Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

Autores:

Ernesto Bárbaro Alvarez Gómez.

Arelys Cerra Domínguez.

La Habana, Cuba

Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

Resumen

La aplicación Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) sustituye al actual sitio del Punto de Dirección, actualizando el contenido de la información a gestionar y la forma en que se realiza. Logra informatizar procesos internos de la Dirección de Seguridad, Protección y Defensa que en la actualidad se mantienen en formatos tradicionales, una retroalimentación informativa eficiente, atractiva y segura con otras áreas, fundamentalmente las sucursales. Utiliza técnicas más actualizadas y con probada seguridad en el desarrollo web. Facilita la disponibilidad de la información y su protección en tiempo real. Apoya en la toma de decisiones, la actualización de planes de prevención, continuidad del servicio y contingencias, exportando dicha información a diversos formatos para los principales directivos del sistema bancario y las entidades involucradas de forma directa o indirecta.

PALABRAS CLAVES:

Seguridad, Punto de Dirección, Parte Diario, Automatización, Gestión, Protección, Información, Vulnerabilidades, Software Libre, Actualización.

Índice

Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

Introducción

El Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) constituye la versión 4.0 del actual Sitio de Gestión Informativa de Seguridad y Protección. Con esta nueva versión se corrigen un grupo de vulnerabilidades tanto de programación como de gestión documental presentes en la actual aplicación. Se simplifican procesos automatizados que en la actualidad son bastante obsoletos en su tratamiento por la web vigente, y se agregan otros procedimientos imprescindibles en el trabajo de intercambio de datos entre la Dirección de Seguridad, Protección y Defensa (DSPD) y las entidades del Banco Metropolitano. Además, se propone un cambio total en la imagen de la aplicación para que sea más atractiva en su uso tanto por las áreas que tributan información, como por los especialistas que la gestionan. Se introduce el empleo de tecnologías actualizadas de software libre, corrigiendo vulnerabilidades técnicas que presenta el actual framework en uso. No se modifica la actual web, sino que se crea una nueva que mantiene su mismo objetivo, pero con nuevos elementos en su desarrollo.

Antecedentes:

Desde el año 2014 fue implementada la primera versión de la web para emitir el Parte Diario que dan las sucursales al Punto de Dirección en la Oficina Central. Este proceso pasa a ser automatizado y centralizado, pasando por diversas etapas de su desarrollo hasta la actualidad donde se emplea la versión 3.0 de la Web, a la cual se le han añadido nuevas funcionalidades pasando a llamarse Web del Parte Diario a Gestión Informativa de Seguridad y Protección, al incluir la gestión documental de esta Dirección en sus diferentes especialidades. El incremento de las tareas en la Dirección, y el creciente intercambio de datos entre otras áreas del banco y entidades externas, ha complejizado el contexto informativo por lo que se propone una nueva actualización de la Web, con una versión más moderna, actualizada a los intereses y estilos de trabajos de las especialidades que integran la seguridad y la Protección,

automatizando diversos procesos dentro de la gestión de la información, que actualmente continúan en formato tradicional, logrando una mayor centralización de la actividad y simplificando procesos previamente identificados.

Con esta nueva versión se corrigen un grupo de vulnerabilidades internas que presenta la aplicación actual.

Vulnerabilidades internas de la versión 3.0 de la aplicación web de Seguridad y Protección:

Mediante la herramienta de seguridad *OWASP ZAP 2.9.0* se realizan escaneos de vulnerabilidades a las aplicaciones web internas, con el objetivo de detectar problemas de seguridad y realizar acciones correctivas para prevenir incidentes asociados a la posible explotación de dichas fallas.

La actual Web presenta las siguientes vulnerabilidades en su desarrollo interno, las cuales se eliminan con la implementación de la nueva versión de la Web, el sistema GESPROD:

Vulnerabilidades	**Descripción**
Encabezado X-Frame-Options no establecido.	El encabezado X-Frame_options no está incluido en la respuesta **HTTP** para proteger ante ataques '**ClickJacking**'.
Exploración de Directorios.	Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc, que se pueden acceder para leer información sensible.
Cookie No HttpOnly Flag.	Se ha establecido una cookie sin la **bandera HttpOnly**, lo que significa que la cookie puede ser accedida mediante **JavaScript**. Si un script malicioso puede ser

	ejecutado en esta página entonces la cookie será accesible y podrá ser transmitida a otro sitio. Si esta es una cookie de sesión entonces el secuestro de sesión podría ser posible.
Protección de buscador de web **XSS** no disponible.	La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el servidor de web.
No se encuentra encabezado X-Content-Type-Options **Header**.	El encabezado **Anti-MIME-Sniffing** X-Content-Type-Options no estaba configurado para '**nosniff**'. Esto permite versiones antiguas de Internet Explore y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado.
Absence of Anti-CSRF **Tokens.**	Provoca una solicitud falsa entre sitios durante un ataque que compromete, y obliga, a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento, o intención, para poder realizar una acción como víctima. CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a **XSS**, porque se puede utilizar como una plataforma para CSRF, lo que le permite al atacante operar desde adentro de la aplicación.
Cookie Without SameSite Attribute.	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an

	effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Metodología de la Investigación:

En la versión anterior de la aplicación nos encontramos con los siguientes **problemas**:

- Los Partes Diarios desde las oficinas bancarias hacia el Punto de Dirección de la Oficina Central se realizan en formato plano, sin elementos interactivos, y depende de que las áreas tecleen la información, que en ocasiones no es la que se necesita, o llega incompleta.
- El Oficial de Guardia no puede editar los partes enviados, en caso de que alguno tenga errores al finalizar la jornada.
- Las áreas no pueden corregir el parte enviado, en un tiempo establecido, en caso de que hayan emitido información con errores.
- El Primer Nivel de Dirección no tiene una retroalimentación automatizada de los partes que emiten las áreas mediante la aplicación web.
- No existe un sistema centralizado de archivos y gestión documental de la dirección, que permita la consulta de los datos almacenados por los especialistas de la dirección y directivos que se designen.
- Los usuarios dependen de la acción y el tiempo de los administradores de la web para realizar tareas tan sencillas como el cambio de claves personales.
- Se emplea framework desactualizado, vulnerable a fallos técnicos en la aplicación.

Para darle una solución automatizada a esta **problemática** se actualiza la versión de la actual aplicación, denominada Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD):

1. ¿Cómo automatizar los procesos actualizados de gestión documental, internos y externos, en la Dirección de seguridad, Protección y Defensa?
2. ¿Cómo dinamizar los procesos de intercambio de información sobre el estado de la seguridad entre las áreas mediante la aplicación?
3. ¿Cómo emplear el uso de nuevas tecnologías de software libre para el desarrollo web y su empleo en la informatización de procesos internos?

Se establece como **Objeto de Estudio** la actualización de la plataforma automatizada para el trabajo de gestión informativa de la Dirección de Seguridad, Protección y Defensa, y se define como **Campo de Acción** los procesos para el control, análisis y toma de decisiones dentro de la misma, y hacia el resto de la entidad bancaria.

El **Objetivo General** de GESPROT consiste en**:** Actualizar la automatización los procesos de gestión de la información oficial ordinaria de la Dirección de Seguridad, Protección y Defensa.

Teniendo en cuenta el objetivo general planteado, se proponen los siguientes **objetivos específicos:**

- Implementar la automatización de la gestión de la información en la Dirección y permitir el acceso en tiempo real de otras áreas autorizadas y sus directivos.
- Automatizar procesos de intercambio de información entre la base y los niveles centrales, adaptando los partes diarios a los intereses reales de la entidad con un enfoque de Seguridad.

- Garantizar la disponibilidad, integridad y confidencialidad de la información ordinaria de la Dirección, centralizada en una plataforma única.
- Apoyar en los procesos de control y toma de decisiones, tanto preventivas como correctivas, de las especialidades que integran la dirección de Seguridad, Protección y Defensa.

Durante el cumplimiento de los objetivos propuestos se desarrollan las siguientes **tareas investigativas**:

- ✓ Actualización de los procesos de gestión de la información en la Dirección y sus niveles de operatividad e impacto en la seguridad de la entidad bancaria y sus activos.
- ✓ Actualizar los requerimientos funcionales y no funcionales para el desarrollo de este sistema.
- ✓ Aplicación de las herramientas y tecnologías seleccionadas para el desarrollo del sistema.
- ✓ Puesta en marcha de la aplicación en tiempo real y evaluación diaria de resultados en la solución de los problemas planteados.

Estructura de este trabajo:

Capítulo 1: Fundamentación Teórica

Se incluye el análisis de las herramientas informáticas, lenguajes de programación, y tecnologías de la información empleados.

Capítulo 2: Diseño e Implementación

Se realiza la propuesta del diseño del sistema y la implementación de las funcionalidades identificadas.

Capítulo 3: Pruebas

Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

Se presenta la plataforma de pruebas con los resultados obtenidos en cada fase del proyecto.

Capítulo 1: Fundamentación Teórica

1.1 Introducción

El propósito de este capítulo es realizar un estudio sobre los fundamentos teóricos que se emplean en el desarrollo del trabajo, con el resumen de las herramientas, lenguaje y tecnologías utilizadas.

1.2 Tendencias y tecnologías empleadas

Con la implementación de GESPROD, se actualizan las tecnologías de desarrollo de la aplicación web, utilizando un conjunto de plataformas, lenguajes y herramientas que se describen a continuación.

1.2.1 Modelo-Vista-Controlador.

El Modelo Vista Controlador es un patrón de arquitectura de sistemas informáticos que tiene como principal característica la separación de la lógica del negocio, los datos a gestionar, y la interfaz a nivel de usuario. Este modelo se mantiene de la versión anterior, por su importancia y flexibilidad en el desarrollo de aplicaciones afines al objetivo del trabajo.

1.2.2 Framework web2py.

Web2py es un marco de código abierto para el desarrollo ágil de aplicaciones web seguras, conectadas a servicios de bases de datos. Está programado en Python. Es un marco de desarrollo completamente integrado, es decir, contiene todos los componentes que se necesita para desarrollar aplicaciones web completamente funcionales.

Web2py se ha diseñado para guiar al desarrollador web a seguir buenas prácticas en ingeniería de software, como por ejemplo el uso del patrón Modelo-Vista-Controlador (MVC).

Web2py separa la *representación* de los datos (el modelo) de la *presentación* de los mismos (la vista) y de los algoritmos del flujo de operación (el controlador). Web2py provee de

librerías que ayudan al desarrollador en el diseño, implementación y realización de pruebas, y las administra de forma tal que trabajen en conjunto.

1.2.3 Lenguaje de Programación.

Python es un lenguaje de programación multipropósito de alto nivel. Tiene un núcleo sintáctico minimalista con unos pocos comandos básicos y semántica simple, pero tiene una enorme y variada librería estándar, que incluye una Interfaz de Programación de Aplicaciones (API) para muchas de las funciones en el nivel del Sistema Operativo.

El código Python define objetos incorporados como listas enlazadas (list), tuplas (tuple), tablas hash (dict), y enteros de longitud arbitraria (long). Soporta múltiples paradigmas de programación como: programación orientada a objetos (class), programación imperativa (def) y funcional (lambda). Python tiene un sistema de tipado dinámico y manejo automatizado de memoria utilizando conteo de referencias (similar a Perl, Ruby y Scheme).

1.2.4 Gestor de Base de Datos.

Para el desarrollo, en entorno de pruebas locales de GESPROD, se emplea **sqlite3**, pero en producción se proyecta la migración a MYSQL.

1.2.5 Otros aplicativos para complementar el desarrollo de la Web.

Se utiliza el framework **Bootstrap** y la librería **jquery**, que vienen integradas con **web2py**.

Se emplea el IDE de desarrollo **Geany,** que es otra solución de software libre.

En la etapa de desarrollo, para verificar la integridad y los datos ingresados a la Base de Datos se emplea el software **DB Browser for SQLite**.

1.3 Conclusiones del Capítulo

En este capítulo se ha dado a conocer el conjunto de elementos técnicos seleccionados para el desarrollo de GESPROD, y las características por los cuales fueron seleccionados. El

empleo de estas herramientas y tecnologías responde al interés de dar solución al problema planteado para agilizar el proceso de automatización, la inmediata administración en tiempo real sin afectar el trabajo del usuario, contar con las versiones actualizadas minimizando el impacto de posibles amenazas asociadas a estudios de riesgos realizados. Es importante que se desarrolle esta aplicación con herramientas que se integren a varias plataformas y poder extender el proyecto a diversos sistemas operativos.

Capítulo 2: Diseño e Implementación

2.1 Introducción

Este capítulo presenta el diseño e implementación de la aplicación, sus requerimientos funcionales y no funcionales, el sistema de seguridad, las peculiaridades del despliegue y la estructura de la base de datos.

2.2 Requerimientos funcionales

A continuación, se presentan los requerimientos de la aplicación para cumplir con los objetivos propuestos.

2.2.1 Módulo de Autenticación.

GESPROD establece un mecanismo de autenticación de usuarios para acceder a cada módulo del sistema. Cada usuario accede solamente a la información para la cual es previamente autorizada.

Solamente los administradores pueden acceder a todos los módulos.

En esta aplicación el usuario puede cambia su clave de acceso, evitando tener que contactar a los administradores como se hacía en las versiones anteriores para esta funcionalidad.

2.2.2. Gestionar el Parte Diario al Punto de Dirección.

Este es el principal módulo que permite la interacción entre las áreas del banco y la Oficina Central, representado en la figura del Oficial de Guardia del Punto de Dirección (OGO) quienes gestionan los datos recibidos de cada sucursal.

Los formularios son más precisos, se adaptan al contenido que se indica enviar, se diseñan de forma tal que el usuario cometa la mínima cantidad de errores y la información sea recibida con un mayor nivel de organización.

Además, se ha implementado una función que permita que esta información llega de forma automática, mediante correo electrónico, al Primer Nivel de Dirección, en formatos previamente establecido para su actualización diaria del estado de la seguridad en el Banco en tiempo real.

(Ver Anexo 1. Diagramas de Caso de Uso del Módulo del Parte Diario con los actores fundamentales y de Secuencias.)

2.2.3. Gestionar Archivo de la Dirección.

Este módulo permite gestionar en la base de datos los documentos ordinarios de la Dirección (cartas, facturas, dictámenes, entre otros) permitiendo una búsqueda más rápida de cualquier información que se desee consultar. Establece los números consecutivos de SPD-1 y crea una ficha actualizada de los documentos archivados. *(Ver Anexo 1. Diagramas de*

Actividades para los Principales Requerimientos Funcionales del Sistema. Gestión de Datos Estadísticos.)

2.2.4. Gestionar Control Estadístico del Estado de la Seguridad y la Protección.

Este módulo permite, mediante formularios y tablas, tener una base de datos estadística del estado de la Seguridad en cada área del banco, permitiendo a los usuarios autorizados realizar consultas directas, actualizar datos, y mediante estos tomar las acciones preventivas y/o correctivas que se consideren por las diferentes especialidades.

(Ver Anexo 1. Diagrama de Caso de Uso del Módulo de Control Estadístico del Estado de la Seguridad y la Protección.)

2.2.5. Gestionar Control Estadístico del Estado de la Protección de Cajeros Automáticos.

Este módulo permite, mediante formularios y tablas, tener una base de datos estadística del estado de la Seguridad en cada Cajero Automático del Banco, fundamentalmente mantener una gestión documental actualizada del sistema de control por cámaras de cada objetivo.

2.2.6. Gestionar Control Estadístico del Estado de la Seguridad Informática.

Esté módulo, como los mencionados anteriormente, gestiona mediante base de datos estadísticas, el estado de la Seguridad Informática por los diferentes parámetros que trabaja esta especialidad. Por su complejidad se le agregan varios subgrupos:

Registro de Dictámenes Técnicos.

En este subgrupo se relacionan todos los dictámenes técnicos de Seguridad Informática y pueden ser consultados por las áreas que se autoricen.

Autocontrol online.

Se implementan listas de chequeo remoto que permite, tanto a especialistas de la Dirección como a los informáticos en sucursales y la Oficina Central, realizar una autoevaluación del estado de la Seguridad Informática en su área, y a partir de los resultados gestionar el Sistema de Gestión de la Seguridad Informática.

Registro de la Protección Antivirus y Base de Datos de Malware.

En este subgrupo se relaciona por área el estado de su protección antivirus, las versiones instaladas, actualizaciones, malware detectados y las acciones realizadas. Permite elaborar informes estadísticos tanto locales como generales sobre esta protección en todo el banco y un monitoreo del comportamiento de las incidencias de programas malignos.

2.2.7. Capacitación Online y Test de Evaluación.

Este módulo permite publicar información didáctica de capacitación online para usuarios sobre temas de Seguridad y Protección, además de crear test de evaluación que permitan evaluar el conocimiento básico sobre estos temas, incluyendo cursos remotos para especialistas y técnicos informáticos en temas de ciberseguridad, evitando reuniones presenciales y pruebas en papel.

2.3 Requerimientos no funcionales

- De Software
  - Para el desarrollo de la aplicación:
    - ✓ Sistema Operativo: Windows y Linux (al ser una app web puede ser desarrollado sobre ambos).
    - ✓ Framework web2py y Bootstrap.

- ✓ IDE de desarrollo Geany.
- ✓ Aplicación de gestión de base de datos DB Browser for SQLite.

➢ Para la implementación

- ✓ Del lado del servidor.
  - ▪ Sistema Operativo: Versiones actuales de Windows Server y/o distribuciones Linux.
  - ▪ Servidor Web: Apache (versión actualizada).
- ✓ Del lado del cliente.
  - ▪ Conexión a la Red del Banco Metropolitano.
  - ▪ Navegador Web (Se recomienda Mozilla Firefox en sus últimas versiones).

❖ De Hardware

➢ Para el desarrollo de la aplicación

- ✓ Microprocesador: Intel® Celeron(R) CPU G1840 @ 2.80GHz × 2.
- ✓ Memoria RAM: 2GB.
- ✓ HDD: 80GB.

➢ Del lado del servidor

- ✓ Memoria RAM: 8GB.
- ✓ HDD: 250GB.

2.4 Diseño del sistema

GESPROD está compuesto por los diferentes módulos que ya se han explicado en los capítulos anteriores:

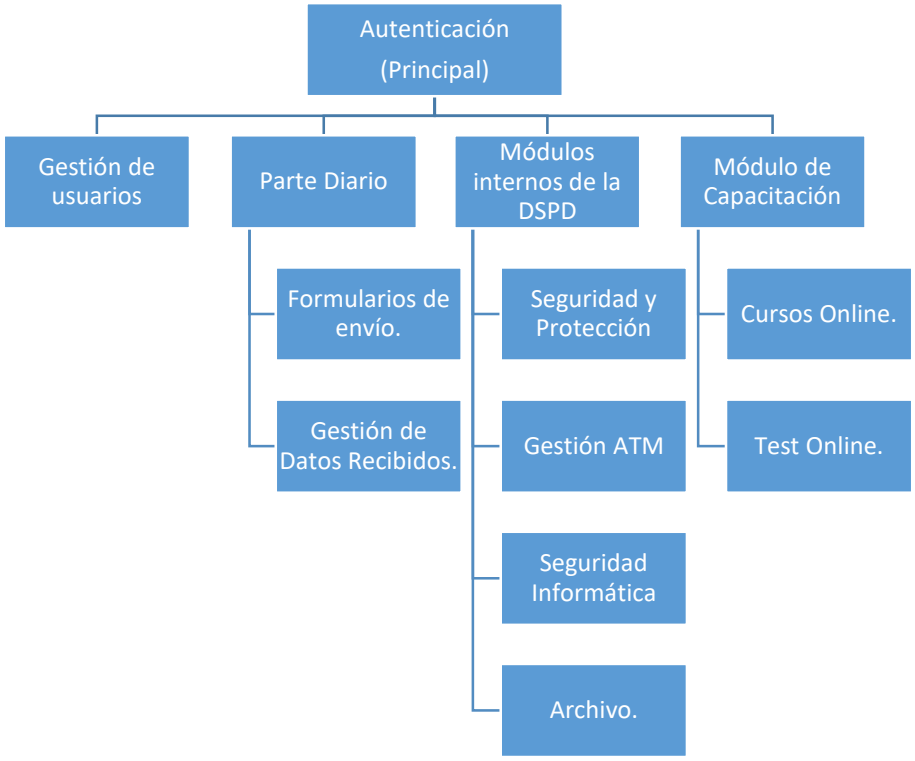


Figura 1. Estructura simplificada de GESPROD.

2.6 Base de Datos

Se trata de una base de datos relacional, que crece a medida que se incrementan los módulos y funciones a desarrollar por la aplicación.

Figura 2. Esquema de la Base de Datos.

2.7 Diagrama de despliegue y componentes.

Este diagrama muestra la estructura de despliegue de los diferentes nodos que intervienen en el flujo informativo de GESPROD e integra los principales componentes (generalizados) que se relacionan con cada entidad.

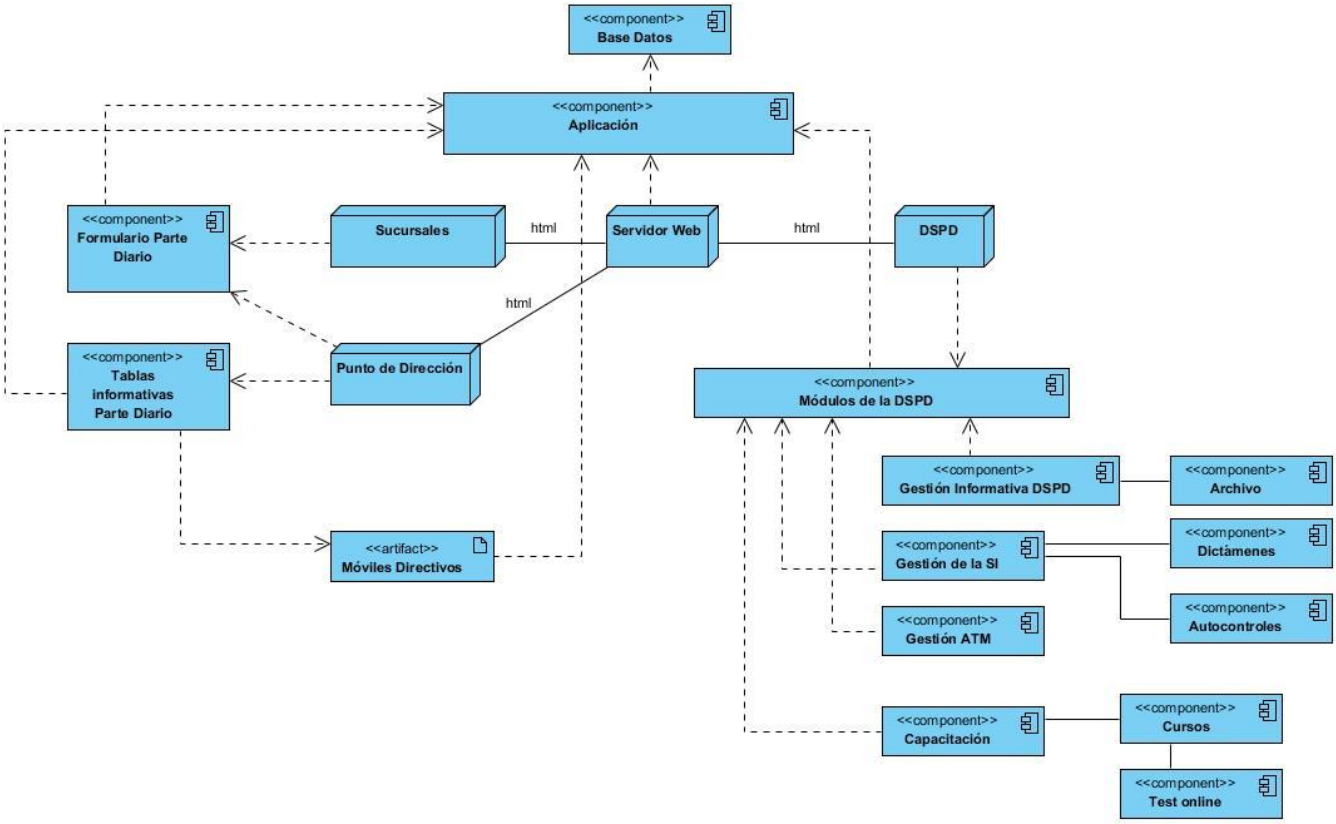


Figura 3. Diagrama de despliegue y componentes.

2.8 Seguridad

Estudio de riesgos de la aplicación:

Se emplea la herramienta de seguridad OWASP ZAP 2.9.0 para el diagnóstico interno de seguridad. En el escaneo realizado a la versión inicial de GESPROD, no se detectan errores críticos que se relacionen con vulnerabilidades internas.

Sistema de respaldo:

La nueva versión elimina las vulnerabilidades de la actual aplicación Web, descritas en este documento, logrando eliminar las amenazas más comunes identificadas para este tipo de sistemas: ataques por fuerza bruta, denegación de servicio e inyección SQL.

Se elimina la posibilidad de escala de privilegios para suplantación de identidad.

Para garantizar la integridad, confidencialidad y disponibilidad de la información, la aplicación Web y la base de datos cuentan con un sistema de salvas cruzadas hacia estaciones de trabajo de la Dirección y en dispositivos de almacenamiento extraíbles.

2.9 Conclusiones del Capítulo

Se han presentado los requerimientos funcionales y no funcionales imprescindibles para la solución automatizada de los objetivos trazados, así como la estructura de la aplicación en todo su conjunto, el despliegue de la misma, su sistema de seguridad, y una breve descripción de las características de la base de datos. Igualmente se concluye el capítulo presentando elementos de la seguridad del sistema, resultado de un estudio de riesgos realizado al efecto.

Capítulo 3: Pruebas

3.1 Introducción

En este capítulo se describe el proceso de pruebas realizado a GESPROD, con los resultados de las mismas, tanto en las tecnologías como en su impacto en el cumplimiento de los objetivos propuestos, y la solución de la problemática planteada.

3.2 Pruebas

Se realizaron pruebas de Caja Negra y Caja Blanca al sistema que ya se encuentra en su primera fase de despliegue. Se realizó un estudio entre los usuarios para conocer el **impacto real** de esta aplicación en la eficiencia del trabajo de la Dirección de Seguridad, Protección y Defensa, y su proyección hacia las dependencias de la entidad bancaria.

3.2.1 Pruebas de Caja Negra

Las pruebas de Caja Negra realizadas a las funcionalidades del sistema fueron las siguientes:

- **Pruebas de compatibilidad**: Se comprobó el funcionamiento de GESPROD y sus funcionalidades en diferentes plataformas: hardware, sistemas operativos, navegadores, y las subredes del Banco Metropolitano (Oficina Central y sucursales).
- **Pruebas de regresión**: Se comprobó el correcto funcionamiento de la aplicación ante cambios de funcionalidad.
- **Pruebas de integración:** Se comprobó la correcta integración de este sistema con otras aplicaciones disponibles en la red del Banco Metropolitano y el Sistema Bancario Nacional.
- **Pruebas de seguridad**: Se realizaron diagnósticos internos para la búsqueda de vulnerabilidades y comprobar la seguridad del sistema implementado, sus métodos de autenticación y la protección a la base de datos. En el capítulo anterior se describen los resultados de estas pruebas.
- **Pruebas de rendimiento**: Para comprobar si el usuario está satisfecho con la velocidad de la aplicación, bajo las condiciones de uso y las características técnicas de las estaciones de trabajo, el servidor y la velocidad de las comunicaciones.

Resultados:

Las pruebas realizadas arrojaron un resultado positivo en el cumplimiento al **98%** de los **requerimientos funcionales** propuestos a nivel de usuario.

El **2%** que aporta un resultado negativo en estas pruebas, corresponde a problemas relacionados con los **requerimientos no funcionales de Hardware del lado del servidor** (prueba de rendimiento), ya que la estación de servidor del Portal Web todavía no cumple con uno de estos parámetros provocando lentitud en algunos de los procesos automatizados. Este resultado deriva en la propuesta para mejorar el rendimiento del servidor donde se hospeda el

sistema GESPROD, o en caso necesario migrar la aplicación de su alojamiento actual a otro que cumpla los requerimientos establecidos.

3.2.2 Pruebas de Caja Blanca

Se aplicó el procedimiento de Camino Básico obteniéndose resultados positivos, teniendo en cuenta que el nivel de complejidad ciclomática de los algoritmos analizados es bajo.

Los casos de prueba derivados se corresponden al bajo nivel de complejidad ciclomática, que al ser comparados con las Pruebas de Bucles (para este caso bucles simples y concatenados) determinaron una efectividad técnica de los procesos automatizados, acortando el tiempo de procesamiento de los datos y el resultado de las operaciones realizadas en cada función.

Estas pruebas demostraron que la solución informática desarrollada es idónea para obtener los resultados esperados para cada operación, con tiempo de procesamiento óptimo y la calidad requerida en la gestión de datos.

3.3 Conclusiones del Capítulo

En este capítulo se ha realizado un resumen de las pruebas realizadas a la aplicación, las cuales aportaron resultados favorables que demuestran el cumplimiento de los requerimientos propuestos para el desarrollo de la misma, y un estado de opinión favorable entre los usuarios actuales del sistema, ya que se evidencia el cumplimiento del **99%** de los objetivos propuestos, faltando el despliegue total de todos los módulos de la aplicación a las dependencias de la entidad bancaria. Se plantea la necesidad de mejorar el rendimiento del equipamiento tecnológico que alberga al servidor.

Conclusiones Generales

1. En la actualidad GESPROD es utilizado para emitir el Parte Diario desde las sucursales al Punto de Dirección. Se encuentran activos los módulos de gestión interna y se trabaja en la actualización de los mismos, y el estudio de nuevos módulos. Con esta aplicación se han dado soluciones a las problemáticas planteadas, lo cual aporta las siguientes conclusiones:

- Se ha logrado dinamizar el proceso de gestión del parte diario y la gestión informativa de la Dirección.
- Permite automatizar procesos de gestión documental, que apoya en la toma de decisiones internas y externas asociadas a la Seguridad y la Protección.
- Simplifica el trabajo de gestión documental de los especialistas y aporta organización y seguridad.
- Contribuye a eliminar volúmenes de información impresa, pues los documentos se almacenan en formato digital, contribuyendo además al uso de firmas digitales en la mayoría de los casos.
- Se pueden realizar capacitaciones online sin la necesidad de emplear tiempo del horario laboral, y fuera de este, en clases presenciales, teniendo en cuenta la dinámica de trabajo de la mayoría de las sucursales y direcciones de la Oficina Central.
- Le permite al usuario evaluar y perfeccionar sus conocimientos en materias de Seguridad, protección y Defensa, además de contar con componentes interactivos que facilitan el autocontrol y la evaluación de los niveles de seguridad en su radio de acción.

2. El módulo del **Parte Diario** se encuentra desplegado en la red, para todo el Banco Metropolitano, accediendo los usuarios autorizados desde las distintas sucursales y otras áreas de la entidad. Esta aplicación ha tenido un impacto positivo ya que:

- Desde su implementación se han eliminado 3 teléfonos en el Punto de Dirección, de 4 que permanecían operativos.
- Los Oficiales de Guardia han reducido el tiempo de respuesta para el informe del Parte Diario, al cual se le han sumado nuevas informaciones de las sucursales y dependencias de la Oficina Central.
- Los Directivos del Primer Nivel pueden acceder a la aplicación desde sus dispositivos móviles y consultar el estado de la Seguridad desde el módulo del Parte diario, y además reciben en sus correos electrónicos los resúmenes de los mismos que se generan de forma automática, esto facilita la gestión de la información y la toma de decisiones sobre temas asociados a las especialidades de la Seguridad y la Protección.
- Estos datos demoraban un promedio de 5 horas para su recopilación vía telefónica, y una adicional para su posterior reordenamiento manual en la elaboración del resumen del día, pero con la automatización del proceso se ha reducido el tiempo a 30 minutos desde que la primera sucursal envía la información hasta que el Oficial de Guardia informa el cierre final.

3. Con los resultados anteriores se puede concluir:

✓ Se cumplió el objetivo general con la actualización de la gestión automatizada de los procesos asociados al flujo informativo de la Dirección de Seguridad, Protección y Defensa.

- ✓ Se actualiza la aplicación anterior, corrigiendo fallos identificados, que dan una solución más óptima a la problemática planteada
- ✓ Se garantiza la eficiencia de las labores de la Dirección, cuyas funciones son vitales e imprescindibles para el resto de los procesos de la entidad bancaria.
- ✓ Los elementos técnicos empleados para desarrollar GESPROD han demostrado eficacia y rapidez para conformar este sistema, y adaptabilidad a los cambios que permite mejorar sus prestaciones e incluir nuevos requerimientos que incrementen la automatización de nuevos procesos que se van incorporando al trabajo de la Dirección.
- ✓ A partir de la concepción del proyecto, se han cumplido con todas las etapas de su desarrollo en los plazos de tiempo establecidos, poniendo en funcionamiento las soluciones propuestas para la problemática planteada. *(Ver Anexo 2. Diagrama de Gantt)*

Recomendaciones

Teniendo en cuenta el incremento y complejidad de los procesos de la Dirección de Seguridad, Protección y Defensa, se recomienda:

- Incluir este sistema con la Intranet de la entidad, cuando esta se encuentre disponible.

- Incrementar nuevas funcionalidades en correspondencia con la actualización de los procesos de gestión de la Dirección de Seguridad, Protección y Defensa, y su impacto para el resto de las áreas del Banco Metropolitano.

Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

Referencias bibliográficas

WEB2PY COMPLETE REFERENCE MANUAL, 5TH EDITION *escrito por Massimo Di Pierro publicado el 15/03/2013.*

El gran libro de HTML5, CSS3 y Javascript*. Juan Diego Gauchat, Primera edición en libro electrónico: Enero de 2012, editorial: MARCOMBO, S.A. 2012 Gran Via de les Corts Catalanes, 594 08007 Barcelona (España).*

Glosario de términos

Punto de Dirección: Entidad encargada de recibir, concentrar y distribuir las informaciones relacionadas con la actividad de seguridad y protección de un organismo determinado.

Parte Diario: Información sistemática sobre un grupo de variables, que se circula a los dirigentes una institución, con el objetivo de mantenerlos actualizados.

Framework: En el desarrollo de software, un framework o infraestructura digital, es una estructura conceptual y tecnológica de soporte definido, normalmente con artefactos o módulos concretos de software, que puede servir de base para la organización y desarrollo de software. Típicamente, puede incluir soporte de programas, bibliotecas, y un lenguaje interpretado, entre otras herramientas, para así ayudar a desarrollar y unir los diferentes componentes de un proyecto. Representa una arquitectura de software que modela las relaciones generales de las entidades del dominio, y provee una estructura y una especial metodología de trabajo, la cual extiende o utiliza las aplicaciones del dominio.

Inyección SQL: Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Cookie (informática): El anglicismo cookie, usado también galleta o galleta informática, es un término que hace referencia a una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.

Token (informática): Un token de seguridad es un dispositivo electrónico de verificación de identidad y acceso al software utilizado en lugar de una contraseña de

autenticación. La tecnología de token de seguridad se basa en la autorización de dos factores o de múltiples factores.

Cabecera (header en inglés): En informática se refiere a la información suplementaria situada al principio de un bloque de información que va a ser almacenada o transmitida y que contiene información necesaria para el correcto tratamiento del bloque de información.

CSRF: Del inglés Cross-site request forgery o falsificación de petición en sitios cruzados, es un tipo de exploit malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, secuestro de sesión, y ataque automático.

Clickjacking: Es una técnica maliciosa para engañar a usuarios de Internet con el fin de que revelen información confidencial o tomar control de su ordenador cuando hacen clic en páginas web aparentemente inocentes. En uno de los muchos navegadores web o plataformas con alguna vulnerabilidad, un ataque de clickjacking puede tomar la forma de código incorporado o script que se ejecuta sin el conocimiento del usuario.

XSS o Cross Site Scripting: Una secuencia de comandos en sitios cruzados o Cross-site scripting (XSS por sus siglas en idioma inglés) es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar.

HttpOnly: Es un indicador adicional incluido en un encabezado de respuesta HTTP Set-Cookie. El uso de la bandera HttpOnly cuando se genera una cookie ayuda a mitigar el riesgo de script del lado del cliente que accede a la cookie protegida, si el navegador lo soporta.

HTTP nosniff: Es un marcador utilizado por el servidor para indicar que los tipos MIME anunciados en los encabezados Content-Type no se deben cambiar ni seguir. Esto permite

desactivar el MIME type sniffing. Este encabezado fue introducido por Microsoft en IE 8 para que los webmasters bloquearan el rastreo de contenido, pudiendo transformar tipos MIME no ejecutables en tipos MIME ejecutables

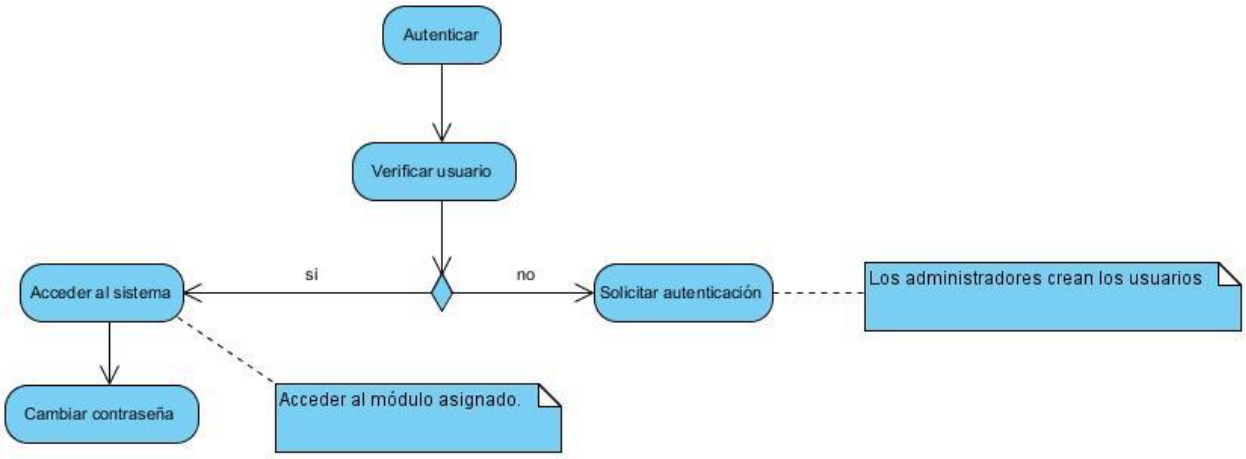
HTML: Siglas en inglés de HyperText Markup Language (‘lenguaje de marcado de hipertexto’), hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código (denominado código HTML) para la definición de contenido de una página web, como texto, imágenes, videos, juegos, entre otros.

JavaScript (abreviado comúnmente JS): Es un lenguaje de programación interpretado. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico. Se utiliza principalmente del lado del cliente, implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas y JavaScript del lado del servidor.

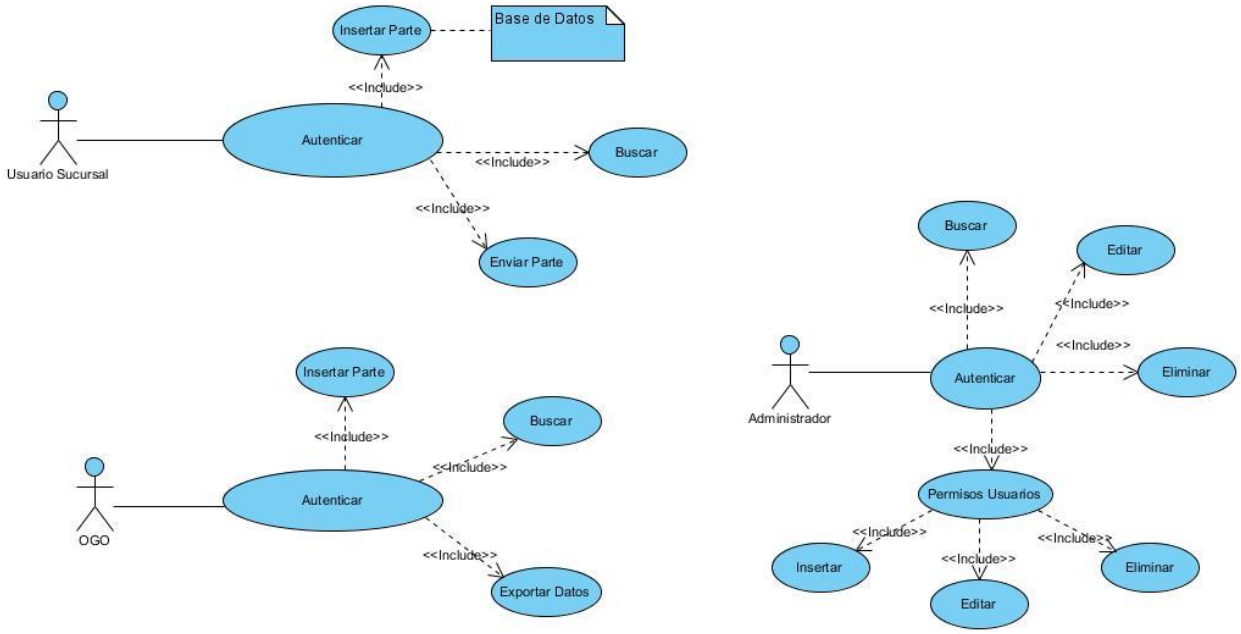
Anexos

Anexo 1.

Diagrama Simplificado de Actividades del Módulo de Autenticación:



Diagramas de Caso de Uso del Módulo del Parte Diario con los actores fundamentales:



---

1. **Diagrama de Secuencias del Parte Diario.**

Sistema de Gestión de Seguridad, Protección y Defensa (GESPROD) del Banco Metropolitano.

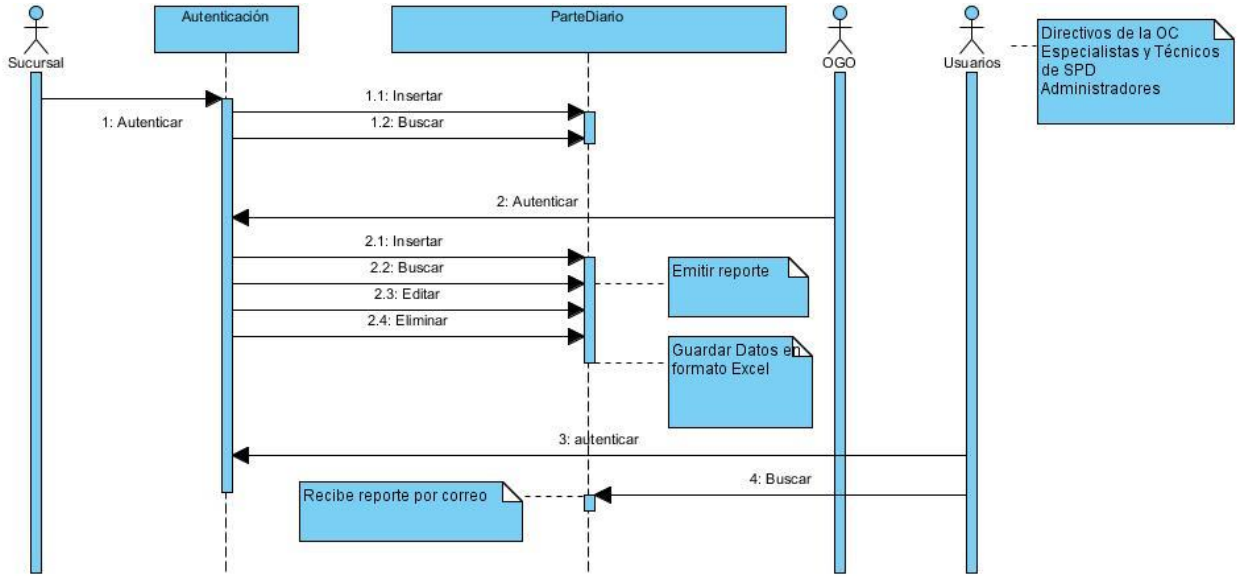
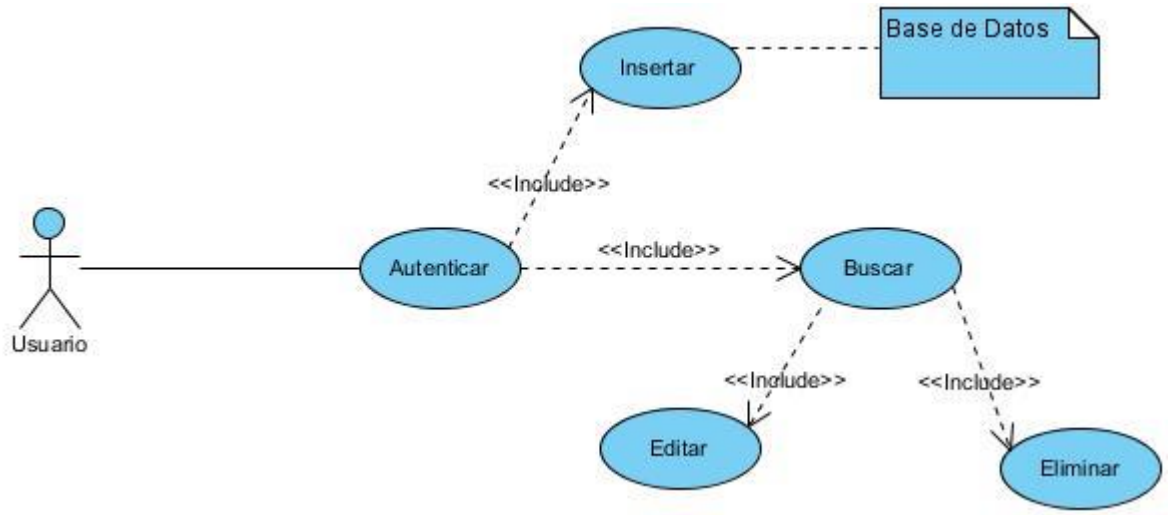


Diagrama de Caso de Uso del Módulo de Control Estadístico del Estado de la Seguridad y la Protección:



Anexo 2.

Diagrama de Gantt.

Representa el cronograma propuesto para el desarrollo de cada etapa del proyecto, por aplicaciones, su despliegue, y el cumplimiento de los plazos establecidos para la puesta en marcha de las soluciones automatizadas.