**Lógica de Negocio**

# Lógica de Negocio - Sistema de Gestión de Riesgos de Conectividad (SDGDRDC)

## Descripción General

La lógica de negocio del Sistema de Gestión de Riesgos de Conectividad (SDGDRDC) define las reglas, procesos y módulos que rigen la gestión de vulnerabilidades en la conectividad de redes. Este documento describe el estado actual, las reglas propuestas y la estructura para su implementación.

## Estado Actual

Actualmente, la lógica implementada incluye:

- \*\*Validación de Datos\*\*: Verifica que los campos obligatorios (`id\_protocolo`, `id\_criticidad`, `id\_estado`, `descripcion`, `fecha\_identificacion`) estén presentes y que los IDs referenciados existan en las tablas relacionadas.

- \*\*Gestión de Vulnerabilidades\*\*: Soporta creación, actualización y eliminación de vulnerabilidades a través de APIs REST.

- \*\*Autenticación\*\*: Utiliza JWT para restringir acceso a operaciones sensibles.

## Reglas de Negocio Propuestas

Las siguientes reglas se proponen para mejorar la gestión de riesgos:

### Transiciones de Estado

- De "Identificada" a "En análisis": Requiere asignar un `responsable`.

- De "En análisis" a "En remediación": Solo si la `criticidad` es "Media" o superior.

- De "En remediación" a "Resuelta": Requiere que hayan pasado más de 30 días desde `fecha\_identificacion`.

- De "Resuelta" a "Cerrada": Automático si no hay cambios en 7 días.

- Transiciones de retroceso (por ejemplo, "En remediación" a "En análisis") permitidas con justificación.