**ÍNDICE**

[1. INTRODUCCIÓN 3](#_Toc200403166)

[2. ANTECEDENTES 3](#_Toc200403167)

[2.1. INTERNACIONAL 3](#_Toc200403168)

[2.2. NACIONAL 3](#_Toc200403169)

[2.3. LOCAL 4](#_Toc200403170)

[3. IDENTIFICACIÓN DEL PROBLEMA 4](#_Toc200403171)

[4. FORMULACIÓN DEL PROBLEMA 4](#_Toc200403172)

[5. OBJETIVOS 5](#_Toc200403173)

[5.1. OBJETIVO GENERAL 5](#_Toc200403174)

[5.2. OBJETIVOS ESPECÍFICOS 5](#_Toc200403175)

[6. JUSTIFICACIÓN 5](#_Toc200403176)

[6.1. JUSTIFICACIÓN SOCIAL 5](#_Toc200403177)

[6.2. JUSTIFICACIÓN ECONÓMICA 6](#_Toc200403178)

[6.3. JUSTIFICACIÓN TÉCNICA 6](#_Toc200403179)

[7. LÍMITES Y ALCANCES 7](#_Toc200403180)

[7.1. LÍMITES 7](#_Toc200403181)

[7.2. ALCANCES 7](#_Toc200403182)

[8. MARCO TEORICO 8](#_Toc200403183)

[9. DESARROLLO DEL SISTEMA 10](#_Toc200403184)

[9.1. ANALISIS DE PROCESOS 10](#_Toc200403185)

[9.1.1. Identificacion Del Area Estudiada 10](#_Toc200403186)

[9.1.2. Diagrama De Procesos 10](#_Toc200403187)

[9.2. DESCRIPCION DEL SISTEMA 11](#_Toc200403188)

[9.2.1. Perspectiva Del Producto 11](#_Toc200403189)

[9.2.2. Funciones Del Producto 11](#_Toc200403190)

[9.2.3. Características Del Usuario 11](#_Toc200403191)

[9.2.4. Restricciones 11](#_Toc200403192)

[9.3. REQUERIMIENTOS DE SOFTWARE 12](#_Toc200403193)

[9.3.1. Historias De Usuario 12](#_Toc200403194)

[9.3.2. Requerimientos Funcionales 17](#_Toc200403195)

[9.3.3. Requerimientos No Funcionales 18](#_Toc200403196)

[9.3.4. Interfaces Externas 18](#_Toc200403197)

[9.4. DISEÑO DEL SISTEMA 18](#_Toc200403198)

[9.4.1. Arquitectura del Sistema (Modelo MVC) 18](#_Toc200403199)

[9.4.2. Diagrama de Casos de Uso 18](#_Toc200403200)

[9.4.3. Diagrama de Secuencia 18](#_Toc200403201)

[9.4.4. Diagrama de Clases 19](#_Toc200403202)

[9.4.5. Diseño de la Base de Datos 20](#_Toc200403203)

[9.5. DESARROLLO DE SISTEMA WEB 21](#_Toc200403204)

[9.5.1. Módulo de Gestión de Documentos 21](#_Toc200403205)

[9.6. COSTO DEL SISTEMA 25](#_Toc200403206)

[9.6.1. Supuestos Del Sistema 25](#_Toc200403207)

[9.6.2. Fórmula de Esfuerzo Básica de COCOMO II 25](#_Toc200403208)

[9.6.3. Tiempo Estimado de Desarrollo (Duración 26](#_Toc200403209)

[9.6.4. Costo Estimado Total 26](#_Toc200403210)

[9.6.5. Resumen 26](#_Toc200403211)

[10. CONCLUSIONES Y RECOMENDACIONES 27](#_Toc200403212)

[11. REFERENCIA BIBLIOGRÁFICA 28](#_Toc200403213)

[ANEXOS 29](#_Toc200403214)

# INTRODUCCIÓN

En el contexto de las instituciones militares, la gestión de información clasificada representa un aspecto crítico para garantizar la seguridad nacional y la integridad de las operaciones internas. La creciente digitalización de los procesos ha incrementado la necesidad de sistemas informáticos especializados que aseguren un control estricto, trazabilidad, confidencialidad y disponibilidad de los documentos sensibles. En respuesta a esta necesidad, se plantea el desarrollo del sistema **SEGEDOC-MILITAR**, una solución tecnológica diseñada específicamente para la gestión segura de documentos clasificados en entidades militares bolivianas. Este sistema busca establecer un control jerárquico sobre los accesos, integrar auditorías rigurosas de las acciones realizadas y asegurar el resguardo de los datos conforme a estándares de seguridad militar.

# ANTECEDENTES

En el contexto actual, tanto a nivel internacional como nacional, las fuerzas armadas y otras instituciones estratégicas requieren herramientas tecnológicas avanzadas que permitan gestionar documentos confidenciales sin poner en riesgo la seguridad institucional. A continuación, se detallan tres proyectos relacionados al sistema SEGEDOC-MILITAR:

## INTERNACIONAL

**Sistema SIPRNet (Secret Internet Protocol Router Network)** **–** **Estados Unidos**

Es una red clasificada utilizada por el Departamento de Defensa de los Estados Unidos para el manejo seguro de información secreta. Permite el acceso a documentos militares de alto nivel, protegidos mediante cifrado y segmentación de acceso por rango. Este sistema establece un precedente de alto nivel en cuanto a control de accesos y trazabilidad militar.

## NACIONAL

**Sistema de Gestión Documental del Ministerio de Defensa de Bolivia**

Es una plataforma nacional utilizada para el registro y gestión de documentos oficiales dentro del Ministerio de Defensa. Si bien cumple funciones de digitalización y archivo, carece de mecanismos avanzados de auditoría, clasificación militar y jerarquización de permisos según niveles de seguridad. SEGEDOC-MILITAR amplía y mejora esta idea, incorporando medidas de clasificación militar, jerarquía y confidencialidad reforzada.

## LOCAL

**Sistema Interno de Gestión de Documentos del Regimiento 1ro de Infantería (El Alto)**

Sistema interno básico utilizado para almacenar documentación administrativa y operativa. Opera de manera limitada mediante carpetas compartidas en red, sin control de accesos, cifrado ni registro de actividades, generando riesgos de filtración o manipulación de información crítica.

# IDENTIFICACIÓN DEL PROBLEMA

En las instituciones militares de Bolivia, la gestión de documentos clasificados presenta múltiples deficiencias que afectan la seguridad, confidencialidad y eficiencia del manejo de información sensible. Los principales problemas identificados son los siguientes:

a) La gestión documental se realiza en gran medida mediante medios físicos o sistemas informáticos genéricos que no contemplan mecanismos específicos de control jerárquico.

b) No existe trazabilidad ni registro detallado de las acciones ejecutadas sobre documentos clasificados, lo cual impide identificar responsables en casos de filtración o manipulación.

c) La validación de la integridad documental no está contemplada, lo que expone los archivos a modificaciones sin detección.

d) La falta de autenticación sólida y cifrado adecuado incrementa los riesgos de accesos no autorizados, pérdidas de datos y uso indebido de la información.

e) No se cuenta con una infraestructura tecnológica adaptada a la estructura de mando militar ni a los requerimientos de seguridad institucional.

Estas carencias representan una amenaza para la seguridad nacional y limitan la capacidad operativa y estratégica de las instituciones militares.

# FORMULACIÓN DEL PROBLEMA

¿La gestión de documentos clasificados para garantizar la confidencialidad, integridad y trazabilidad dentro de instituciones militares puede lograrse mediante el diseño e implementación de un sistema digital jerarquizado que refuerce la seguridad institucional del Estado?

# OBJETIVOS

## OBJETIVO GENERAL

Diseñar e implementar un sistema informático militar de gestión de documentos clasificados que refuerce la seguridad institucional del sistema académico militar, mediante la definición de jerarquías de acceso, el registro controlado de usuarios, la trazabilidad de acciones y el aseguramiento de la integridad de la información almacenada.

## OBJETIVOS ESPECÍFICOS

Analizar el proceso de gestión de documentos clasificados.

Desarrollar un módulo de registro de documentos.

Implementar un módulo de clasificación de documentos con niveles de acceso.

Desarrollar un módulo de reportes que permita generar informes sobre accesos, descargas, movimientos y uso del sistema por parte de los usuarios registrados.

# JUSTIFICACIÓN

## JUSTIFICACIÓN SOCIAL

El sistema SEGEDOC-MILITAR busca fortalecer la gestión segura y eficiente de documentos clasificados en las instituciones militares bolivianas. Su implementación aportará beneficios directos a:

Personal militar: Al garantizar que solo el personal autorizado pueda acceder a información clasificada según su jerarquía y funciones.

Instituciones castrenses: Mejorará la transparencia, la rendición de cuentas y la organización estructural de la documentación sensible.

Sociedad boliviana: Al reducir riesgos de filtración y proteger información estratégica del Estado, se contribuye a la estabilidad institucional y a la seguridad nacional.

## JUSTIFICACIÓN ECONÓMICA

Actualmente, el uso de archivos físicos y procesos manuales implica altos costos de almacenamiento, riesgo de pérdida de documentos, errores humanos y demoras operativas. La digitalización y automatización mediante SEGEDOC-MILITAR permitirá:

Disminución significativa de costos operativos en almacenamiento, papel y procesos administrativos.

Mayor eficiencia en la gestión de documentos, accesos y respuestas ante auditorías.

Reducción de riesgos y costos asociados a la filtración, pérdida o alteración de información crítica.

## JUSTIFICACIÓN TÉCNICA

El desarrollo de SEGEDOC-MILITAR se sustenta en tecnologías modernas, escalables y orientadas a la seguridad militar:

FastAPI (Backend): Framework robusto, con soporte para autenticación, control de accesos, y protección contra vulnerabilidades comunes.

PostgreSQL (Base de Datos): Estable, confiable y seguro, con soporte para control de accesos, transacciones y alta concurrencia.

Frontend (HTML, CSS, JavaScript con Tailwind o React): Flexible y compatible con interfaces modernas y accesibles desde navegadores seguros.

**Seguridad:**

Cifrado de contraseñas (bcrypt)

Hash de integridad documental (SHA-256)

Autenticación de usuarios y control de sesiones

Estas herramientas aseguran el cumplimiento de los estándares de calidad, eficiencia y protección de datos necesarios en un entorno militar.

# LÍMITES Y ALCANCES

## LÍMITES

El sistema SIGEDOC-MILITAR estará orientado exclusivamente a instituciones militares dentro del territorio boliviano. No contempla su uso en organizaciones civiles, educativas ni en el sector privado. Su alcance se limita a la gestión segura de documentación clasificada, control de accesos por jerarquía, monitoreo de sesiones y trazabilidad de acciones sobre documentos digitales. No incluye procesamiento de imágenes, escaneo de documentos físicos ni integración con sistemas externos.

## ALCANCES

El sistema cubrirá los siguientes módulos funcionales:

1. Módulo de Gestión de Usuarios:

* Registro y autenticación de usuarios militares.
* Asignación de roles jerárquicos según grado militar.
* Control de sesiones (fecha, hora e IP de acceso y cierre).

1. Módulo de Gestión de Roles y Permisos:

* Definición de jerarquías y permisos sobre documentos clasificados.
* Niveles de acceso (A, B, C, D) por tipo de usuario y contenido.

1. Módulo de Documentos Clasificados:

* Subida, edición, consulta y descarga de documentos
* Clasificación según nivel de confidencialidad
* Verificación de integridad con hash SHA-256

1. Módulo de Auditoría

* Registro de acciones realizadas (lectura, edición, eliminación).
* Seguimiento individual por usuario y documento.

1. Módulo de Unidades Militares:

* Organización por divisiones, regimientos o áreas militares.
* Asignación de documentos y accesos por unidad.

1. Módulo de Estados de Usuarios y Documentos:

* Control de disponibilidad (activos/inactivos).
* Gestión de vigencia y restricciones de acceso.

1. Módulo de Seguridad:

* Cifrado de contraseñas con bcrypt.
* Validación de acceso y política de autenticación.
* Protección contra accesos no autorizados.

1. Módulo de Reportes:

* Generación de informes por actividad de usuario.
* Descargas, accesos y cambios en documentos.
* Exportación en formato digital para revisión institucional.

# MARCO TEORICO

La gestión documental en entornos militares exige un tratamiento riguroso de la información, tanto en el almacenamiento como en la transmisión, debido a la naturaleza clasificada y estratégica de los contenidos. En este sentido, el sistema SIGEDOC-MILITAR busca responder a las necesidades específicas del Ejército de Bolivia, mediante la implementación de una plataforma informática moderna, jerarquizada y segura, que permita gestionar documentos reservados, secretos y ultrasecretos conforme a los niveles de autorización del personal militar.

Para el desarrollo del sistema se utilizarán herramientas tecnológicas actuales, enfocadas en rendimiento, seguridad y mantenibilidad. En el lado del cliente (frontend), se empleará la biblioteca React, que permite construir interfaces dinámicas, modulares y altamente reactivas. React facilita la actualización automática del contenido visual mediante su modelo virtual DOM, permitiendo una experiencia de usuario eficiente, incluso cuando se manejan múltiples módulos como gestión de usuarios, auditoría y reportes.

Para el servidor (backend), se utilizará FastAPI, un framework moderno basado en Python que permite el desarrollo de APIs REST de alto rendimiento. FastAPI destaca por su facilidad de documentación automática, tipado fuerte y validación de datos, lo que permite construir servicios seguros y robustos, ideales para entornos sensibles como el militar. Además, al ser asincrónico y basado en estándares modernos como OpenAPI y JSON Schema, facilita la escalabilidad del sistema.

La base de datos seleccionada es PostgreSQL, un sistema de gestión de base de datos relacional de código abierto, altamente confiable, con soporte para consultas complejas, control de transacciones, funciones avanzadas de seguridad, cifrado y manejo de grandes volúmenes de información. PostgreSQL es idóneo para almacenar registros jerárquicos de usuarios, acciones de auditoría, documentos clasificados con hash y registros de sesión.

Las principales funcionalidades del sistema SIGEDOC-MILITAR incluyen:

* Módulo de Gestión de Usuarios: permite registrar personal militar con jerarquías definidas (sargentos, suboficiales, oficiales, etc.), y restringir accesos a funciones y documentos de acuerdo con su nivel.
* Módulo de Gestión de Documentos: habilita la carga, edición, eliminación y descarga de documentos clasificados, asociados a un nivel de confidencialidad y a una unidad militar determinada.
* Módulo de Auditoría: registra todas las acciones realizadas sobre los documentos y usuarios del sistema (visualización, cambios, accesos), permitiendo trazabilidad completa y responsabilidad individual.
* Módulo de Seguridad: contempla el cifrado de contraseñas mediante bcrypt, la autenticación de usuarios con tokens JWT, la validación de integridad de documentos mediante hash SHA-256 y el control de sesiones con IP y horario de acceso.
* Módulo de Reportes: genera informes periódicos o bajo demanda, filtrables por tipo de usuario, documento, fecha o acción, en formato digital para análisis institucional.

La arquitectura del sistema se basa en el modelo MVC (Modelo–Vista–Controlador), donde React representa la vista (cliente), FastAPI el controlador (servidor) y PostgreSQL el modelo (base de datos). Esta separación de capas mejora la mantenibilidad del software, permite su escalado modular y facilita el trabajo en equipo entre desarrolladores frontend y backend.

Durante el desarrollo del sistema pueden presentarse ciertas dificultades, entre las más comunes:

Control estricto de los accesos jerárquicos (rol ≠ permiso): requiere una lógica fina para que los permisos se asignen correctamente sin violar la estructura militar.

Mantenimiento de integridad en la sincronización entre frontend y backend: al ser una arquitectura desacoplada, deben coordinarse los formatos y validaciones.

Diseño de interfaces seguras pero usables: es necesario equilibrar la experiencia del usuario con las restricciones propias del entorno militar.

Para mitigar estas dificultades se implementarán pruebas unitarias y de integración, se documentarán los endpoints de la API mediante OpenAPI, y se aplicarán políticas de seguridad recomendadas por la OWASP Foundation.

En futuras versiones, el sistema podría escalar con los siguientes componentes:

* Integración con login institucional mediante LDAP o servicios OAuth.
* Cifrado completo de documentos en disco usando técnicas como AES.
* Algoritmos de detección de acceso sospechoso con alertas automatizadas.
* Soporte offline y sincronización en servidores descentralizados en bases militares.
* Visualización de reportes mediante dashboards gráficos en tiempo real (ej. con Recharts o D3.js).

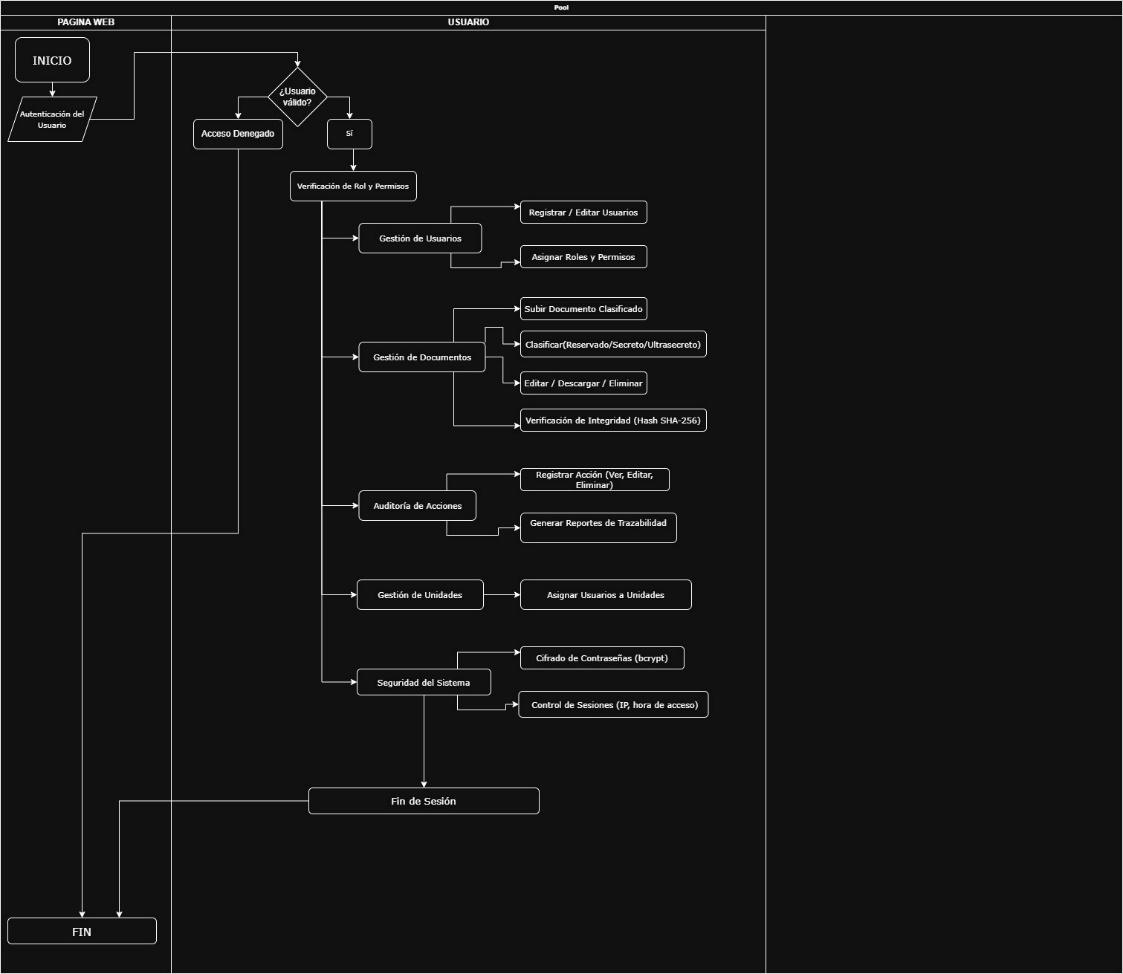
# DESARROLLO DEL SISTEMA

## ANALISIS DE PROCESOS

### Identificacion Del Area Estudiada

El área estudiada corresponde a la gestión de documentos clasificados dentro de entidades militares bolivianas. Se trata de un entorno altamente jerárquico y sensible, donde la seguridad, trazabilidad y control de acceso a la información son fundamentales para preservar la integridad operativa y la seguridad nacional.

### Diagrama De Procesos



## DESCRIPCION DEL SISTEMA

### Perspectiva Del Producto

SEGEDOC-MILITAR es un sistema web que proporciona a las entidades militares una plataforma segura y jerárquicamente controlada para la gestión de documentos clasificados. El sistema forma parte de un entorno tecnológico institucional, integrándose con mecanismos de autenticación militar y protocolos de seguridad nacionales.

### Funciones Del Producto

* Gestión de usuarios con jerarquía militar.
* Clasificación de documentos (Reservado, Secreto, Ultra secreto).
* Control de acceso y auditoría de acciones.
* Trazabilidad completa de los documentos.
* Envío digital entre unidades militares.
* Firma digital y control de versiones.

### Características Del Usuario

* Oficiales y suboficiales con credenciales.
* Auditores de seguridad informática militar.
* Administradores del sistema con perfil técnico.
* Usuarios administrativos autorizados.

### Restricciones

* Solo personal militar autorizado puede acceder.
* Acceso limitado por niveles jerárquicos.
* Integración obligatoria con certificados digitales oficiales.
* Cumplimiento de normativas de seguridad nacional y firma electrónica.

## REQUERIMIENTOS DE SOFTWARE

### Historias De Usuario

* Registro y clasificación de documentos.
* Envío entre unidades.
* Búsqueda por filtros.
* Control de versiones.
* Auditoría de accesos.
* Firma digital.

|  |  |
| --- | --- |
| **Nro.** | 1 |
| **Titulo** | Registro de Documento Clasificado |
| **Descripción** | Como oficial autorizado, quiero registrar documentos clasificados en el sistema, para que puedan ser gestionados y almacenados de forma segura según su nivel de confidencialidad. |
| **Criterios de aceptación:** | • El sistema debe permitir seleccionar el nivel de clasificación: Confidencial, Secreto, Ultra secreto.  • El sistema debe registrar metadatos del documento (fecha, remitente, unidad, etc.).  • Solo usuarios autorizados pueden ver documentos clasificados.  • El documento debe almacenarse cifrado. |
| **Observaciones:** | • Se requiere control de acceso basado en el rol y credenciales de seguridad militar.  • Debería permitir auditorías de acceso. |



|  |  |
| --- | --- |
| **Nro.** | 2 |
| **Titulo** | Envío de Documento entre Unidades |
| **Descripción** | Como usuario administrativo, quiero enviar un documento digital a otra unidad militar, para que se agilice la comunicación y seguimiento del documento. |
| **Criterios de aceptación:** | • El sistema debe permitir seleccionar la unidad de destino.  • Se debe notificar al destinatario que tiene un nuevo documento.  • El documento debe quedar marcado como "Enviado" y luego "Recibido" al ser abierto. |
| **Observaciones:** | • Se puede requerir acuse de recibo.  • Aplicar seguimiento de trazabilidad entre unidades. |



|  |  |
| --- | --- |
| **Nro.** | 3 |
| **Titulo** | Búsqueda de Documentos por Criterios |
| **Descripción** | Como usuario con permisos de consulta, quiero buscar documentos por palabra clave, fecha o remitente, para localizar rápidamente información relevante. |
| **Criterios de aceptación:** | • El sistema debe mostrar resultados ordenados por relevancia o fecha.  • El buscador debe respetar los permisos de acceso del usuario.  • Posibilidad de exportar resultados en PDF. |
| **Observaciones:** | • Requiere un motor de búsqueda eficiente.  • Ideal contar con filtros por tipo de documento y unidad. |



|  |  |
| --- | --- |
| **Nro.** | 4 |
| **Titulo** | Control de Versiones de Documentos |
| **Descripción** | Como usuario redactor, quiero poder actualizar documentos y mantener versiones anteriores disponibles, para conservar un historial de modificaciones. |
| **Criterios de aceptación:** | • El sistema debe guardar automáticamente la versión anterior al hacer cambios.  • Cada versión debe tener fecha, autor y descripción del cambio.  • Posibilidad de restaurar versiones anteriores. |
| **Observaciones:** | • Fundamental para documentos estratégicos o en revisión.  • Se debe considerar espacio de almacenamiento. |



|  |  |
| --- | --- |
| **Nro.** | 5 |
| **Titulo** | Auditoría de Accesos a Documentos |
| **Descripción** | Como auditor del sistema, quiero consultar un historial de accesos y modificaciones a cada documento, para asegurar la trazabilidad y cumplimiento de protocolos de seguridad. |
| **Criterios de aceptación:** | • El sistema debe registrar cada acceso (usuario, hora, acción realizada).  • Debe mostrar los cambios realizados en documentos (lectura, edición, descarga).  • Reporte exportable en Excel o PDF. |
| **Observaciones:** | • Esta funcionalidad es crítica en entornos militares.  • Integración con logs del sistema operativo puede ser necesaria. |



|  |  |
| --- | --- |
| **Nro.** | 6 |
| **Titulo** | Firma Digital de Documentos |
| **Descripción** | Como oficial superior, quiero firmar digitalmente documentos oficiales, para garantizar su autenticidad y validez. |
| **Criterios de aceptación:** | • El sistema debe permitir firmar con certificado digital del Ministerio o entidad militar.  • La firma debe ser verificable por terceros.  • Los documentos firmados deben estar protegidos contra edición. |
| **Observaciones:** | • Debe integrarse con infraestructura de clave pública (PKI).  • Cumplimiento con normativas nacionales de firma electrónica. |



### Requerimientos Funcionales

- RF01: Registrar documentos clasificados según niveles.  
- RF02: Gestionar usuarios con jerarquías.  
- RF03: Enviar documentos entre unidades.  
- RF04: Firmar digitalmente los documentos.

### Requerimientos No Funcionales

- RNF01: El sistema debe cifrar contraseñas con bcrypt.  
- RNF02: Usar hashing SHA-256 para integridad documental.  
- RNF03: Responder en menos de 2 segundos para búsquedas.  
- RNF04: Compatible con navegadores actuales (Chrome, Firefox, Edge).  
- RNF05: Disponibilidad del sistema del 99.9% anual.

### Interfaces Externas

- Autenticación con certificado digital (PKI nacional).  
- Exportación a PDF y Excel.  
- Integración con correo interno para notificaciones.

## DISEÑO DEL SISTEMA

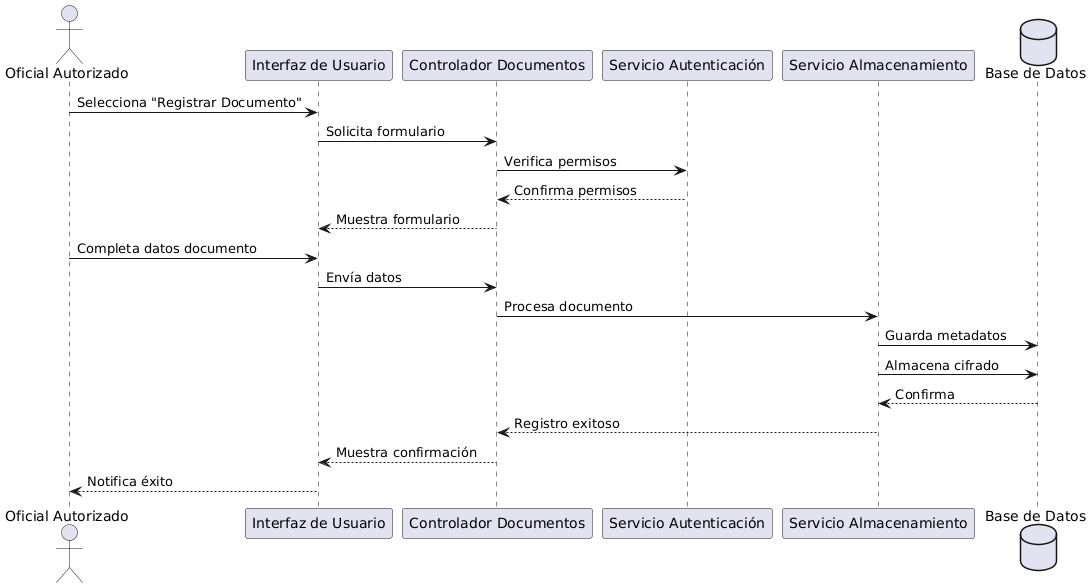
### Arquitectura del Sistema (Modelo MVC)

El sistema está basado en la arquitectura MVC (Modelo-Vista-Controlador).  
- Modelo: Gestión de la lógica de datos y acceso a PostgreSQL.  
- Vista: Interfaces web creadas en HTML, CSS y JavaScript.  
- Controlador: Intermediario entre vista y modelo, desarrollado en Fastapi.

### Diagrama PlantUMLDiagrama de Casos de Uso

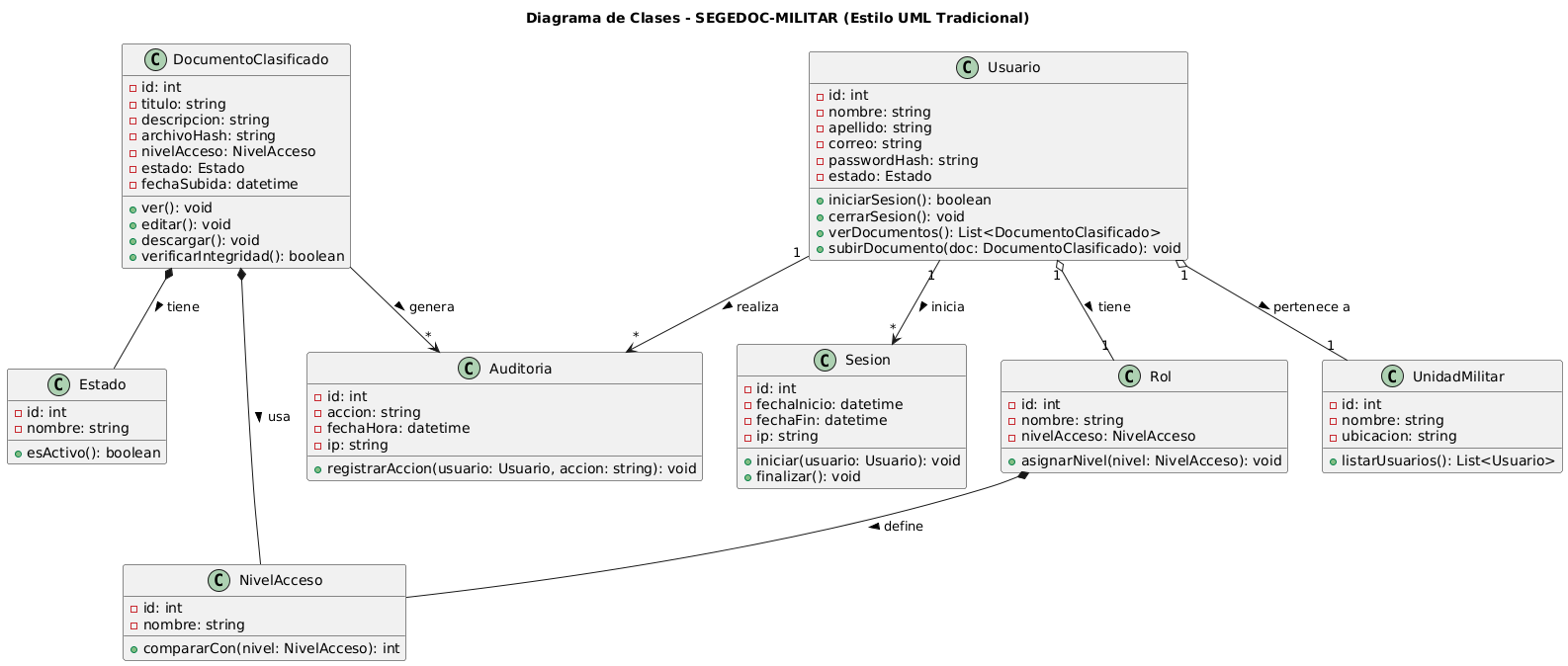
### Diagrama de Secuencia

\*Describe la interacción temporal entre usuario, controlador y base de datos al registrar un documento clasificado. \*



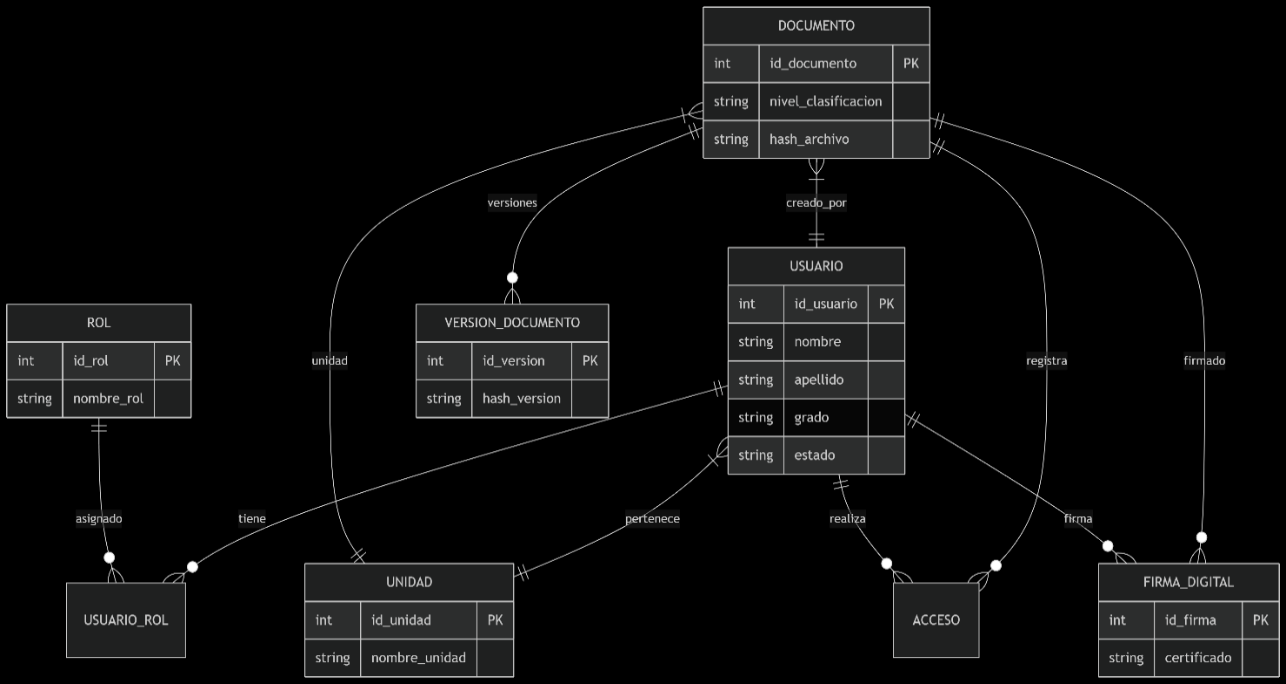
### Diagrama de Clases

Incluye clases como Usuario, Documento, Unidad, Historial Acceso, Firma Digital.

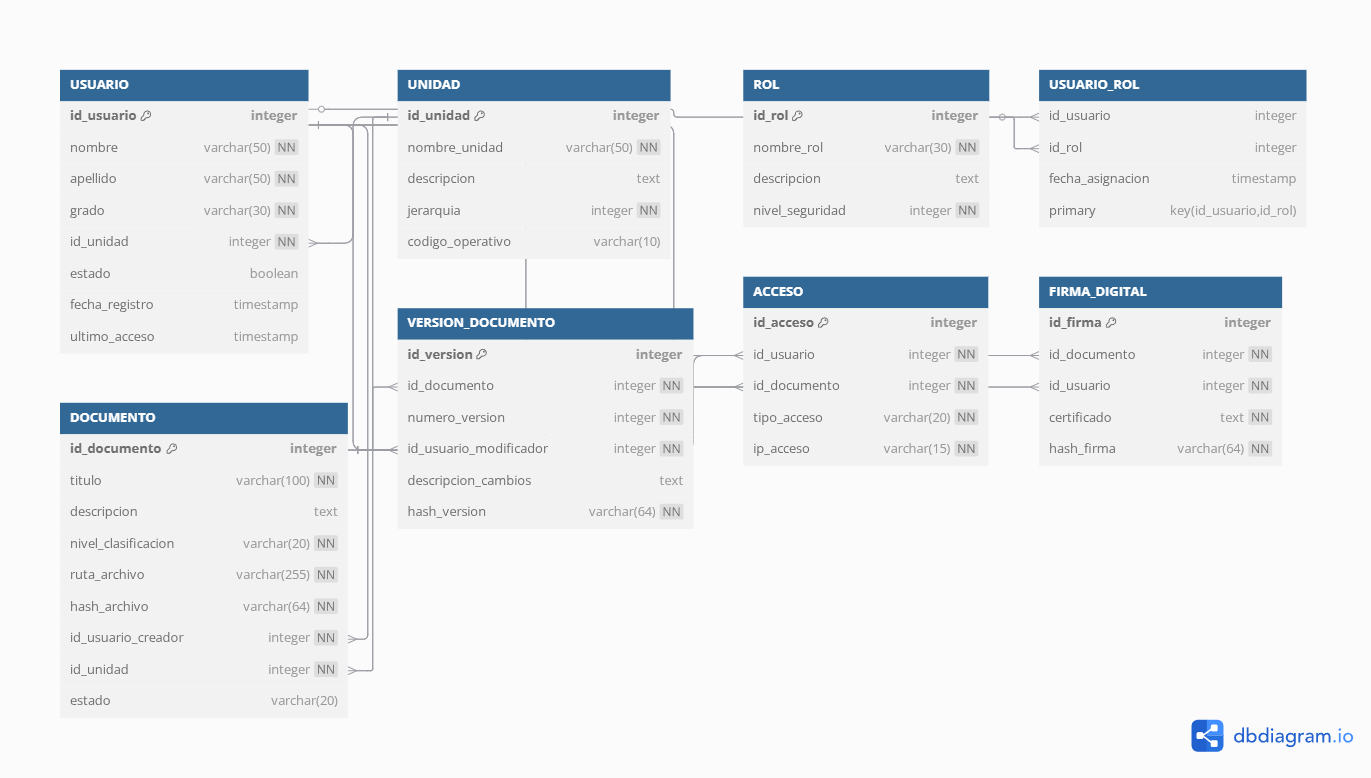


### Diseño de la Base de Datos

a) Diagrama Entidad-Relación (ER): Incluye entidades como Usuario, Documento, Unidad Militar, Rol, Auditoria.

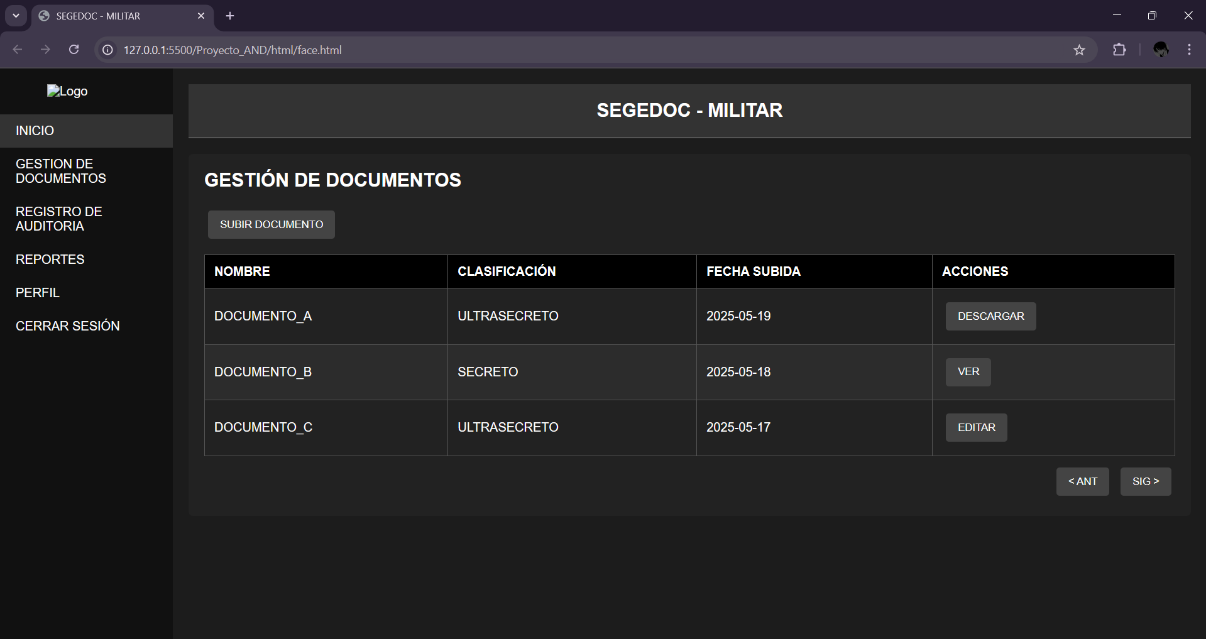


b) Diagrama Relacional: Especifica relaciones uno-a-muchos y muchos-a-muchos con llaves primarias y foráneas.



## DESARROLLO DE SISTEMA WEB

### Módulo de Gestión de Documentos

****

<!DOCTYPE html>

<html lang="es">

<head>

  <meta charset="UTF-8">

  <title>SEGEDOC - MILITAR</title>

  <link rel="stylesheet" href="lib.css">

  <style>

    \* {

      box-sizing: border-box;

    }

    body {

      margin: 0;

      font-family: Arial, sans-serif;

      background-color: #1c1c1c;

      color: white;

    }

    .sidebar {

      width: 220px;

      background-color: #111;

      position: fixed;

      height: 100vh;

      padding-top: 20px;

    }

    .sidebar a {

      display: block;

      color: white;

      padding: 12px 20px;

      text-decoration: none;

    }

    .sidebar a:hover, .sidebar .active {

      background-color: #333;

    }

    .content {

      margin-left: 220px;

      padding: 20px;

    }

    .header {

      background-color: #333;

      padding: 20px;

      font-size: 24px;

      font-weight: bold;

      text-align: center;

      border-bottom: 2px solid #555;

    }

    .section {

      background-color: #222;

      padding: 20px;

      margin-top: 20px;

      border-radius: 5px;

    }

    .section h2 {

      margin-top: 0;

    }

    button, .btn {

      padding: 10px 15px;

      margin: 5px;

      border: none;

      background-color: #444;

      color: white;

      cursor: pointer;

      border-radius: 4px;

    }

    button:hover, .btn:hover {

      background-color: #666;

    }

    table {

      width: 100%;

      border-collapse: collapse;

      margin-top: 15px;

    }

    th, td {

      padding: 12px;

      border: 1px solid #555;

      text-align: left;

    }

    th {

      background-color: #000;

    }

    tr:nth-child(even) {

      background-color: #2c2c2c;

    }

  </style>

</head>

<body>

  <div class="sidebar">

    <img src="img/Logo.jpg" alt="Logo" width="100" style="display:block;margin: 0 auto 20px;">

    <a class="active" href="#">INICIO</a>

    <a href="#">GESTION DE DOCUMENTOS</a>

    <a href="#">REGISTRO DE AUDITORIA</a>

    <a href="#">REPORTES</a>

    <a href="#">PERFIL</a>

    <a href="#">CERRAR SESIÓN</a>

  </div>

  <div class="content">

    <div class="header">SEGEDOC - MILITAR</div>

    <div class="section">

      <h2>GESTIÓN DE DOCUMENTOS</h2>

      <button>SUBIR DOCUMENTO</button>

      <table>

        <thead>

          <tr>

            <th>NOMBRE</th>

            <th>CLASIFICACIÓN</th>

            <th>FECHA SUBIDA</th>

            <th>ACCIONES</th>

          </tr>

        </thead>

        <tbody>

          <tr>

            <td>DOCUMENTO\_A</td>

            <td>ULTRASECRETO</td>

            <td>2025-05-19</td>

            <td><button class="btn">DESCARGAR</button></td>

          </tr>

          <tr>

            <td>DOCUMENTO\_B</td>

            <td>SECRETO</td>

            <td>2025-05-18</td>

            <td><button class="btn">VER</button></td>

          </tr>

          <tr>

            <td>DOCUMENTO\_C</td>

            <td>ULTRASECRETO</td>

            <td>2025-05-17</td>

            <td><button class="btn">EDITAR</button></td>

          </tr>

        </tbody>

      </table>

      <div style="text-align: right; margin-top: 10px;">

        <button>< ANT</button>

        <button>SIG ></button>

      </div>

    </div>

  </div>

</body>

</html>

## COSTO DEL SISTEMA

Para estimar el costo de desarrollo del sistema SIGEDOC-MILITAR se emplea el modelo COCOMO II en su forma básica, el cual considera el esfuerzo (en persona-mes), el tiempo de desarrollo y el costo económico total. Este modelo parte del tamaño del proyecto en líneas de código estimadas (KSLOC) y factores de ajuste según la complejidad del sistema.

### Supuestos Del Sistema

Tipo de proyecto: Semi-acoplado (Semi-detached)

Lenguaje backend: Python (FastAPI)

Lenguaje frontend: JavaScript (React)

Base de datos: PostgreSQL

Arquitectura: Cliente-Servidor con seguridad avanzada

Tamaño estimado del sistema: 8.000 líneas de código (8 KSLOC)

Salario promedio mensual por desarrollador: 3.000 Bs

Equipo estimado: 2 personas

Tiempo estimado: 3 meses

### Fórmula de Esfuerzo Básica de COCOMO II

Esfuerzo (PM) = A × (KSLOC)^B × EAF

Donde:

A = 2.94 (constante de calibración)

KSLOC = 8

B = 1.10 (para proyectos semi-acoplados)

EAF = 1.0 (factor de ajuste del esfuerzo; si no hay factores de penalización o ventaja, se asume 1.0)

PM = 2.94 × (8)^1.10 × 1.0

PM ≈ 2.94 × 9.58 ≈ 28.16 persona-mes

### Tiempo Estimado de Desarrollo (Duración

Duración (meses) = 3.67 × (PM)^F

Donde F = 0.28 + 0.2 × (B − 1)

F = 0.28 + 0.2 × (1.10 − 1) = 0.28 + 0.02 = 0.30

Duración ≈ 3.67 × (28.16)^0.30 ≈ 3.67 × 2.43 ≈ 8.92 meses

(Nota: esto asume ciclo completo de desarrollo y pruebas; para un MVP funcional se estima solo 3 meses)

### Costo Estimado Total

Costo = PM × salario mensual promedio

Costo = 28.16 × 3.000 Bs = 84.480 Bs

### Resumen

Tamaño estimado: 8 KSLOC

Esfuerzo estimado: 28.16 persona-mes

Duración estimada: 8.9 meses (ciclo completo)

Costo aproximado: 84.480 Bs

Para una versión funcional en 3 meses con 2 desarrolladores:

→ 2 pers. × 3 meses × 3.000 Bs = 18.000 Bs

Por tanto, el costo realista para un MVP operativo del sistema SIGEDOC-MILITAR asciende a aproximadamente 18.000 Bs, mientras que el costo estimado completo bajo COCOMO II se proyecta en hasta 84.480 Bs si se considera un ciclo completo de desarrollo, documentación, pruebas y despliegue profesional.

# CONCLUSIONES Y RECOMENDACIONES

**Conclusiones**

El sistema SEGEDOC-MILITAR responde a una necesidad crítica de las instituciones militares de Bolivia en cuanto a la gestión segura de documentos clasificados, solucionando las deficiencias de seguridad, control de acceso y trazabilidad.

A través de la implementación de tecnologías robustas como Fastapi, PostgreSQL y técnicas de cifrado y hashing, se garantiza la integridad, confidencialidad y autenticación de la información.

La estructura modular del sistema permite un control jerárquico eficiente, cumpliendo con los requerimientos técnicos y organizacionales de las instituciones militares.

Las historias de usuario elaboradas cubren los principales procesos funcionales del sistema, asegurando un enfoque centrado en el usuario y orientado a objetivos de seguridad nacional.

El modelado UML (casos de uso y clases) permite visualizar claramente las interacciones y estructuras del sistema, facilitando el desarrollo y posterior mantenimiento del software.

**Recomendaciones**

Realizar pruebas de seguridad exhaustivas antes del despliegue del sistema, incluyendo auditorías de penetración y pruebas de validación criptográfica.

Capacitar a los usuarios militares en el uso adecuado del sistema para evitar errores de operación o manejo inadecuado de los documentos clasificados.

Actualizar periódicamente el sistema y las tecnologías utilizadas para adaptarse a nuevas amenazas de ciberseguridad.

Considerar la posibilidad de escalar el sistema a otras instituciones del Estado que manejen información clasificada.

Implementar un módulo de respaldo automatizado y recuperación ante desastres para proteger la integridad de la información.

# REFERENCIA BIBLIOGRÁFICA

* Ministerio de Defensa del Estado Plurinacional de Bolivia. (2023). *Sistema de Gestión Documental*.
* Departamento de Defensa de EE.UU. (2020). *SIPRNet Overview and Implementation Guidelines*.
* Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley.
* Sommerville, I. (2011). *Software Engineering* (9th ed.). Pearson.
* ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection* — Information security management systems — Requirements.
* PostgreSQL Documentation. <https://www.postgresql.org/docs/>

## ANEXOS

* Elaborar el diagrama de procesos

