sobre el acceso, tratamiento y resguardo de la información personal de los usuarios [5].

Ejemplos de implementación práctica en plataformas de comercio electrónico muestran que la diferenciación clara entre funciones administrativas y de clientes mejora la organización del sistema y reduce errores operativos en la gestión de productos y servicios [1].

Adicionalmente, la literatura resalta la relación entre RBAC y la escalabilidad de los sistemas. En plataformas que experimentan un crecimiento progresivo en el número de usuarios y dominios, la capacidad de definir nuevos roles y permisos de manera modular facilita la expansión de la infraestructura sin necesidad de rediseñar por completo el esquema de seguridad [1].

Sistemas de Solicitudes Técnicas en Plataformas Digitales

Los sistemas de solicitudes técnicas se consideran herramientas orientadas a la gestión estructurada de solicitudes de soporte, incidentes y requerimientos de servicio. Su función principal es centralizar la comunicación entre los usuarios y los equipos de soporte, estableciendo flujos de trabajo que permitan priorizar, asignar y dar seguimiento a cada caso de manera formal [3].

La literatura señala que este tipo de sistemas contribuye de manera significativa a la eficiencia operativa de las organizaciones, al disponer de un registro centralizado de incidentes los equipos pueden identificar patrones recurrentes, evaluar tiempos de respuesta y desarrollar estrategias de mejoras continuas basadas en datos históricos [4]. Esta trazabilidad también fortalece la transparencia en la relación con los usuarios, quienes pueden monitorear el estado de sus solicitudes y recibir retroalimentación sobre las acciones realizadas.

En entornos de comercio electrónico alojados en infraestructuras en la nube los sistemas de solicitudes técnicas adquieren una dimensión adicional relacionada con el cumplimiento

normativo. La documentación de las interacciones y los eventos técnicos facilita la generación de evidencias que pueden ser requeridas por marcos regulatorios asociados con la protección de datos y la gestión de servicios digitales [3].

Integración de Seguridad y Gestión Operativa

La unión entre los modelos de control de acceso y los sistemas de solicitudes técnicas refleja una tendencia hacia arquitecturas integradas que abordan los aspectos preventivos y reactivos de la gestión tecnológica [2] [3]. Mientras que RBAC actúa como un mecanismo orientado a la prevención de accesos indebidos, las solicitudes técnicas funcionan como una herramienta de respuesta estructurada ante incidentes y solicitudes.

METODOLOGÍA DE DISEÑO DEL SISTEMA

El desarrollo del modelo propuesto se basa en un enfoque práctico orientado al diseño de una arquitectura clara para plataformas de comercio electrónico multidominio. La metodología se organiza en cuatro etapas que permiten pasar de la identificación del problema a la definición de una solución técnica completa, siguiendo principios de diseño modular y escalabilidad propuestos en la literatura [1].

En la primera etapa se identifican los principales tipos de usuarios, los dominios del sistema y los recursos más importantes de la plataforma. Esto incluye la diferenciación entre usuarios de los dominios, personal administrativo de cada dominio y administradores globales del sistema. También se definen las relaciones entre usuarios y dominios, así como los puntos de control de acceso asociados a cada contexto [2].

La segunda etapa se enfoca en el diseño del modelo RBAC. En esta fase se definen dos esquemas diferenciados: uno para los roles asociados a los dominios y otro para los roles de los administradores globales. Para los dominios se definen entidades funcionales y acciones disponibles por dominio, además de la asignación de permisos a roles

mediante tablas intermedias. Para los administradores se define un conjunto independiente de entidades, acciones y permisos que permite gestionar de manera centralizada la configuración global del sistema [2].

En la tercera etapa se diseña el sistema de solicitudes técnicas. Aquí se establecen las estructuras para la creación de solicitudes, la asociación de cada solicitud con el usuario que lo genera y con el dominio al que pertenece, así como la definición de comentarios y archivos adjuntos vinculados al ciclo de vida de cada solicitud. Este diseño permite manejar tanto evidencias asociadas directamente a la solicitud como aquellas relacionadas con comentarios específicos dentro del flujo de soporte [3] [4].

Finalmente, en la cuarta etapa se integran ambos modelos en una sola arquitectura. Esta integración permite que la gestión de accesos y la atención de incidentes compartan una base lógica común, enfocada en la aplicación de reglas por rol y en el seguimiento estructurado de las solicitudes técnicas.

ARQUITECTURA PROPUESTA DEL SISTEMA

La arquitectura propuesta se organiza en una estructura modular compuesta por tres capas principales: presentación, lógica de negocio y gestión de datos, siguiendo principios de separación de responsabilidades y escalabilidad propuestos en arquitecturas de plataformas digitales [2] [1]. Esta separación permite mantener un bajo acoplamiento entre los componentes y facilita la expansión del sistema. La estructura general del sistema y la interacción entre las capas se ilustran en la Figura 1.

La capa de presentación incluye las interfaces utilizadas por los distintos perfiles de usuario como los administradores de cada dominio y los administradores globales del sistema. Cada interfaz se adapta dinámicamente en función del rol asignado, lo que garantiza que las funcionalidades visibles correspondan únicamente a los permisos autorizados.

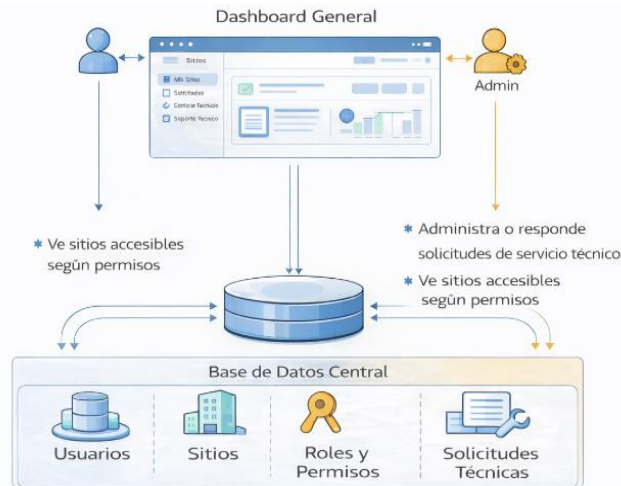


Figura 1

Diagrama de Arquitectura General del Sistema Integrado RBAC para Dominios, RBAC para Administradores y Solicitudes Técnicas

La capa de lógica de negocio integra los servicios de autenticación, autorización y gestión de solicitudes. En este nivel se procesan las solicitudes de acceso, se validan los roles y permisos de ambos esquemas RBAC y se ejecutan las reglas que determinan la creación, el enrutamiento y la actualización del estado de las solicitudes técnicas.

La capa de gestión de datos contiene las entidades relacionadas con usuarios y dominios existentes en la plataforma, así como las nuevas estructuras de roles, entidades y acciones tanto para los esquemas RBAC de dominio como para el esquema RBAC administrativo. Adicionalmente, almacena las tablas asociadas a las solicitudes técnicas, sus comentarios y los archivos adjuntos vinculados a cada etapa del flujo de soporte. Este repositorio centralizado permite mantener la consistencia de la información y soportar la operación del sistema.

MODELO DE DATOS Y CONTROL DE ACCESOS

El modelo de datos se basa en un conjunto de entidades interrelacionadas que representan los elementos fundamentales del sistema. Las tablas de usuarios y dominios se mantienen como estructuras existentes de la plataforma, mientras que el control de accesos se implementa a través de nuevas tablas

que definen roles, entidades y acciones tanto a nivel de dominio como a nivel administrativo [2] [3].

Para el esquema RBAC de dominio, cada usuario puede estar asociado a un rol dentro de un dominio específico. Los roles se vinculan con entidades funcionales disponibles en el dominio y con acciones permitidas sobre cada entidad mediante estructuras intermedias que permiten una asignación flexible y escalable.

Para el esquema RBAC administrativo, los administradores globales se asocian a roles independientes que definen permisos sobre un conjunto separado de entidades administrativas. Este enfoque permite gestionar la configuración global del sistema sin depender de los contextos particulares de cada dominio.

En el caso del sistema de solicitudes técnicas cada solicitud se vincula directamente con el usuario que la genera y con el dominio al que pertenece. Los comentarios asociados a una solicitud se relacionan con la solicitud principal y con el usuario que los crea. Los archivos adjuntos pueden asociarse tanto a la solicitud original como a comentarios específicos, permitiendo almacenar evidencias visuales o documentales en distintas etapas del flujo de soporte [3] [4].

Las relaciones entre roles, entidades y acciones se gestionan mediante tablas intermedias que incorporan indicadores de disponibilidad y

autorización. Esto permite controlar de manera dinámica qué operaciones están habilitadas para cada rol en función del contexto del dominio o del entorno administrativo.

ANÁLISIS Y DISCUSIÓN

El modelo propuesto mantiene una relación directa con los principios destacados en la literatura, especialmente en lo relacionado con la separación de privilegios y la organización modular de los sistemas de control de acceso, los cuales se reflejan en los diagramas entidad-relación del sistema de solicitudes técnicas (Figura 2), del esquema RBAC administrativo (Figura 3) y del esquema RBAC para los dominios (Figura 4) [2]. La inclusión del sistema de solicitudes técnicas como parte del diseño principal refuerza el enfoque operativo de la solución y permite establecer flujos de trabajo claros para la atención de solicitudes e incidentes [3].

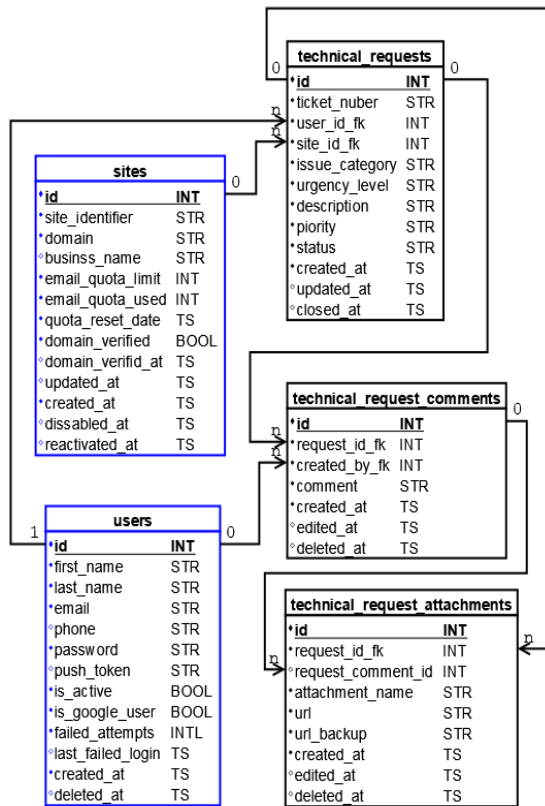


Figura 2

Diagrama Entidad-Relación del Modelo Integrado de Solicitudes Técnicas

En comparación con enfoques en los que la seguridad y el soporte técnico se manejan como módulos separados, la propuesta integrada ofrece una visión más completa de las interacciones del usuario con la plataforma a través de los roles y las solicitudes. Esto facilita el seguimiento de los incidentes y la gestión del soporte [4].

Sin embargo, el modelo también presenta algunos retos. En plataformas con muchos dominios y una gran cantidad de roles, la administración de permisos puede volverse más compleja y requerir herramientas adicionales para automatizar tareas y evitar inconsistencias en la configuración del sistema, tal como se señala en estudios sobre escalabilidad en arquitecturas de comercio electrónico [1].

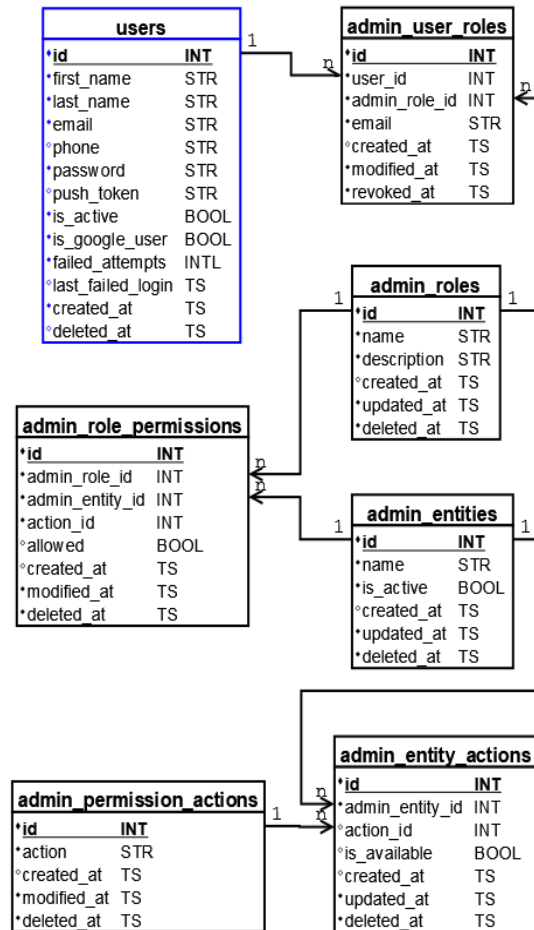


Figura 3

Diagrama Entidad-Relación del Modelo Integrado RBAC para Administradores

- e-commerce system,” *International Journal of Electrical and Computer Engineering*, 2022, vol. 12, no. 1, pp. 560.
- [3] P. Patel, “A Web-Based Ticketing System: Improving IT Support Efficiency and Employee Productivity,” 2025.
 - [4] J. Wiratama and F. A. T. Tobing, “Analysis and Design of a Web-Based Ticketing Service Helpdesk at Food and Packaging Machinery Company,” *Ultima InfoSys: Jurnal Ilmu Sistem Informatika*, 2022, vol. 13, no. 1, pp. 19–28.
 - [5] M. Pun, “Ensuring Data Privacy and Compliance in Cloud-Based E-Commerce: Strategies for Secure Platform Design,” 2024.