**Análisis de requerimientos**

**Corporación Universitaria Minuto de Dios – UNIMINUTO**

**Ingeniería de Sistemas**

**Practica Profesional**

**Jhon Daniel Ortiz Martínez**

**ID:** 865416

**NRC:** 45-67827

Tabla de Contenido

[1. INTRODUCCIÓN 3](#_Toc203998616)

[1.1. Propósito del Documento 3](#_Toc203998617)

[1.2. Contexto del Problema 3](#_Toc203998618)

[1.3. Objetivos del Sistema 3](#_Toc203998619)

[2. ALCANCE DEL PROYECTO 3](#_Toc203998620)

[2.1. Dentro del Alcance 3](#_Toc203998621)

[2.2. Fuera del Alcance 4](#_Toc203998622)

[3. STAKEHOLDERS 4](#_Toc203998623)

[4. REQUERIMIENTOS FUNCIONALES 4](#_Toc203998624)

[4.1. Módulo de Gestión de Vulnerabilidades 4](#_Toc203998625)

[4.2. Módulo de Clasificación 5](#_Toc203998626)

[4.3. Módulo de Seguimiento 6](#_Toc203998627)

[4.4. Módulo de Reportes 6](#_Toc203998628)

[4.5. Base de Conocimiento 7](#_Toc203998629)

[4.6. Dashboard y Métricas 7](#_Toc203998630)

[5. REQUERIMIENTOS NO FUNCIONALES 8](#_Toc203998631)

[5.1. Rendimiento 8](#_Toc203998632)

[5.2. Usabilidad 8](#_Toc203998633)

[5.3. Seguridad 9](#_Toc203998634)

[5.4. Confiabilidad 9](#_Toc203998635)

[5.5. Compatibilidad 9](#_Toc203998636)

[6. CASOS DE USO 10](#_Toc203998637)

[6.1. CU001 - Registrar Nueva Vulnerabilidad 10](#_Toc203998638)

[6.2. CU002 - Consultar Vulnerabilidades 10](#_Toc203998639)

[6.3. CU003 - Generar Reporte 10](#_Toc203998640)

[6.4. CU004 - Actualizar Estado de Vulnerabilidad 10](#_Toc203998641)

# INTRODUCCIÓN

## Propósito del Documento

Este documento establece los requerimientos funcionales y no funcionales para el desarrollo del Sistema de Gestión de Riesgos de Conectividad (SDGDRDC) del Banco Agrario de Colombia.

## Contexto del Problema

El Banco Agrario presenta las siguientes problemáticas en la gestión de vulnerabilidades:

* Falta de automatización en detección y reporte de vulnerabilidades.
* Ausencia de documentación estandarizada.
* Necesidad de centralización de información.
* Tiempo de identificación variado dependiendo de factores como la herramienta a utilizar, el alcance del escaneo, el tipo de vulnerabilidad, la frecuencia de la actualización de firmas y experiencia del analista, pero por lo general puede demorar entre 1 o 2 días y como mucho una semana.
* Falta de trazabilidad en remediación.

## Objetivos del Sistema

* Centralizar la gestión de vulnerabilidades SMB, TLS y SSL.
* Automatizar procesos de identificación y documentación.
* Mejorar trazabilidad y seguimiento.
* Generar reportes automatizados.

# ALCANCE DEL PROYECTO

## Dentro del Alcance

* Gestión de vulnerabilidades SMB, TLS y SSL.
* Sistema de clasificación por criticidad.
* Módulo de seguimiento y trazabilidad.
* Generación de reportes automáticos.
* Base de conocimiento de remediación.
* Dashboard con métricas básicas.

## Fuera del Alcance

* Integración con herramientas de escaneo automático.
* Gestión de otros protocolos diferentes a SMB/TLS/SSL.
* Módulo de notificaciones por email/SMS.
* Integración con Active Directory.

# STAKEHOLDERS

|  |  |  |
| --- | --- | --- |
| **Rol** | **Nombre** | **Responsabilidad** |
| **Usuario Final** | Analistas de Seguridad. | Uso diario del sistema. |
| **Usuario Supervisor** | Walter Oswaldo Mora Javela. | Supervisión y reportes. |
| **Desarrollador** | Jhon Daniel Ortiz Martinez. | Desarrollo y documentación. |
| **Docente Supervisor** | Julio Eduardo Valenzuela Díaz. | Seguimiento académico. |

# REQUERIMIENTOS FUNCIONALES

## Módulo de Gestión de Vulnerabilidades

**RF001 - Registrar Vulnerabilidad**

* **Descripción:** El sistema debe permitir registrar nuevas vulnerabilidades.
* **Campos obligatorios:**
  + ID único de vulnerabilidad.
  + Descripción detallada.
  + Protocolo afectado (SMB/TLS/SSL).
  + Nivel de criticidad (Crítica/Alta/Media/Baja).
  + Fecha de descubrimiento.
  + Fuente de detección.
  + Sistema/servidor afectado.
* **Validaciones:**
* ID único en el sistema.
* Campos obligatorios completos.
* Formato de fecha válido.

**RF002 - Consultar Vulnerabilidades**

* **Descripción:** Permitir búsqueda y consulta de vulnerabilidades.
* **Filtros disponibles:**
  + Por protocolo.
  + Por criticidad.
  + Por estado.
  + Por rango de fechas.
  + Por responsable asignado.
* **Resultados:** Lista paginada con opciones de ordenamiento.

**RF003 - Actualizar Vulnerabilidad**

* **Descripción:** Modificar información de vulnerabilidades existentes.
* **Campos editables:** Estado, responsable, comentarios, fecha de remediación.
* **Restricciones:** Solo usuarios autorizados pueden editar.

**RF004 - Eliminar Vulnerabilidad**

* **Descripción:** Eliminación lógica de vulnerabilidades.
* **Restricciones:** Solo administradores, mantener historial.

## Módulo de Clasificación

**RF005 - Clasificar por Criticidad**

* **Niveles:** Crítica, Alta, Media, Baja.
* **Criterios automáticos:** Basado en protocolo y tipo de vulnerabilidad.
* **Clasificación manual:** Opción de override por usuarios autorizados.

**RF006 - Gestión de Estados**

* **Estados disponibles:**
  + Pendiente.
  + En Proceso.
  + Remediada.
  + Cerrada.
  + Reabierta.
* **Transiciones permitidas:** Validar flujo de estados lógico.

## Módulo de Seguimiento

**RF007 - Asignar Responsables**

* **Funcionalidad:** Asignar vulnerabilidades a usuarios específicos.
* **Notificación:** Registro de asignación en historial.

**RF008 - Historial de Cambios**

* **Registro:** Todos los cambios con timestamp y usuario.
* **Información:** Qué cambió, quién lo cambió, cuándo.

**RF009 - Comentarios y Observaciones**

* **Funcionalidad:** Agregar comentarios a vulnerabilidades.
* **Formato:** Texto libre con fecha y autor.

## Módulo de Reportes

**RF010 - Reporte por Protocolo**

* **Contenido:** Vulnerabilidades agrupadas por SMB/TLS/SSL.
* **Formatos:** PDF, Excel.
* **Filtros:** Período, estado, criticidad.

**RF011 - Reporte por Criticidad**

* **Contenido:** Distribución y detalle por nivel de criticidad.
* **Gráficos:** Incluir visualizaciones.

**RF012 - Reporte Ejecutivo**

* **Contenido:** Métricas resumen para gerencia.
* **Frecuencia:** Configurable (semanal/mensual).

**RF013 - Exportar Datos**

* **Formatos:** CSV, Excel, PDF.
* **Contenido:** Datos filtrados según criterios del usuario.

## Base de Conocimiento

**RF014 - Gestionar Procedimientos**

* **Contenido:** Procedimientos de remediación por tipo de vulnerabilidad.
* **Organización:** Por protocolo y tipo.

**RF015 - Búsqueda de Conocimiento**

* **Funcionalidad:** Búsqueda por palabras clave.
* **Resultados:** Lista con relevancia.

**RF016 - Referencias Externas**

* **Integración:** Enlaces a CVE, NIST, otras fuentes.
* **Validación:** Verificar enlaces activos.

## Dashboard y Métricas

**RF017 - Dashboard Principal**

* **Métricas principales:**
* Total de vulnerabilidades activas.
* Distribución por criticidad.
* Distribución por protocolo.
* Tendencia mensual.
* Tiempo promedio de remediación.

**RF018 - Gráficos Interactivos**

* **Tipos:** Barras, líneas, tortas.
* **Interactividad:** Filtros en tiempo real.

# REQUERIMIENTOS NO FUNCIONALES

## Rendimiento

**RNF001 - Tiempo de Respuesta**

* **Criterio:** ≤ 3 segundos para operaciones normales.
* **Medición:** 95% de las transacciones.

**RNF002 – Concurrencia**

* **Criterio:** Soporte mínimo para 100 usuarios concurrentes.
* **Degradación:** Graceful degradation bajo carga.

**RNF003 – Capacidad**

* **Criterio:** Base de datos para 10,000+ vulnerabilidades.
* **Escalabilidad:** Arquitectura escalable.

## Usabilidad

**RNF004 - Interfaz Responsive**

* **Dispositivos:** Desktop, tablet, móvil.
* **Resoluciones:** Desde 320px hasta 1920px+.

**RNF005 - Navegación Intuitiva**

* **Criterio:** Usuario nuevo debe completar tareas básicas en < 10 minutos.
* **Validación:** Pruebas de usabilidad.

**RNF006 – Accesibilidad**

* **Estándar:** WCAG 2.1 nivel AA mínimo.
* **Validación:** Herramientas de evaluación automática.

## Seguridad

**RNF007 – Autenticación**

* **Método:** Usuario y contraseña.
* **Políticas:** Contraseñas seguras, expiración.

**RNF008 – Autorización**

* **Roles:** Administrador, Supervisor, Analista.
* **Permisos:** Basado en roles (RBAC).

**RNF009 – Auditoría**

* **Registro:** Todas las acciones críticas.
* **Información:** Usuario, acción, timestamp, IP.

**RNF010 - Protección de Datos**

* **Cifrado:** Datos sensibles en base de datos.
* **Comunicación:** HTTPS obligatorio.

## Confiabilidad

**RNF011 – Disponibilidad**

* **Meta:** 99% de tiempo operativo durante horario laboral.
* **Medición:** Monitoreo continuo.

**RNF012 – Recuperación**

* **Backup:** Respaldo diario automático.
* **RTO:** Recovery Time Objective < 4 horas.

## Compatibilidad

**RNF013 – Navegadores**

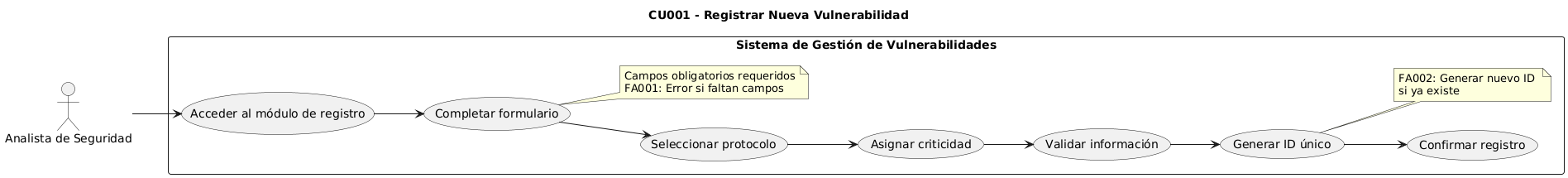
* **Soporte:** Chrome 90+, Firefox 85+, Safari 14+, Edge 90+.
* **Funcionalidad:** 100% en navegadores soportados.

**RNF014 – Integración**

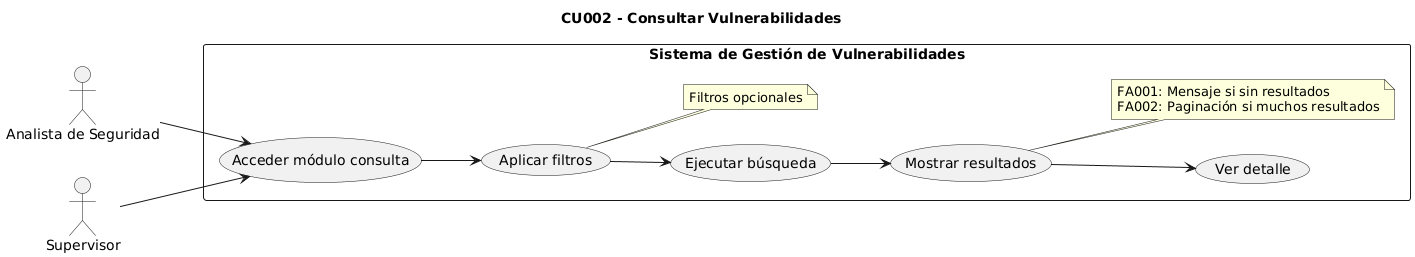
* **APIs:** REST para futuras integraciones.
* **Formato:** JSON para intercambio de datos.

# CASOS DE USO

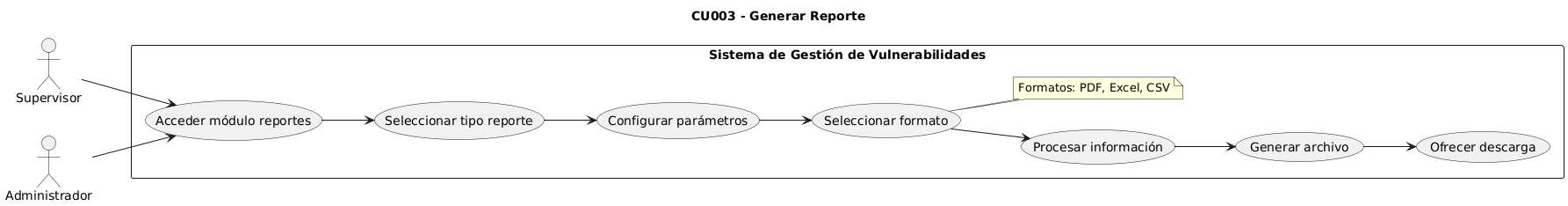
## CU001 - Registrar Nueva Vulnerabilidad



## CU002 - Consultar Vulnerabilidades



## CU003 - Generar Reporte



## CU004 - Actualizar Estado de Vulnerabilidad

