# UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

## FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

# “SISTEMA DE GESTIÓN DE INCIDENTES DE INFORMACIÓN COMO SOPORTE EN LAS COMUNICACIONES Y OPERACIONES EN LA EMPRESA DIGIWARE”

**TRABAJO DE SUFICIENCIA PROFESIONAL**

Para optar el Título Profesional de

**INGENIERO DE SISTEMAS**

**PRESENTADO POR EL BACHILLER**

MONTENEGRO RAMIREZ, VICTOR ALFREDO

**Villa El Salvador**
**2015**

## DEDICATORIA

A Dios, por permitirme el haber llegado hasta este momento tan importante de mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorar cada día más. A mi madre por ser el pilar más importante y por acompañarme incondicionalmente durante todo mi trayecto estudiantil. A mi padre quien con sus sabios consejos ha sabido guiarme para culminar mi carrera profesional. A mis hermanos que siempre han estado junto a mí brindándome su apoyo.

# AGRADECIMIENTO

Este proyecto no hubiera podido realizarse sin el aporte de todas las personas e instituciones que intervinieron en algún momento sobre el proyecto, y que gracias a su experiencia, interés, dedicación, apoyo y confianza hicieron posible su realización. Por ello tengo que agradecer:

A la Universidad Nacional Tecnológica de Lima Sur, por contribuir en mi formación profesional.

A la empresa Digiware S.A., por la oportunidad de permitirme realizar en su Centro de Operaciones de Seguridad el desarrollo del presente proyecto.

A los asesores, que fueron una valiosa guía y por su dedicación a la realización de la misma.

A mis profesores, gracias por su tiempo, por su apoyo así como por la sabiduría que me trasmitieron en el desarrollo de mi formación profesional.

A mis compañeros, que de alguna forma intervinieron en la realización de este proyecto.

# ÍNDICE

# LISTADO DE FIGURAS

# LISTADO DE TABLAS

# INTRODUCCIÓN

El presente trabajo de investigación lleva por título “Sistema de gestión de incidentes de información como soporte en las comunicaciones y operaciones en la empresa Digiware”.

Digiware es una empresa con más de 18 años de experiencia protegiendo a las organizaciones frente a los retos de seguridad que conlleva los riesgos del crecimiento tecnológico; consientes del enorme reto que tienen las áreas de seguridad de la información hoy en día, las apoya en la definición, implementación y mantenimiento de programas estratégicos de seguridad de la información, que se integren con la estrategia del negocio.

El mundo ha cambiado. Tiempos atrás sustraer un activo de una organización implicaba llevárselo físicamente. Algunos se llevaban material de oficina (folios, grapas, etc.), otros documentos confidenciales originales o fotocopiados.

En la actualidad, los datos y la información que manejan las empresas son activos muy valiosos y no es necesario esconderlos en la chaqueta cuando el jefe no mira para robarlos. La información se puede enviar por correo electrónico, mensajería instantánea, subir a una página de Internet, imprimir o copiar en un dispositivo de almacenamiento USB o de otras maneras inventadas o por inventar.

Por consiguiente, aparecen las herramientas perimetrales de seguridad de la información que permiten monitorear, facilitar y optimizar la administración de los riesgos y el cumplimiento de normativas en organizaciones de cualquier tamaño.

Por otro lado, el Centro de Operaciones de Seguridad (SOC) de la empresa Digiware S.A., se encarga del monitoreo 24x7 de la herramienta perimetral (McAfee ePolicy Orchestrator) notificando los incidentes de pérdida de datos mediante correos electrónicos, el cual, estos no son gestionados adecuadamente ya que la empresa no cuenta con un sistema que facilite a los operadores la ejecución del procedimiento de Prevención de Pérdida de Datos (DLP) y así poder llevar un mejor control y seguimiento de los casos que diariamente se presentan.

Debido a lo planteado, se desarrolla un sistema de gestión de incidentes que permite a los operadores la ejecución del procedimiento de Prevención de Pérdida de Datos, así mismo, notificar y registrar los incidentes de forma eficaz, además de generar reportes mensuales con el status de los casos notificados.

La mejora de las comunicaciones y operaciones permite a la empresa obtener un mejor reconocimiento en el mercado frente a sus competidores en seguridad de la información ya que dicho sistema automatiza el proceso manual que se tiene en la actualidad.

En relación con la estructura con la que se presenta este proyecto, se tiene que la misma está conformada de la siguiente manera:

El Capítulo I Corresponde al planteamiento del problema y contiene la descripción de la realidad problemática, justificación del problema, delimitación del proyecto, formulación del problema y objetivos.

El capítulo II comprende el marco teórico y contiene los antecedentes de la investigación, la teoría relacionada con la investigación y las definiciones técnicas del proyecto.

Finalmente en el capítulo III presenta la parte del desarrollo del sistema así como los resultados obtenidos de la mejora en las comunicaciones y operaciones en la empresa.

# CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

## 1.1 Descripción de la Realidad Problemática

La gestión de los incidentes de seguridad es un aspecto muy importante para lograr el mejoramiento continuo de la seguridad de la información de cualquier compañía, el principal inconveniente es que muchas organizaciones no lo utilizan adecuadamente.

A pesar que la norma ISO 27001 hace mención de este tema como uno de los dominios fundamentales, se le presta más importancia a temas de índole tecnológico dejando de lado los temas de gestión.

Cuando se habla de la gestión de incidentes, la norma hace referencia a recomendaciones relacionadas con la notificación de eventos, procedimientos y responsabilidades que se deberían asignar para la gestión de incidentes y mejoras de seguridad de la información.

Digiware es una empresa Colombiana que se encarga de generar estrategias integrales en seguridad de la información al banco Interbank, el cual, dicha empresa cuenta con Centros de Operaciones de Seguridad de la Información (SOC).

El SOC es el área encargada de ejecutar el Procedimiento de Monitoreo de Incidencias del DLP (Prevención de Pérdida de Datos), el cual, permite realizar un monitoreo ante la incidencia de envío de correos con datos de tarjetas a dominios externos.

Para ello los operadores del SOC monitorean el ePolicy Orchestrator, herramienta que permite detectar los eventos mail por tienda, el cual, muestra la cantidad de correos que son enviados diariamente desde el dominio del banco Interbank hacia las cuentas de dominios externos.

Realizan la validación enviando un correo al jefe directo del colaborador que realizó el envío del correo, el cual, los datos del incidente son obtenidos de la herramienta perimetral de monitoreo, donde son almacenados como evidencia en un archivo Excel que manejan los operadores SOC, luego, proceden a generar los correos de notificación donde extraen nuevamente los datos del incidente desde el archivo Excel presentándose un doble trabajo para los operadores y un mayor tiempo en la ejecución del procedimiento, a su vez, por la cantidad de envíos de correos diarios que se monitorean es complicado llevar un control y seguimiento de los casos, haciéndose evidente una mala calidad de servicio afectando de esta manera la imagen de la institución.

Una vez obtenida la respuesta por parte del jefe directo del colaborador, esta se procede a analizar verificando si el envío de correo con datos de tarjeta al dominio externo forma parte del proceso.

Si el envío de correo con datos de tarjeta al dominio externo no forma parte del proceso de negocio será considerado como una posible fuga de información y el caso será derivado al área de Gobierno y Control de Seguridad de la Información para que definan las acciones a tomar.

Al finalizar el mes, el Jefe de Seguridad de la Información del Banco Interbank, solicita al supervisor del SOC, un informe mensual de todos los casos presentados, estas actividades manuales mencionados anteriormente, perjudican a la institución, en vista que la información registrada puede presentar datos inconsistentes y redundantes, lo cual, ocasiona reportes no del todo objetivo, que a su vez demanda mucho tiempo en su elaboración y por temas de auditoria al no disponer de las evidencias de realización del procedimiento perjudica de forma legal a la institución.

## 1.2 Justificación del Problema

Partiendo de la problemática mencionada anteriormente, se propone la implementación de un sistema de gestión de incidentes para la mejora de las comunicaciones y operaciones en la empresa Digiware.

El presente desarrollo del sistema de gestión, se basa por la necesidad de contar con una plataforma web que facilite la notificación de los eventos de incidencias vía correo electrónico y que a su vez almacene la información de forma rápida, eficaz y accesible las 24 horas del día.

El sistema de gestión de incidentes, ayudará a los operadores SOC a minimizar tiempos de ejecución del procedimiento, llevar un mejor control y seguimiento de los incidentes que se presentan a diario en el monitoreo de DLP (Prevención de Pérdida de Datos). Así mismo, se tendrá disponibilidad de la información en el momento que se requiera, generando informes mensuales que permitirán apoyar temas de auditorías para el beneficio de una mejor calidad de servicio e imagen institucional de la empresa.

## 1.3 Delimitación del Proyecto

### 1.3.1. Espacial.

El presente trabajo se realizó en la empresa Digiware, empresa que brinda el servicio de seguridad de la información al banco “Interbank Sede Camaná” ubicado en Jirón Camaná 545 Lima – Perú.


Figura 1. Interbank Sede Camaná
Fuente: https://www.google.com/maps/place/Interbank+Sede+Camana

### 1.3.2. Temporal.

La presente investigación ha tomado como punto de partida el mes de marzo hasta el mes de octubre del año 2015.

## 1.4 Formulación del Problema

¿En qué medida un sistema de gestión de incidentes mejora las comunicaciones y operaciones de la empresa Digiware?

## 1.5 Objetivos

### 1.5.1. Objetivo General

Realizar un sistema de gestión de incidentes para la mejora de las comunicaciones y operaciones en la empresa Digiware.

### 1.5.2. Objetivos Específicos

a) Analizar el procedimiento de monitoreo de incidentes de prevención de pérdida de datos para mejorar las comunicaciones y operaciones en la empresa Digiware.

b) Diseñar un sistema de gestión de incidentes para mejorar las comunicaciones y operaciones en la empresa Digiware.

c) Establecer los requisitos para la construcción de reportes estadísticos que facilite conocer la situación actual sobre la prevención de pérdida de datos.

# CAPÍTULO II: MARCO TEÓRICO

## 2.1 Antecedentes de la Investigación

### 2.1.1. Internacional

**a)** José, Buenaño Quintana y Marcelo Alfonso, Granda Luces (2009), **"*Planeación y Diseño de un Sistema de Gestión de seguridad de la Información basado en la norma ISO/IEC 27001 – 27002*"**, Universidad Politécnica Salesiana, Guayaquil – Ecuador.

Los autores en referencia, en su tesis demostraron, que al encontrar un mecanismo que logre regularizar, gestionar y mitigar al máximo los riesgos actuales por el uso de la información le será posible a la institución controlar las amenazas actuales en los sistemas informáticos.[1]

[1] José, Buenaño Quintana y Marcelo Alfonso, Granda Luces (2009, Pág. 8), "Planeación y Diseño de un Sistema de Gestión de seguridad de la Información basado en la norma ISO/IEC 27001 – 27002", Universidad Politécnica Salesiana, Guayaquil – Ecuador.

Al evaluar lo puntos más críticos que se ha venido presentando con el avance de la tecnología, se logra obtener resultados positivos, citando algunos de estos como la calidad de servicio brindados por la institución y el servicio de mensajería, que al no obtener una política que regularice el uso de estos servicios, es considerado como un factor grave y perjudicial a la calidad de servicio y esta repercutirá en los controles de la seguridad de la información.[2]

El adecuado manejo de una política documentada ayudará a futuros procesos de auditoria a saber los orígenes de cada uno de los cambios, como también a identificar posibles omisiones a la seguridad que se han originados con el transcurso y avance de la tecnología.

**b)** Arnaldo José, Añez Araujo y Marco Antonio, Rodríguez Henríquez (2011) "***Implantación de un sistema de gestión de incidencias para la empresa Servicios Fv Venezuela 2010***", Universidad Nueva Esparta, Caracas – Venezuela.

En la presente tesis los autores plantean como objetivo, en la investigación, desarrollar e implantar un sistema que ayudará a la empresa a automatizar el proceso de recepción, gestión y entrega de equipos, facilitando así el registro de datos de sus clientes y el monitoreo de los equipos que ingresan al taller.

[2] José, Buenaño Quintana y Marcelo Alfonso, Granda Luces (2009, Pág. 186), "Planeación y Diseño de un Sistema de Gestión de seguridad de la Información basado en la norma ISO/IEC 27001 – 27002", Universidad Politécnica Salesiana, Guayaquil – Ecuador.

Asimismo, el desarrollo de este proyecto se realizó bajo los lineamientos de la metodología RUP (Rational Unified Process); y para la construcción del sistema, se utilizó PHP como lenguaje de programación y PostgreSQL como manejador de base de datos relacional.

Dicho sistema representa un aporte fundamenta, puesto que se logró interconectar a las 3 sedes que posee la empresa en el país, facilitando el acceso a sus usuarios a través de internet. Permitiendo así, a los usuarios manejar con mayor velocidad la información requerida, ya sea por el cliente o por la misma empresa.

Con esta implantación, la empresa alcanzó un posicionamiento más alto entre las otras empresas que se dedican a ofrecer tales servicios, obteniendo mejores reconocimientos, rentabilidad y mucha mayor lealtad de parte de sus clientes debido a la gran eficacia.[3]

### 2.1.2. Nacional

**a)** Vilma Crist, Palli Apaza (2014), "***Modelo de gestión de incidencias basado en ITIL para reducir el tiempo de diagnóstico de incidentes del servicio de soporte técnico en la Universidad Nacional del Altiplano Puno - 2014***" Universidad Nacional del Altiplano, Puno – Perú.

[3] Arnaldo José, Añez Araujo y Marco Antonio, Rodríguez Henríquez (2011, Pág. 18) "Implantación de un sistema de gestión de incidencias para la empresa Servicios Fv Venezuela 2010", Universidad Nueva Esparta, Caracas – Venezuela.

El autor en su tesis, tiene como objetivo general desarrollar un modelo de gestión de incidencias basado en ITIL, para reducir el tiempo de diagnóstico de incidentes. El manejo inadecuado de la gestión de incidencias ocasiona tiempos largos para su diagnóstico, según registro de trámite documentario.

Es necesario mejorar el actual proceso de gestión de incidencias estandarizando según el modelo propuesto por ITIL, para ello, se realizaron las pruebas correspondientes y teniendo ya los datos recopilados a través de fichas de observación se aplicó una prueba de entrada (Pre-test) y una prueba de salida (Pos-test).

Los resultados obtenidos fueron claros al mostrar una reducción de 59 198 minutos de tiempo promedio de diagnóstico de incidentes sin modelo a 457 minutos de tiempo promedio de diagnóstico de incidentes con modelo. Finalmente una vez realizada la prueba de hipótesis, a través de los resultados de las fichas de observación se muestra empíricamente y estadísticamente, que el desarrollo de un Modelo de gestión de incidencias basado en ITIL, reduce en un 77% el tiempo de diagnóstico de incidencias del servicio de soporte técnico en la Universidad.[4]

[4] Vilma Crist, Palli Apaza (2014, Pág. 10), "Modelo de gestión de incidencias basado en ITIL para reducir el tiempo de diagnóstico de incidentes del servicio de soporte técnico en la Universidad Nacional del Altiplano Puno - 2014" Universidad Nacional del Altiplano, Puno – Perú.

## 2.2 Bases Teóricas

### 2.2.1. RUP

En el proyecto de investigación titulado “Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de Proceso Unificado Racional (RUP)” (2010), menciona resumidamente los fundamentos de la metodología RUP.

El Proceso Unificado Racional (Rational Unified Process en inglés, habitualmente resumido como RUP) es un proceso de desarrollo de software y junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.

El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización. También se conoce por este nombre al software desarrollado por Rational, hoy propiedad de IBM, el cual incluye información entrelazada de diversos artefactos y descripciones de las diversas actividades. Está incluido en el Rational Method Composer (RMC), que permite la personalización de acuerdo a necesidades.[5]

[5] Serna Barrera Juan Alberto. (2010, Pág. 2), “Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)”.

Originalmente se diseñó un proceso genérico y de dominio público, el Proceso Unificado, y una especificación más detallada, el Rational Unified Process, que se vendiera como producto independiente.

**a) Historia de la metodología RUP.**

La Figura 2 ilustra la historia de RUP. El antecedente más importante se ubica en 1967 con la Metodología Ericsson (Ericsson Approach) elaborada por Ivar Jacobson, una aproximación de desarrollo basada en componentes, que introdujo el concepto de Caso de Uso. Entre los años de 1987 a 1995 Jacobson fundó la compañía Objectory AB y lanza el proceso de desarrollo Objectory (abreviación de Object Factory).[6]

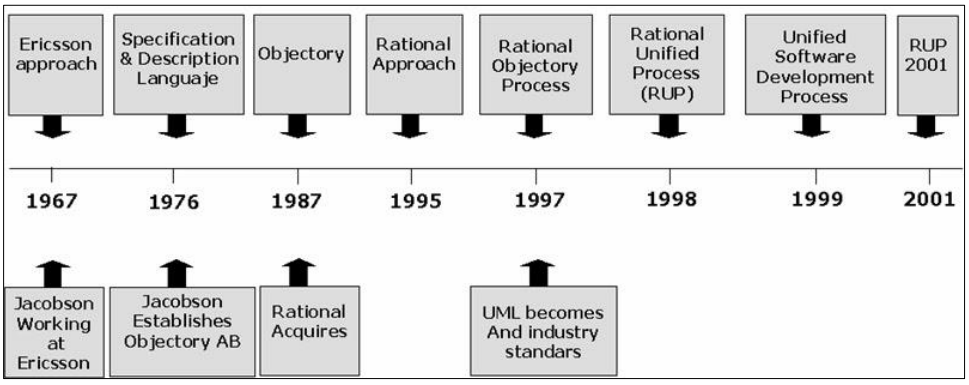



Figura 2. Historia de RUP
Fuente: http://soyanalista2011.blogspot.pe/

[6] Serna Barrera Juan Alberto. (2010, Pág. 2), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Posteriormente en 1995 Rational Software Corporation adquiere Objectory AB y entre 1995 y 1997 se desarrolla Rational Objectory Process (ROP) a partir de Objectory 3.8 y del Enfoque Rational (Rational Approach) adoptando UML como lenguaje de modelado.

Desde ese entonces y a la cabeza de Grady Booch, Ivar Jacobson y James Rumbaugh, Rational Software desarrolló e incorporó diversos elementos para expandir ROP, destacándose especialmente el flujo de trabajo conocido como modelado del negocio. En junio del 1998 se lanza Rational Unified Process.

**b) Características esenciales del RUP.**

Los autores de RUP destacan que el proceso de software propuesto por RUP tiene tres características esenciales: está dirigido por los Casos de Uso, está centrado en la arquitectura, y es iterativo e incremental.[7]

- **Proceso dirigido por Casos de Uso.-** Los Casos de Uso son una técnica de captura de requisitos que fuerza a pensar en términos de importancia para el usuario y no sólo en términos de funciones que sería bueno contemplar. Se define un Caso de Uso como un fragmento de funcionalidad del sistema que proporciona al usuario un valor añadido. Los Casos de Uso representan los requisitos funcionales del sistema.

[7] Serna Barrera Juan Alberto. (2010, Pág. 3), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

En RUP los Casos de Uso no son sólo una herramienta para especificar los requisitos del sistema. También guían su diseño, implementación y prueba. Los Casos de Uso constituyen un elemento integrador y una guía del trabajo como se muestra en la Figura 3.

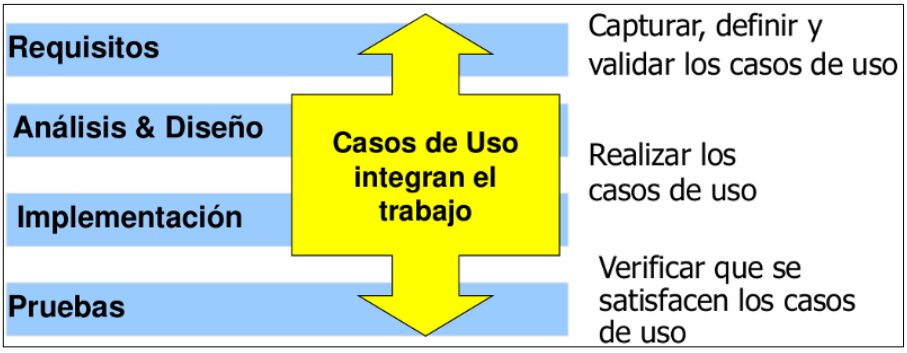



Figura 3. Los Casos de Uso integran el trabajo.
Fuente: http://ttps-ruby.github.io/capacitacion-ruby-ttps/file/01-agiles/08-rup-casos-de-uso.png

Los Casos de Uso no sólo inician el proceso de desarrollo sino que proporcionan un hilo conductor, permitiendo establecer trazabilidad entre los artefactos que son generados en las diferentes actividades del proceso de desarrollo.[8]

Como se muestra en la Figura 4, basándose en los Casos de Uso se crean los modelos de análisis y diseño, luego la implementación que los lleva a cabo, y se verifica que efectivamente el producto implemente adecuadamente cada Caso de Uso. Todos los modelos deben estar sincronizados con el modelo de Casos de Uso.

[8] Serna Barrera Juan Alberto. (2010, Pág. 3), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

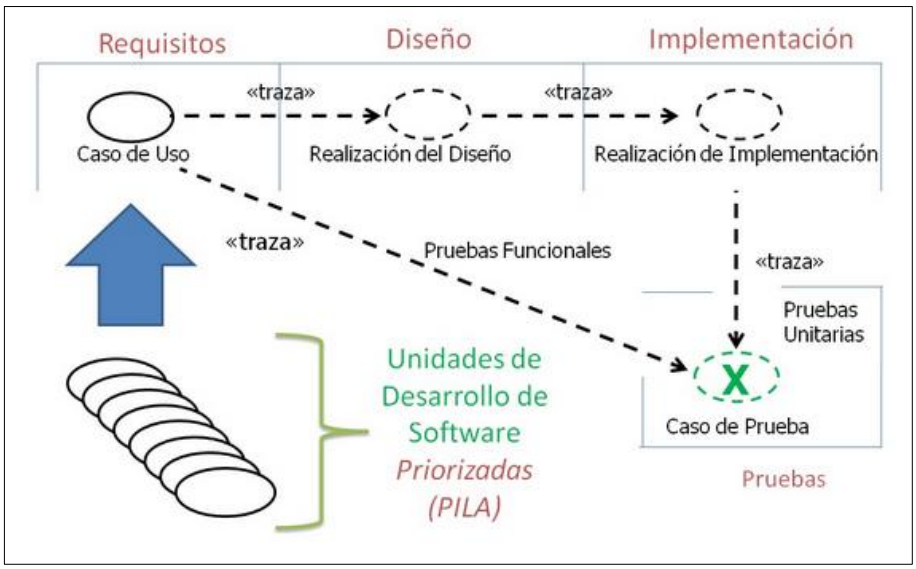



Figura 4. Flujo a partir de los Casos de Uso
Fuente: http://escritura.proyectolatin.org/gestion-de-proyectos-de-software/ejemplos-de-procesos/

- **Proceso centrado en la arquitectura.-** La arquitectura de un sistema es la organización o estructura de sus partes más relevantes, lo que permite tener una visión común entre todos los involucrados (desarrolladores y usuarios) y una perspectiva clara del sistema completo, necesaria para controlar el desarrollo.[9]

  La arquitectura involucra los aspectos estáticos y dinámicos más significativos del sistema, está relacionada con la toma de decisiones que indican cómo tiene que ser construido el sistema y ayuda a determinar en qué orden.

[9] Serna Barrera Juan Alberto. (2010, Pág. 4), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Además la definición de la arquitectura debe tomar en consideración elementos de calidad del sistema, rendimiento, reutilización y capacidad de evolución por lo que debe ser flexible durante todo el proceso de desarrollo.

La arquitectura se ve influenciada por la plataforma software, sistema operativo, gestor de bases de datos, protocolos, consideraciones de desarrollo como sistemas heredados. Muchas de estas restricciones constituyen requisitos no funcionales del sistema.

En el caso de RUP además de utilizar los Casos de Uso para guiar el proceso se presta especial atención al establecimiento temprano de una buena arquitectura que no se vea fuertemente impactada ante cambios posteriores durante la construcción y el mantenimiento.[10]

Cada producto (documento, modelo, elemento del modelo) tiene tanto una función como una forma. La función corresponde a la funcionalidad reflejada en los Casos de Uso y la forma la proporciona la arquitectura. Existe una interacción entre los Casos de Uso y la arquitectura, los Casos de Uso deben encajar en la arquitectura cuando se llevan a cabo y la arquitectura debe permitir el desarrollo de todos los Casos de Uso requeridos, actualmente y en el futuro.

[10] Serna Barrera Juan Alberto. (2010, Pág. 4), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Esto provoca que tanto arquitectura como Casos de Uso deban evolucionar en paralelo durante todo el proceso de desarrollo de software.

En la Figura 5 se ilustra la evolución de la arquitectura durante las fases de RUP. Esta arquitectura, es una implementación parcial del sistema, construida para demostrar algunas funciones y propiedades.

RUP establece refinamientos sucesivos de una arquitectura ejecutable, construida como un prototipo evolutivo.[11]

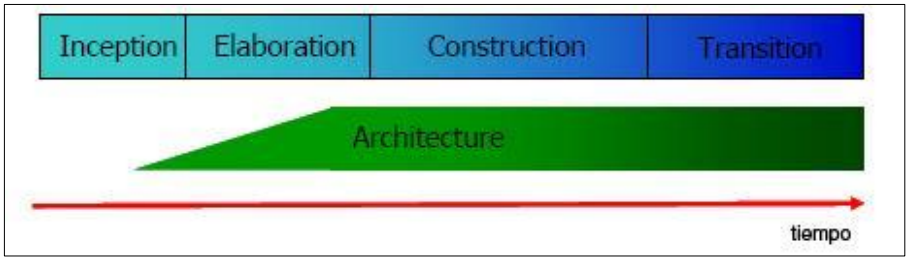



Figura 5. Evolución de la arquitectura del sistema.
Fuente: http://gestionrrhhusm.blogspot.pe/2011/05/modelo-rup-rational-unified-process-o.html

- **Proceso iterativo e incremental.-** El equilibrio correcto entre los Casos de Uso y la arquitectura es algo muy parecido al equilibrio de la forma y la función en el desarrollo del producto, lo cual se consigue con el tiempo.

[11] Serna Barrera Juan Alberto. (2010, Pág. 4), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Para esto, la estrategia que se propone en RUP es tener un proceso iterativo e incremental en donde el trabajo se divide en partes más pequeñas o mini proyectos. Permitiendo que el equilibrio entre Casos de Uso y arquitectura se vaya logrando durante cada mini proyecto, así durante todo el proceso de desarrollo.

Cada mini proyecto se puede ver como una iteración (un recorrido más o menos completo a lo largo de todos los flujos de trabajo fundamentales) del cual se obtiene un incremento que produce un crecimiento en el producto.

Una iteración puede realizarse por medio de una cascada de etapas como se muestra en la Figura 6. Se pasa por los flujos fundamentales (Requisitos, Análisis, Diseño, Implementación y Pruebas), también existe una planificación de la iteración, un análisis de la iteración y algunas actividades específicas de la iteración. Al finalizar se realiza una integración de los resultados con lo obtenido de las iteraciones anteriores.[12]

[12] Serna Barrera Juan Alberto. (2010, Pág. 5), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

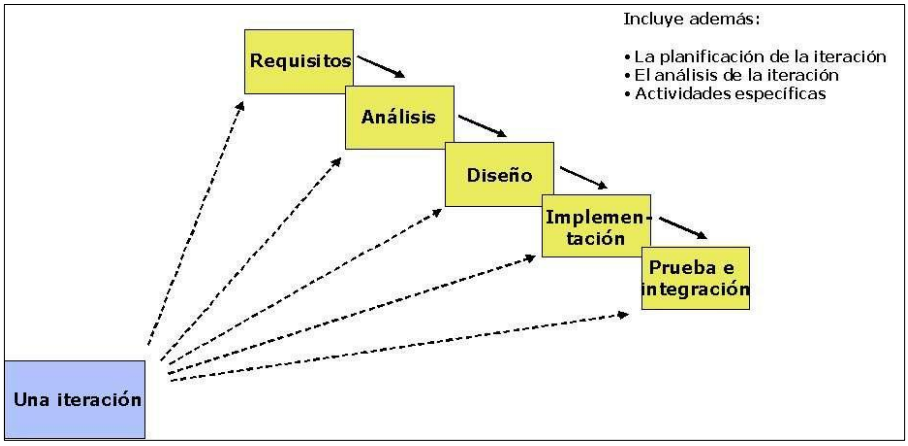



Figura 6. Una iteración RUP
Fuente: http://gestionrrhhusm.blogspot.pe/2011/05/modelo-rup-rational-unified-process-o.html

El proceso iterativo e incremental consta de una secuencia de iteraciones. Cada iteración aborda una parte de la funcionalidad total, pasando por todos los flujos de trabajo relevantes y refinando la arquitectura. Cada iteración se analiza cuando termina. Se puede determinar si han aparecido nuevos requisitos o han cambiado los existentes, afectando a las iteraciones siguientes. Durante la planificación de los detalles de la siguiente iteración, el equipo también examina cómo afectarán los riesgos que aún quedan al trabajo en curso. Toda la retroalimentación de la iteración pasada permite reajustar los objetivos para las siguientes iteraciones. Se continúa con esta dinámica hasta que se haya finalizado por completo con la versión actual del producto.[13]

[13] Serna Barrera Juan Alberto. (2010, Pág. 5), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

**c) El RUP está basado en 3 principios clave, estos son:**

- **Adaptar el proceso.-** El proceso deberá adaptarse a las características propias del proyecto u organización. El tamaño del mismo, así como su tipo o las regulaciones que lo condicionen, influirán en su diseño específico. También se deberá tener en cuenta el alcance del proyecto.[14]

- **Equilibrar prioridades.-** Los requerimientos de los diversos participantes pueden ser diferentes, contradictorios o disputarse recursos limitados. Debe encontrarse un equilibrio que satisfaga los deseos de todos. Gracias a este equilibrio se podrán corregir desacuerdos que surjan en el futuro.

- **Demostrar valor iterativamente.-** Los proyectos se entregan, aunque sea de un modo interno, en etapas iteradas. En cada iteración se analiza la opinión de los inversores, la estabilidad y calidad del producto, y se refina la dirección del proyecto así como también los riesgos involucrados.

**d) Ciclo de vida RUP**

El ciclo de vida RUP es una implementación del Desarrollo en espiral.

[14] Serna Barrera Juan Alberto. (2010, Pág. 7), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Fue creado ensamblando los elementos en secuencias semi-ordenadas. El ciclo de vida organiza las tareas en fases e iteraciones.[15]

RUP divide el proceso en cuatro fases, dentro de las cuales se realizan varias iteraciones en número variable según el proyecto y en las que se hace un mayor o menor hincapié en las distintas actividades. En la Figura 7 muestra cómo varía el esfuerzo asociado a las disciplinas según la fase en la que se encuentre el proyecto RUP.

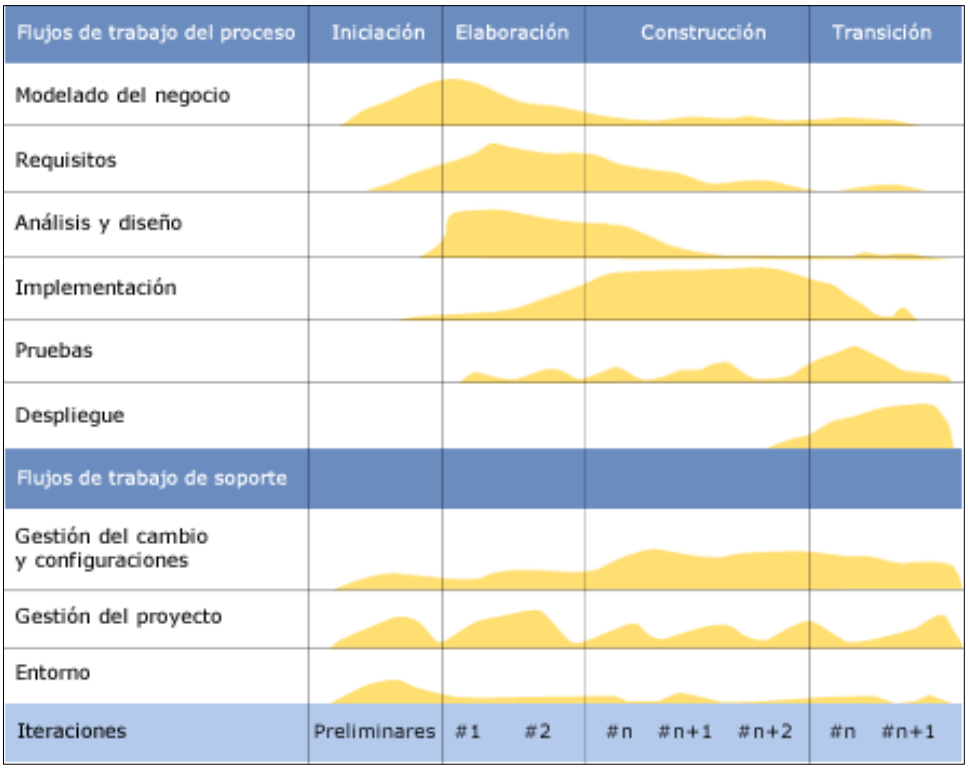



Figura 7. Ciclo de vida RUP
Fuente: https://jummp.wordpress.com/2011/04/06/desarrollo-de-software-ciclo-de-vida-rup-rational-unified-process/

[15] Serna Barrera Juan Alberto. (2010, Pág. 7), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Las primeras iteraciones (en las fases de Inicio y Elaboración) se enfocan hacia la comprensión del problema y la tecnología, la delimitación del ámbito del proyecto, la eliminación de los riesgos críticos, y al establecimiento de una primera aproximación o línea base de la arquitectura.[16]

Durante la fase de inicio las iteraciones hacen mayor énfasis en actividades de modelado del negocio y de requerimientos.

En la fase de elaboración, las iteraciones se orientan al desarrollo de la línea base de la arquitectura, abarcan más los flujos de trabajo de requerimientos, modelo de negocios (refinamiento), análisis, diseño y una parte de implementación orientado a la línea base de la arquitectura.

En la fase de construcción, se lleva a cabo la construcción del producto por medio de una serie de iteraciones (implementación, pruebas y muestra del sistema).

Para cada iteración se selecciona algunos Casos de Uso, se refina su análisis y diseño y se procede a su implementación y pruebas. Se realiza una pequeña cascada para cada ciclo. Se realizan tantas iteraciones hasta que se termine la implementación deseada de la nueva versión del producto.

[16] Serna Barrera Juan Alberto. (2010, Pág. 8), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

En la fase de transición se pretende garantizar que se tiene un producto preparado para su entrega a la comunidad de usuarios con el fin de que la prueben.

Como se puede observar en cada fase participan todas las disciplinas, pero que dependiendo de la fase el esfuerzo dedicado a una disciplina o actividad varía.

**e) Otras prácticas**

RUP identifica 6 prácticas deseables con las que define una forma efectiva de trabajar para los equipos de desarrollo de software.[17]

- **Gestión de requisitos.-** RUP brinda una guía para encontrar, organizar, documentar, y seguir los cambios de los requisitos funcionales y restricciones. Utiliza una notación de Caso de Uso y escenarios para representar los requisitos.

- **Desarrollo de software iterativo.-** Desarrollo del producto mediante iteraciones con hitos bien definidos, en las cuales se repiten las actividades pero con distinto énfasis, según la fase del proyecto.

[17] Serna Barrera Juan Alberto. (2010, Pág. 8), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

- **Desarrollo basado en componentes.-** La creación de sistemas intensivos en software requiere dividir el sistema en componentes con interfaces bien definidas, que posteriormente serán ensamblados para generar el sistema. Esta característica en un proceso de desarrollo permite que el sistema se vaya creando a medida que se obtienen o se desarrollan sus componentes.[18]

- **Modelado visual (usando UML).-** UML es un lenguaje para visualizar, especificar, construir y documentar los artefactos de un sistema software. Es un estándar de la OMG (http://www.omg.org). Utilizar herramientas de modelado visual facilita la gestión de dichos modelos, permitiendo ocultar o exponer detalles cuando sea necesario. El modelado visual también ayuda a mantener la consistencia entre los artefactos del sistema: requisitos, diseños e implementaciones. En resumen, el modelado visual ayuda a mejorar la capacidad del equipo para gestionar la complejidad del software.

- **Verificación continúa de la calidad.-** Es importante que la calidad de todos los artefactos se evalúe en varios puntos durante el proceso de desarrollo, especialmente al final de cada iteración.

[18] Serna Barrera Juan Alberto. (2010, Pág. 8), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

En esta verificación las pruebas juegan un papel fundamental y se integran a lo largo de todo el proceso. Para todos los artefactos no ejecutables las revisiones e inspecciones también deben ser continuas.

- **Gestión de los cambios.-** Los cambios son un factor de riesgo crítico en los proyectos de software. Los artefactos de software cambian no sólo debido a acciones de mantenimiento posteriores a la entrega del producto, sino que durante el proceso de desarrollo, especialmente importantes por su posible impacto son los cambios en los requisitos.[19]

Por otra parte, otro gran desafío que debe abordarse es la construcción de software con la participación de múltiples desarrolladores, posiblemente distribuidos geográficamente, trabajando a la vez en una entrega y quizás en distintas plataformas.

La ausencia de una disciplina rápidamente conduciría al caos. La Gestión de Cambios y de Configuración es la disciplina de RUP encargada de este aspecto.

[19] Serna Barrera Juan Alberto. (2010, Pág. 9), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

### f) Estructura del proceso

El proceso puede ser descrito en dos dimensiones o ejes.

- **Eje horizontal.-** Representa el tiempo y es considerado el eje de los aspectos dinámicos del proceso. Indica las características del ciclo de vida del proceso expresado en términos de fases, iteraciones e hitos. Se puede observar en la Figura 8 que RUP consta de cuatro fases: Inicio, Elaboración, Construcción y Transición. Como se mencionó anteriormente cada fase se subdivide a la vez en iteraciones.

- **Eje vertical.-** Representa los aspectos estáticos del proceso. Describe el proceso en términos de componentes de proceso, disciplinas, flujos de trabajo, actividades, artefactos y roles.[20]

[20] Serna Barrera Juan Alberto. (2010, Pág. 9), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

Los casos de uso integran el flujo o las actividades.

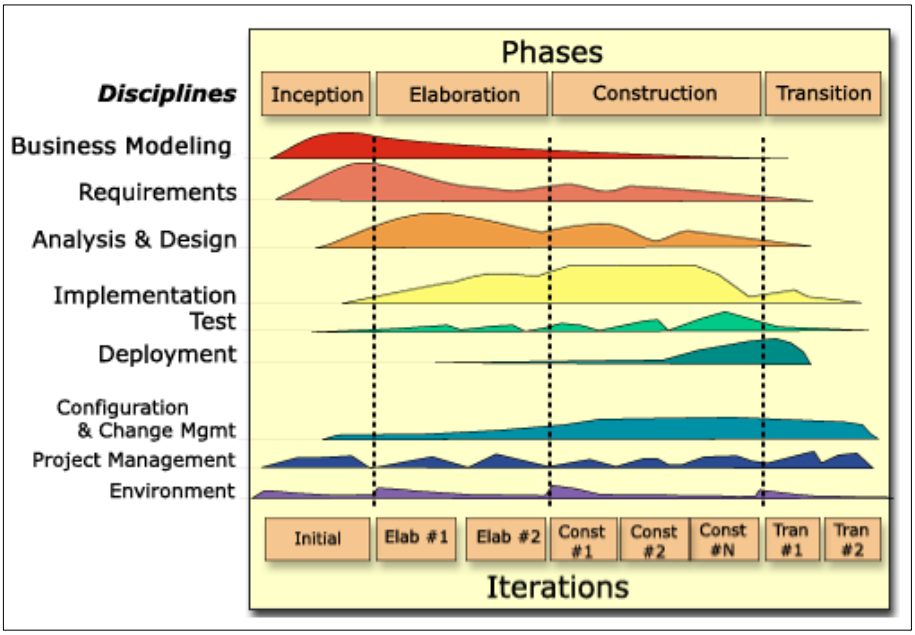



Figura 8. Estructura de RUP
Fuente: http://sce.uhcl.edu/helm/rationalunifiedprocess/

## g) Estructura Dinámica del proceso. Fases e iteraciones

RUP se repite a lo largo de una serie de ciclos que constituyen la vida de un producto. Cada ciclo concluye con una generación del producto para los clientes. Cada ciclo consta de cuatro fases: Inicio, Elaboración, Construcción y Transición. Cada fase se subdivide a la vez en iteraciones, el número de iteraciones en cada fase es variable.[21]

[21] Serna Barrera Juan Alberto. (2010, Pág. 10), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

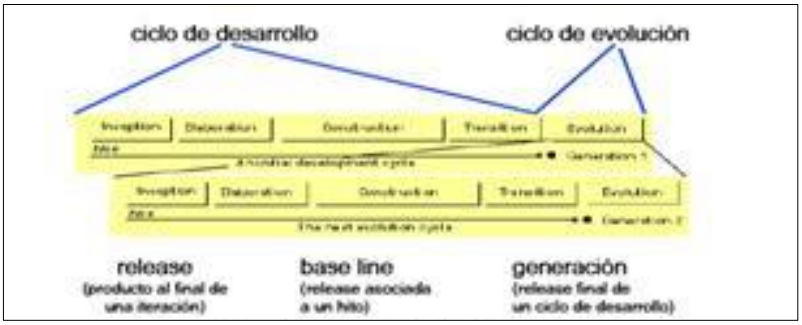



Figura 9. Ciclos, Releases, Base line.
Fuente: http://gestionrrhhusm.blogspot.pe/2011/05/modelo-rup-rational-unified-process-o.html

Cada fase se concluye con un hito (entregable) bien definido, un punto en el tiempo en el cual se deben tomar ciertas decisiones críticas y alcanzar las metas clave antes de pasar a la siguiente fase, ese hito principal de cada fase se compone de hitos menores que podrían ser los criterios aplicables a cada iteración. Los hitos para cada una de las fases son: Inicio - Lifecycle Objectives, Elaboración - Lifecycle Architecture, Construcción - Initial Operational Capability, Transición - Product Release. Las fases y sus respectivos hitos se ilustran en la Figura 10.[22]

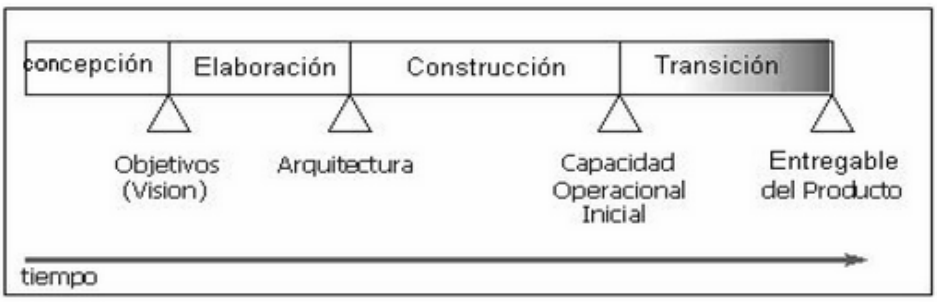



Figura 10. Fases e Hitos en RUP
Fuente: http://lacuevadelasabiduria.blogspot.pe/

[22] Serna Barrera Juan Alberto. (2010, Pág. 10), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

La duración y esfuerzo dedicado en cada fase es variable dependiendo de las características del proyecto. Sin embargo, la Figura 11 ilustra porcentajes frecuentes al respecto. Consecuente con el esfuerzo señalado, la Figura 12 ilustra una distribución típica de recursos humanos necesarios a lo largo del proyecto.[23]

| | Concepción | Elaboración | Construcción | Transición |
|---|---|---|---|---|
| Esfuerzo | ~5 % | 20 % | 65 % | 10% |
| Horario | 10 % | 30 % | 50 % | 10% |

Figura 11. Distribución típica de esfuerzo y tiempo.
Fuente: http://lacuevadelasabiduria.blogspot.pe/

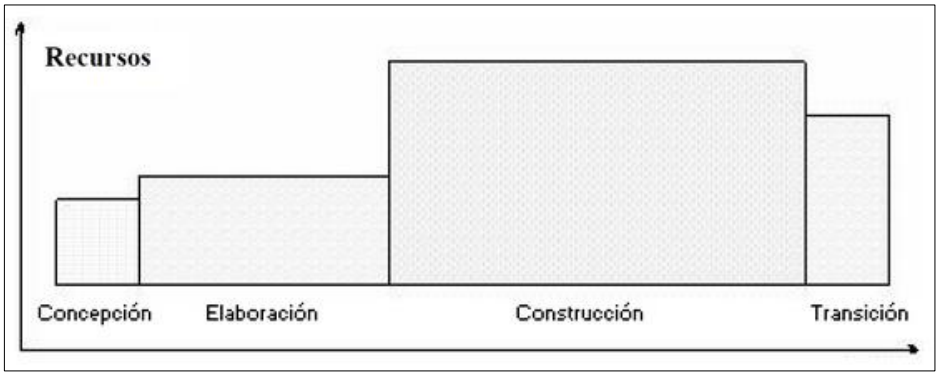



Figura 12. Distribución típica de recursos humanos.
Fuente: http://lacuevadelasabiduria.blogspot.pe/

[23] Serna Barrera Juan Alberto. (2010, Pág. 10), "Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".

### 2.2.2. UML

Según los autores Xavier Ferré Grau y María Isabel Sánchez Segura, en su trabajo de investigación titulado “Desarrollo Orientado a Objetos con UML” (2011), menciona resumidamente que UML (Unified Modeling Language) es un lenguaje que permite modelar, construir y documentar los elementos que forman un sistema software orientado a objetos.

El UML se ha convertido en el estándar de facto de la industria, debido a que ha sido concebido por los autores de los tres métodos más usados de orientación a objetos: Grady Booch, Ivar Jacobson y Jim Rumbaugh. Estos autores fueron contratados por la empresa Rational Software Co. para crear una notación unificada en la que basar la construcción de sus herramientas CASE. En el proceso de creación de UML han participado, no obstante, otras empresas de gran peso en la industria como Microsoft, Hewlett - Packard, Oracle o IBM, así como grupos de analistas y desarrolladores.[24]

Esta notación ha sido ampliamente aceptada debido al prestigio de sus creadores y debido a que incorpora las principales ventajas de cada uno de los métodos particulares en los que se basa: Booch, OMT y OOSE.

[24] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 1),”Desarrollo Orientado a Objetos con UML”.

UML ha puesto fin a las llamadas “guerras de métodos” que se han mantenido a lo largo de los 90, en las que los principales métodos sacaban nuevas versiones que incorporaban las técnicas de los demás. Con UML se fusiona la notación de estas técnicas para formar una herramienta compartida entre todos los ingenieros software que trabajan en el desarrollo orientado a objetos.

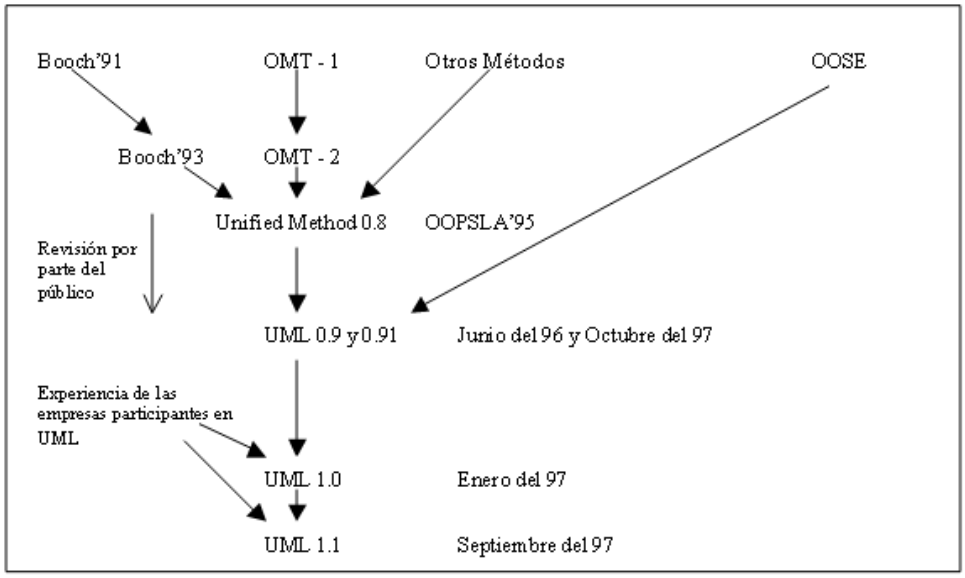



Figura 13. Historia del UML.
Fuente: http://www.uv.mx/personal/maymendez/files/2011/05/umlTotal.pdf

El objetivo principal cuando se empezó a gestar UML era posibilitar el intercambio de modelos entre las distintas herramientas CASE orientadas a objetos del mercado. Para ello era necesario definir una notación y semántica común.[25]

[25] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 2),”Desarrollo Orientado a Objetos con UML”.

## a) Diagrama de Estructura Estática

Con el nombre de Diagramas de Estructura Estática se engloba tanto al Modelo Conceptual de la fase de Análisis como al Diagrama de Clases de la fase de diseño. Ambos son distintos conceptualmente, mientras el primero modela elementos del dominio el segundo presenta los elementos de la solución software.

Sin embargo, ambos comparten la misma notación para los elementos que los forman (clases y objetos) y las relaciones que existen entre los mismos (asociaciones).[26]

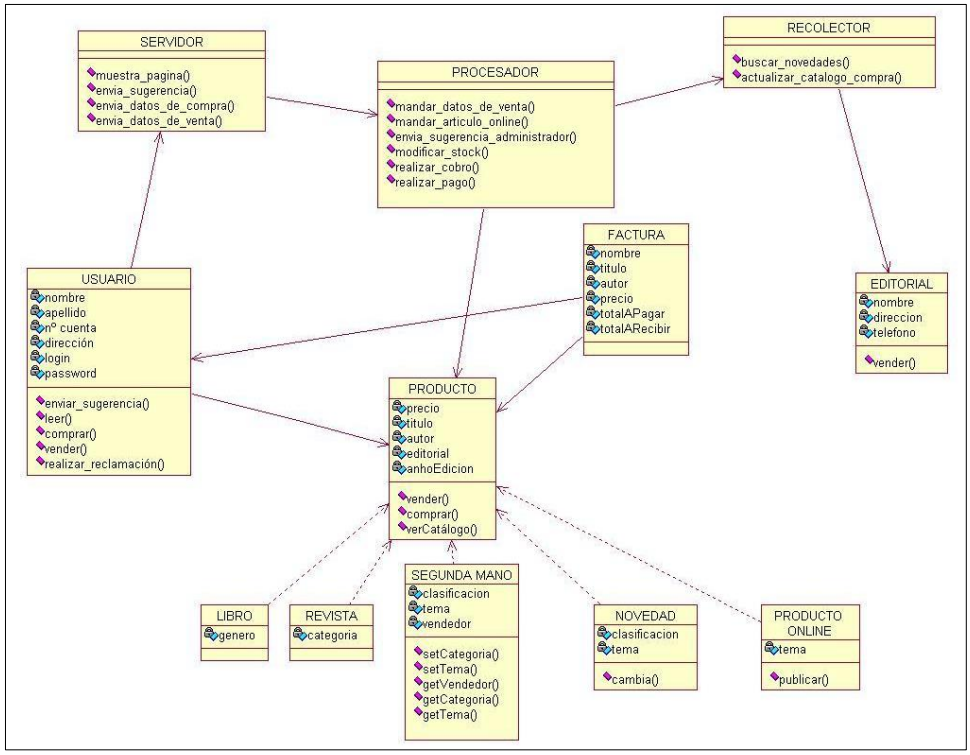



Figura 14. Diagrama de Clases.
Fuente: https://onlineshop09.wordpress.com/nuestro-proyecto/diagrama-de-clases/

[26] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 4),"Desarrollo Orientado a Objetos con UML".

### b) Diagrama de caso de uso

Un Diagrama de Casos de Uso muestra la relación entre los actores y los casos de uso del sistema. Representa la funcionalidad que ofrece el sistema en lo que se refiere a su interacción externa.

- **Elementos.-** Los elementos que pueden aparecer en un Diagrama de Casos de Uso son: actores, casos de uso y relaciones entre casos de uso.

- **Actores.-** Un actor es una entidad externa al sistema que realiza algún tipo de interacción con el mismo. Se representa mediante una figura humana dibujada con palotes. Esta representación sirve tanto para actores que son personas como para otro tipo de actores (otros sistemas, sensores, etc.).

- **Casos de uso.-** Un caso de uso es una descripción de la secuencia de interacciones que se producen entre un actor y el sistema, cuando el actor usa el sistema para llevar a cabo una tarea específica. Expresa una unidad coherente de funcionalidad, y se representa en el Diagrama de Casos de Uso mediante una elipse con el nombre del caso de uso en su interior.

  El nombre del caso de uso debe reflejar la tarea específica que el actor desea llevar a cabo usando el sistema.[27]

[27] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 9),"Desarrollo Orientado a Objetos con UML".

- **Relaciones entre Casos de Uso.-** Entre dos casos de uso puede haber las siguientes relaciones:

  - **Extiende:** Cuando un caso de uso especializa a otro extendiendo su funcionalidad.

  - **Usa:** Cuando un caso de uso utiliza a otro.

  Se representan como una línea que une a los dos casos de uso relacionados, con una flecha en forma de triángulo y con una etiqueta <<extiende>> o <<usa>> según sea el tipo de relación.

  En el diagrama de casos de uso se representa también el sistema como una caja rectangular con el nombre en su interior. Los casos de uso están en el interior de la caja del sistema, y los actores fuera, y cada actor está unido a los casos de uso en los que participa mediante una línea. En la Figura 15 se muestra un ejemplo de Diagrama de Casos de Uso para un cajero automático.[28]

[28] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 10),"Desarrollo Orientado a Objetos con UML".

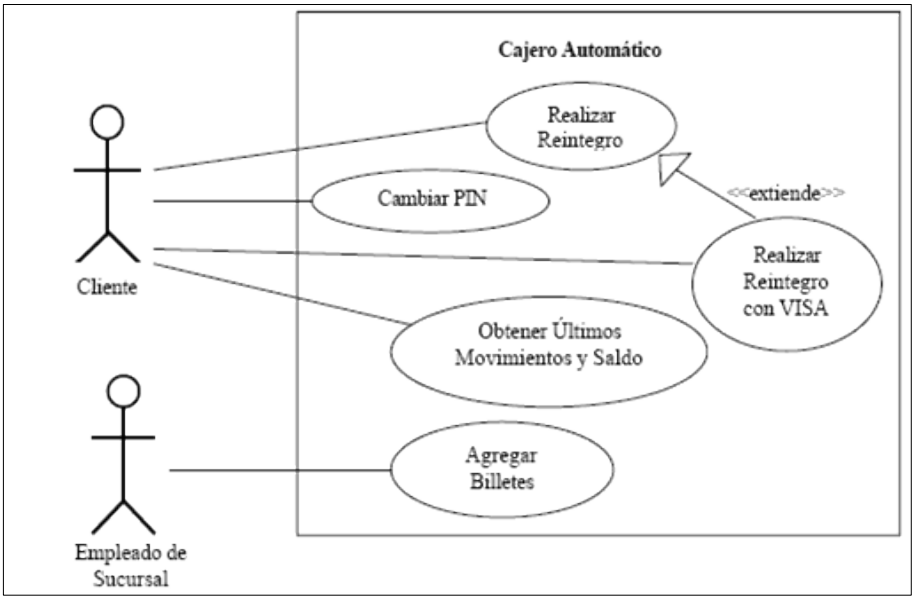



Figura 15. Diagrama de Caso de Uso.
Fuente: http://www.geocities.ws/rescala29/fase2/t1/t1_pregunta02.html

### c) Diagrama de secuencia

Un diagrama de Secuencia muestra una interacción ordenada según la secuencia temporal de eventos.

En particular, muestra los objetos participantes en la interacción y los mensajes que intercambian ordenados según su secuencia en el tiempo.

El eje vertical representa el tiempo, y en el eje horizontal se colocan los objetos y actores participantes en la interacción, sin un orden prefijado. Cada objeto o actor tiene una línea vertical, y los mensajes se representan mediante flechas entre los distintos objetos. El tiempo fluye de arriba abajo.[29]

[29] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 10),"Desarrollo Orientado a Objetos con UML".

Se pueden colocar etiquetas (como restricciones de tiempo, descripciones de acciones, etc.) bien en el margen izquierdo o bien junto a las transiciones o activaciones a las que se refieren.

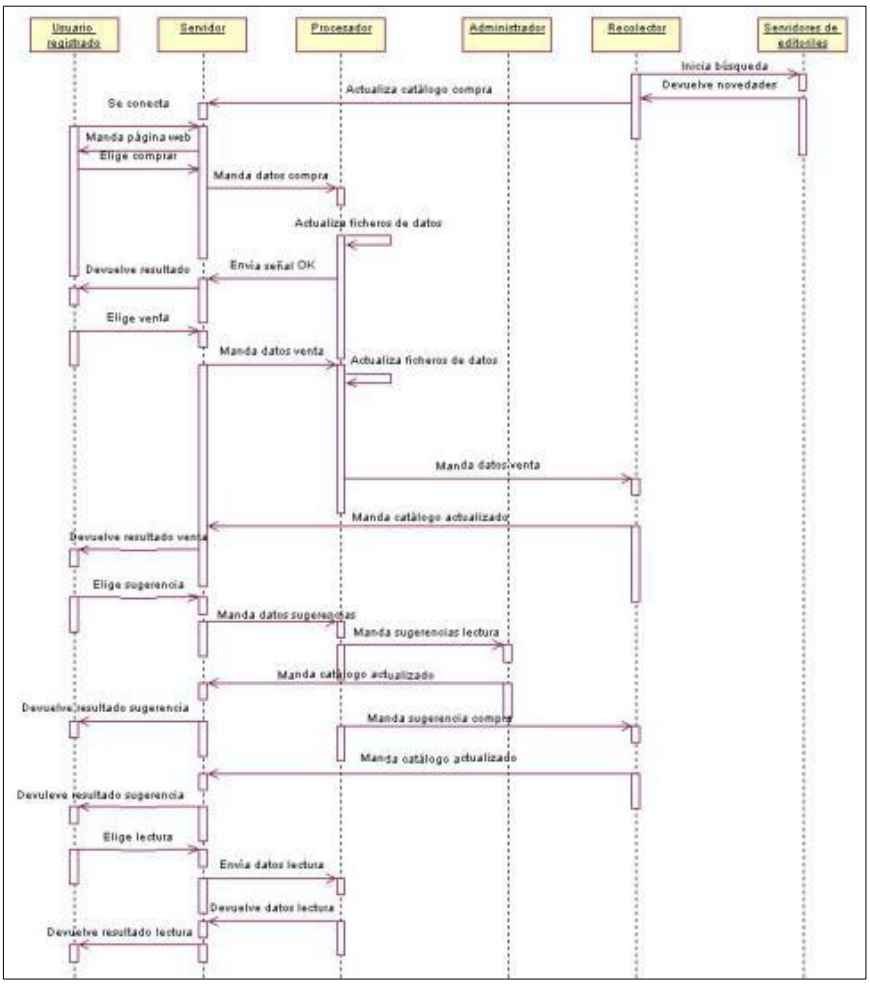



Figura 16. Diagrama de Secuencia.
Fuente: http://www.geocities.ws/rescala29/fase2/t1/t1_pregunta02.html

### d) Diagrama de actividades

El diagrama de actividades sirve para representar el sistema desde otra perspectiva, y de este modo complementa a los anteriores diagramas vistos. Gráficamente un diagrama de actividades será un conjunto de arcos y nodos.[30]

[30] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 14),"Desarrollo Orientado a Objetos con UML".

Desde un punto de vista conceptual, el diagrama de actividades muestra cómo fluye el control de unas clases a otras con la finalidad de culminar con un flujo de control total que se corresponde con la consecución de un proceso más complejo.

Por este motivo, en un diagrama de actividades aparecerán acciones y actividades correspondientes a distintas clases. Colaborando todas ellas para conseguir un mismo fin.

Ejemplo: Abrir Caja Chica.[31]

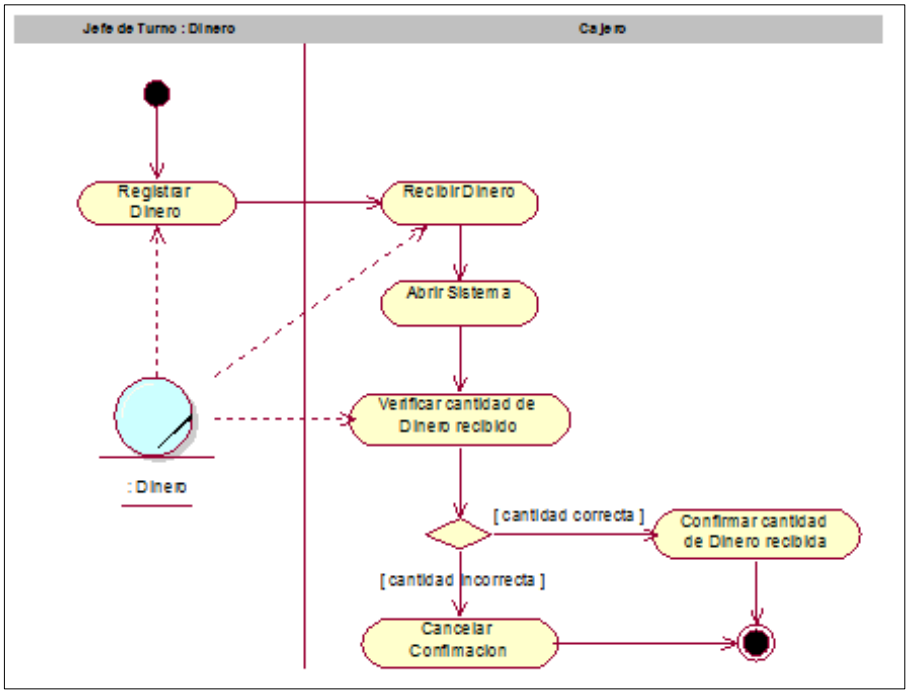



Figura 17. Diagrama de Actividades.
Fuente: http://modeladodesistemas1.blogspot.pe/2012/04/modelado-de-sitemas.html

[31] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 14),"Desarrollo Orientado a Objetos con UML".

### e) Diagrama de Componentes

Los componentes pertenecen al mundo físico, es decir, representa un bloque de construcción al modelar aspectos físicos de un sistema.

Cada componente debe tener un nombre que lo distinga de los demás. Al igual que las clases los componentes pueden enriquecerse con compartimientos adicionales que muestran sus detalles.[32]

## 2.2.3. PHP

PHP es definida por los autores Cobo Ángel, Gómez Patricia, Pérez Daniel y Rocha Roció. (2005, Pág. 99), en su libro titulado PHP y MySql Tecnologías para el desarrollo de aplicaciones web, como un lenguaje interpretado del lado del servidor que se caracteriza por su potencia, versatilidad, robustez y modularidad. Los programas escritos en PHP son embebidos directamente en el código HTML y ejecutados por el servidor web a través de un intérprete antes de transferir al cliente que lo ha solicitado un resultado en forma de código HTML puro.

Al ser un lenguaje que sigue las corrientes open source, tanto el intérprete como su código fuente son totalmente accesibles de forma gratuita en la red.

[32] Xavier Ferré Grau, María Isabel Sánchez Segura. (2011, Pág. 14),"Desarrollo Orientado a Objetos con UML".

En concreto, la dirección oficial en la que puede descargarse es: http://www.php.net/ por su flexibilidad, PHP resulta un lenguaje muy sencillo de aprender; especialmente para programadores familiarizados con lenguajes como C, Perl o Java, debido a las similitudes de sintaxis entre ellos.

Por supuesto, es un lenguaje multiplataforma; los programas funcionales igual sobre diferentes plataformas, trabajando sobre la mayoría de servidores web y estando preparado para interactuar con más de 20 tipos de bases de datos.[33]

En comparación con otro tipo de tecnologías similares, PHP resulta más rápido, independiente de la plataforma y más sencillo de aprender y utilizar.

Inicialmente diseñado para realizar poco más de contadores y libros de visita de páginas, en la actualidad PHP permite realizar una multitud de tareas útiles para el desarrollo web. Por ejemplo, dispone, entre otras, de:

- Funciones de administración y gestión de base de datos específicos para la mayoría de gestores comerciales y funciones para conexiones ODBC con base de datos en sistemas Microsoft.

- Funciones de generación y lectura de cookies.

[33] Cobo Ángel, Gómez Patricia, Pérez Daniel y Rocha Roció. (2005, Pág. 99), "PHP y MySql Tecnologías para el desarrollo de aplicaciones web".

- Funciones de gestión de direcciones y ficheros, incluso para la transferencia mediante FTP.

- Funciones de tratamiento de imágenes y librerías de funciones gráficas.

- Funciones de correo electrónico que pueden ser utilizadas para programar completos sistemas de correos electrónicos vía web.

- Funciones para la generación de documentos PDF.[34]

A la innumerable cantidad de funciones predefinidas en PHP deben añadirse, por supuesto, todas aquellas funciones propias de cada programador, y que pueden ser reutilizadas e intercambiadas a través de foros específicos con otros programadores.

[34] Cobo Ángel, Gómez Patricia, Pérez Daniel y Rocha Roció. (2005, Pág. 100), "PHP y MySql Tecnologías para el desarrollo de aplicaciones web".

### 2.2.4. HTML

Según los autores Cobo Ángel, Gómez Patricia, Pérez Daniel y Rocha Roció. (2005, pág. 57), en su libro titulado PHP y MySql Tecnologías para el desarrollo de aplicaciones web, definen HTML como un lenguaje de descripción de hipertexto compuesto por una serie de comandos, marcas, o etiquetas, también denominadas "Tags" que permiten definir la estructura lógica de un documento web y establecer los atributos del mismo (Color del texto, contenidos multimedia, hipervínculos, etc.).

En resumen, es un lenguaje que permite crear páginas web y para ello utiliza unos comandos o etiquetas que indican o marcan que se debe mostrar y de qué forma.

Los comandos siempre van incluidos entre los signos < > e insertadas en el propio texto que compone el contenido de la página. Especificar su estructura (Las distintas partes de la página) y formato. Además, permiten la inserción de contenidos especiales como imágenes, videos, sonidos, etc.[35]

### 2.2.5. ISO 27002

La norma ISO 27002, está organizado en base a los 11 dominios, 39 objetivos de control y 133 controles de ISO/IEC 27002:2005. Como se muestra en la Figura 18.

[35] Cobo Ángel, Gómez Patricia, Pérez Daniel y Rocha Roció. (2005, Pág. 57), "PHP y MySql Tecnologías para el desarrollo de aplicaciones web".


Figura 18. Estructura de la norma ISO 27002
Fuente: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

### 2.2.6. Dominio 10 - Gestión de Comunicaciones y Operaciones[36]

Leonardo Camelo. (2010), en su Blog titulado ISO 27001 e ISO 27002: Dominio 10 - Gestión de Comunicaciones y Operaciones, menciona los 10 Objetivos de control de la siguiente manera:

a) **10.1 Procedimientos Operacionales y responsabilidades**

**Objetivo:** Asegurar la operación correcta y segura de los servicios de procesamiento de información.

[36] Camelo, Leonardo. (19 de marzo del 2010). ISO 27001 e ISO 27002: Dominio 10 - Gestión de Comunicaciones y Operaciones [Blog post]. Recuperado de http://seguridadinformacioncolombia.blogspot.pe/search/label/Comunicaciones y Operaciones

Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se deberla Implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

**Detalle:** Para la gestión y operación de todos los sistemas y servicios de procesamiento de información de la Organización, se deben establecer procedimientos y responsabilidades que incluyan el desarrollo de instrucciones adecuadas para la operación y procedimientos de respuesta a incidentes operativos y de información.

Para reducir el riesgo de usos no adecuados, sin intención, por error o negligencia de los sistemas de información se debe implementar, de ser requerido, la segregación de funciones de los diferentes roles establecidos en la organización.

**b) 10.2 Gestión de la Prestación del Servicio por Terceras partes**

**Objetivo:** Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras.

La organización debería verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

**Detalle:** Se deben definir normas y controles de seguridad que garanticen la adecuada y eficiente entrega de servicios por parte de proveedores externos.

Se deben identificar los posibles riegos de seguridad de la información con relación a los servicios que presta el proveedor externo, para adicionar en el contrato las correspondientes medidas de seguridad que ayudan a la mitigación de estos riesgos.

**c) 10.3 Planificación y Aceptación del Sistema**

**Objetivo:** Minimizar el riesgo de fallas en los sistemas.

Se requieren planificación y preparación avanzadas para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.

**Detalle:** Se deben definir los requerimientos sobre la planeación en cuanto a la capacidad que deben tener los sistemas o servicios de procesamiento de la información de la Organización y sobre los controles que se deben aplicar para la aceptación y desarrollo de actualizaciones o nuevas versiones de los sistemas de información.

Para todas las nuevas actualizaciones a sistemas, nuevas versiones y nuevos sistemas de información se deben establecer criterios de aceptación, se deben realizar planes de pruebas para estos nuevos requerimientos antes de su definitiva aceptación y puesta en producción.

**d) 10.4 Protección contra códigos maliciosos y móviles**

**Objetivo:** Proteger la integridad del software y de la información.

Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos.

Los directores deberían, cuando sea apropiado, introducir controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

**Detalle:** Se deben definir los adecuados controles para prevenir y detectar la introducción de código o software malicioso, los usuarios y funcionarios de la Organización deben tener conocimiento de los peligros que puede ocasionar el software malicioso o no autorizado. Se deben tomar las precauciones adecuadas para la detección e impedimento de los virus informáticos en los equipos de la Organización.

**e) 10.5 Respaldo**

**Objetivo:** Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información, se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada para hacer copias de seguridad de los datos y probar sus tiempos de restauración.

**Detalle:** Se deben establecer normas y procedimientos rutinarios que permitan tener respaldo de la información y procesamientos de información, realizando copias de seguridad, realizando planes de pruebas y simulaciones de la recuperación oportuna de los datos, registrando eventos o fallos y monitoreo de los equipos.

**f) 10.6 Gestión de la Seguridad de Redes**

**Objetivo:** Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección. También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por redes públicas.

**Detalle:** Se deben establecer controles y medidas específicas para la protección de los datos críticos o sensibles que transitan por las redes públicas de la Organización.

**g) 10.7 Manejo de los Medios**

**Objetivos:** Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. Estos medios se deberían controlar y proteger de forma física.

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada, salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

**Detalle:** Para proteger los documentos, soportes de información, como: discos, cintas, etc., se deben establecer procedimientos operativos para la protección de estos activos de información.

### h) 10.8 Intercambio de la Información

**Objetivo:** Mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.

Los intercambios de información y de software entre las organizaciones se deberían basar en una política formal de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente. Se deberían establecer procedimientos y normas para proteger la información y los medios físicos Que contienen información en tránsito.

**Detalle:** Se debe garantizar que toda la información, datos y software intercambiado entre las organizaciones permanezcan controlados y cumpla con las leyes y regulaciones correspondientes.

Se deben establecer acuerdos, procedimientos y normas para el intercambio de información entre organizaciones. Se deben considerar las implicaciones relacionadas con comercio, correo e intercambio electrónico de datos.

### i) 10.9 Servicios de Comercio Electrónico

**Objetivo:** garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.

Es necesario considerar las implicaciones de seguridad asociadas al uso de servicios de comercio electrónico. Incluyendo las transacciones en línea y los requisitos para los controles.

También se deberían considerar la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

**Detalle:** Se deben establecer e implementar controles y normas para proteger el comercio electrónico de amenazas que pueden llevar a actividades fraudulentas, disputas por contratos y divulgación o modificación de la información de la Organización.

### j) 10.10 Monitoreo

**Objetivo:** Detectar actividades de procesamiento de la información no autorizadas.

Se deberían monitorear los sistemas y registrar los eventos de seguridad de la información.

Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de Información.

La organización deberla cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro.

Es recomendable emplear el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

**Detalle:** Se deben definir lineamientos sobre el monitoreo de los sistemas de información de la Organización para la detección de actividades de procesamiento de información no autorizados.

Se deben definir y asignar roles a los funcionarios que tengan la responsabilidad de monitorear la efectividad y eficiencia de los procesos operacionales, de tal forma que se realicen auditorías y se puedan con el tiempo aplicar mejoras a los procesos.

Este es el Dominio más extenso de toda la ISO 27002 y/o ISO 27001, y abarca desde la asignación inicial de responsabilidades, la planeación de la capacidad del sistema, generación de Backups, gestión de redes, monitoreo, TODO lo que esté involucrado con la capacidad productiva de la Organización y de la continuidad de las comunicaciones de la misma para evitar situaciones que puedan eventualmente paralizar la producción con resultados tales como pérdidas económicas, de reputación, demandas, etc.

## 2.3 Marco Conceptual

- **SOC**.- Centro de Operaciones de Seguridad, es un centro donde se gestiona la seguridad de una organización.

  Boto, C. (Diciembre de 2009). Centro de operaciones de seguridad. Obtenido de http://www.revistadintel.es/Revista/Numeros/Numero4/Seguridad/Industria/boto.pdf

- **DLP**.- Data Loss Prevention, Prevención de la pérdida de datos, es una estrategia para asegurarse de que los usuarios finales no envían información sensible o crítica fuera de la red corporativa.

  Rouse, M. (Diciembre de 2013). *Prevención de pérdida de datos (DLP).* Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Prevencion-de-perdida-de-datos-DLP

- **RUP**.- (Rational Unified Process) es un ejemplo de un modelo de proceso moderno que proviene del trabajo en el UML y el asociado Proceso Unificado de Desarrollo de Software.

  Pearson Educación. S.A. (2005, Pag.76). *Ingeniería de software. Séptima Edición.* Obtenido de https://books.google.com.pe/books?id=gQWd49zSut4C&printsec=frontcover&hl=es#v=onepage&q&f=false

- **UML**.- (Lenguaje Unificado de Modelado), es un lenguaje de modelado visual que se usa para especificar, visualizar, construir, y documentar artefactos de un sistema de software.

  Rumbaugh, J., Jacobson I., Booch, G. (2000, Pag.27). *El Lenguaje Unificado de Modelado, Manual de Referencias.* Obtenido de http://www.face.ubiobio.cl/~cvidal/modelamiento/libros/LenguajeUnificadoModelado.pdf

- **SISTEMA**.- Es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común.

  Fernández Alarcón, V. (2006, Pag.11). *Desarrollo de Sistemas de Información, Una metodología basada en el modelado.* Obtenido de https://books.google.com.pe/books?id=Sqm7jNZS_L0C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- **BASE DE DATOS**.- Es un conjunto auto-descriptivo de registros integrados.

  Kroenke, D. (2003, Pag. 15). *Procesamiento de Base de Datos, Fundamentos, diseño e Implementación.* Obtenido de https://books.google.com.pe/books?id=7ORUWItwcNEC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- **INCIDENTE**.- Es un evento o conjunto de eventos que pueden provocar la interrupción de los servicios ofrecidos por un sistema informático e incluso la pérdida de información y de activos valiosos para la organización.

  Chicano Tejada, E. (2014). *Gestión de incidentes de seguridad informática. IFCT0109*. Obtenido de https://books.google.com.pe/books?id=y63KCQAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

- **ISO 27002**.- Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

  Iso27000.es (2007). *El portal de ISO 27001 en español. Gestión de Seguridad de la Información.* Obtenido de http://www.iso27000.es/iso27000.html

- **Gestión de Comunicaciones y Operaciones**.- son la forma de cómo se administra y supervisa todo lo referente a la actividad y comunicación de la empresa, a través del control de la información o servicio que se entrega dentro de ella.

  Peña Torres, L. (2015). *La gestión de las Comunicaciones y Operaciones en la Seguridad Informática* [Mensaje en un blog]. Obtenido de http://100preseguroo.blogspot.pe/2015/06/la-gestion-de-las-comunicaciones-y.html

# CAPÍTULO III: DESARROLLO DEL SISTEMA

## 3.1 Análisis del Modelo

El proyecto abarca el proceso de Monitoreo de incidentes de prevención de pérdida de datos de tarjetas en la empresa Digiware, este proceso se lleva a cabo en el área del SOC (Centro de Operaciones de Seguridad).

El personal involucrado en este proceso es el Jefe del área de Seguridad de la Información del Banco Interbank, el cual, tiene como función solicitar al área del SOC las evidencias de los eventos que se presentan a diario, dicha área está conformada por el Supervisor y los Operadores quienes se encargan del monitoreo de las herramientas perimetrales de seguridad de la información.

### 3.1.1. Análisis y definición de los procesos.

Para la definición de los procesos, se revisó el procedimiento que ejecutan los operadores del SOC llamado **“PSOC 19 Monitoreo de Incidencias del DLP”**.

Este procedimiento tiene como objetivo notificar los incidentes diarios que se presentan por enviar correos que contienen datos de tarjetas a cuentas de correo de dominios externos al banco Interbank.

Del análisis de la documentación del procedimiento actual que maneja el área del SOC y la información brindada por el supervisor de dicha área, se determinó dos procesos importantes en relación al monitoreo de los incidentes de fuga de información.

Los procesos identificados son los siguientes:

a) **Proceso de solicitar ejecutar el procedimiento de monitoreo de incidencias del DLP.**

En este proceso participa el Jefe del área de Ingeniería de Seguridad de la Información del Banco Interbank, los operadores del área del SOC quienes se encargan de monitorear las herramientas perimetrales de seguridad de la información y los Jefes directos de los colaboradores que generan los incidentes por el envío de correos conteniendo datos de tarjeta a dominios externos al banco.

El Jefe del área de Ingeniería de Seguridad de la Información, solicita la ejecución del procedimiento de monitoreo de incidentes del DLP a los operadores SOC.

Los operadores monitorean la herramienta perimetral verificando si se han producidos eventos de envíos de correos con datos de tarjetas hacia dominios externos, en caso los hubiera, notifican al Jefe directo del colaborador que incurrió en el incidente solicitando su descargo donde deben indicar si el envío del correo forma parte del proceso de negocio o es un posible caso de fuga de información. De acuerdo a la respuesta del Jefe directo del colaborador notificado, el operador SOC cerrará el incidente si el caso fuese un falso positivo de lo contrario el incidente se deriva al Área de Gobierno y Control para que tomen las acciones correspondientes.

Ya que el servicio brindado por la empresa Digiware hacia el banco Interbank es de 24x7, los operadores SOC cambian de turno cada 9 días de trabajo, dejando los casos pendientes al siguiente operador que entra de turno, cabe mencionar que el procedimiento de incidencias del DLP se ejecuta en horas de la madrugada.

**b) Proceso de obtener informe mensual de los casos presentado en el monitoreo de incidencias del DLP**

En este proceso participa el Jefe del área de Ingeniería de Seguridad de la Información y el Supervisor del área del SOC.

El proceso lo inicia el Jefe del área de Ingeniería de Seguridad de la Información solicita al Supervisor del SOC el informe e indicadores mensual de los incidentes presentados en todo el mes, el cual, el supervisor entra a la ruta compartida donde se guarda el archivo Excel del mes con los registros de todos los casos notificados por los Operadores SOC, donde se evidencia los casos determinados como Fuga de Información, Falsos Positivos, casos que están Abiertos (No se obtienen respuesta por parte del Jefe Directo del Colaborador) y los casos Cerrados (Se obtuvieron respuesta por parte del Jefe Directo del Colaborador).

Luego de que el Supervisor del área del SOC elabore el informe mensual de los casos de incidentes, envía dicho informe por correo electrónico al Jefe del área de Ingeniería de Seguridad de la Información.

### 3.1.2. Elaboración del modelo de negocio.

Luego de haber identificado los procesos que se desarrollan para la ejecución del procedimiento PSOC 19 Monitoreo de Incidencias del DLP en la empresa Digiware, siguiendo la metodología RUP realizamos el modelo de negocio, el cual, consiste en realizar el diagrama de casos de uso de negocio y los diagramas de actividades de cada caso de uso de negocio.

De acuerdo a los procesos identificados se tiene dos casos de uso de negocio los cual son:

- BUC_RequerirMonitoreoDeIncidentesDLP
- BUC_SolicitarReporteMensualDeIncidentes

Y como actor del negocio tenemos al BA_JefeSI

**DIAGRAMA DE CASOS DE USO DE NEGOCIO**

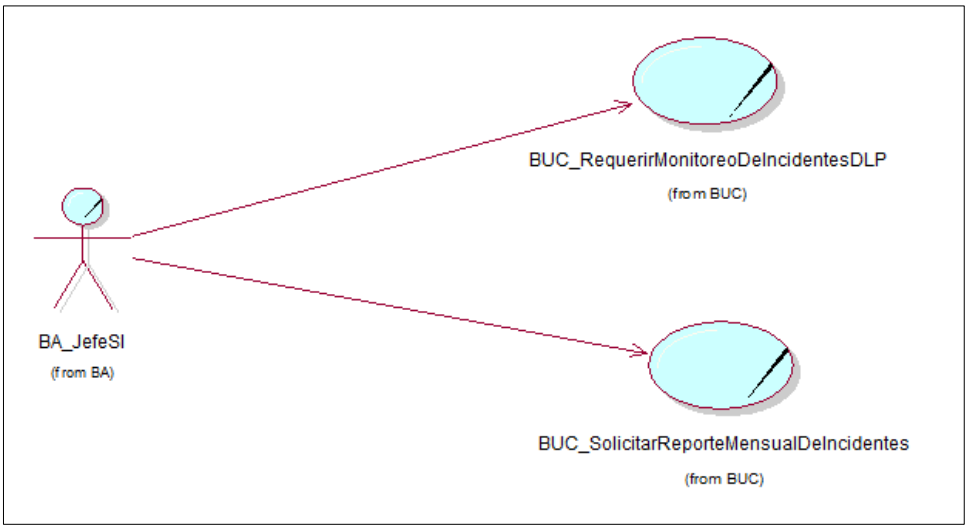



Figura 19. Diagrama de caso de uso de negocio.
Fuente: Elaboración propia.

Una vez identificado los casos de uso de negocio procedemos a realizar el diagrama de actividades de cada caso de uso donde se refleja el flujo de actividades que se da para realizar cada proceso.

## a) Diagrama de Actividades:

- BUC_RequerirMonitoreoDeIncidentesDLP

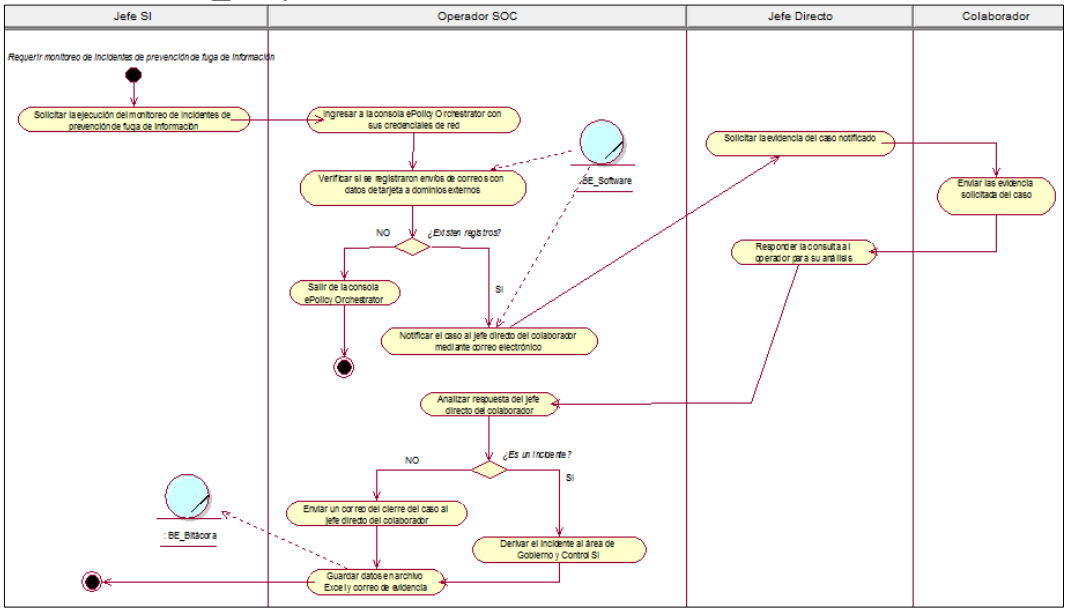



Figura 20. Diagrama de actividades - BUC_RequerirMonitoreoDeIncidentesDLP
Fuente: Elaboración propia.

- BUC_SolicitarReporteMensualDeIncidentes

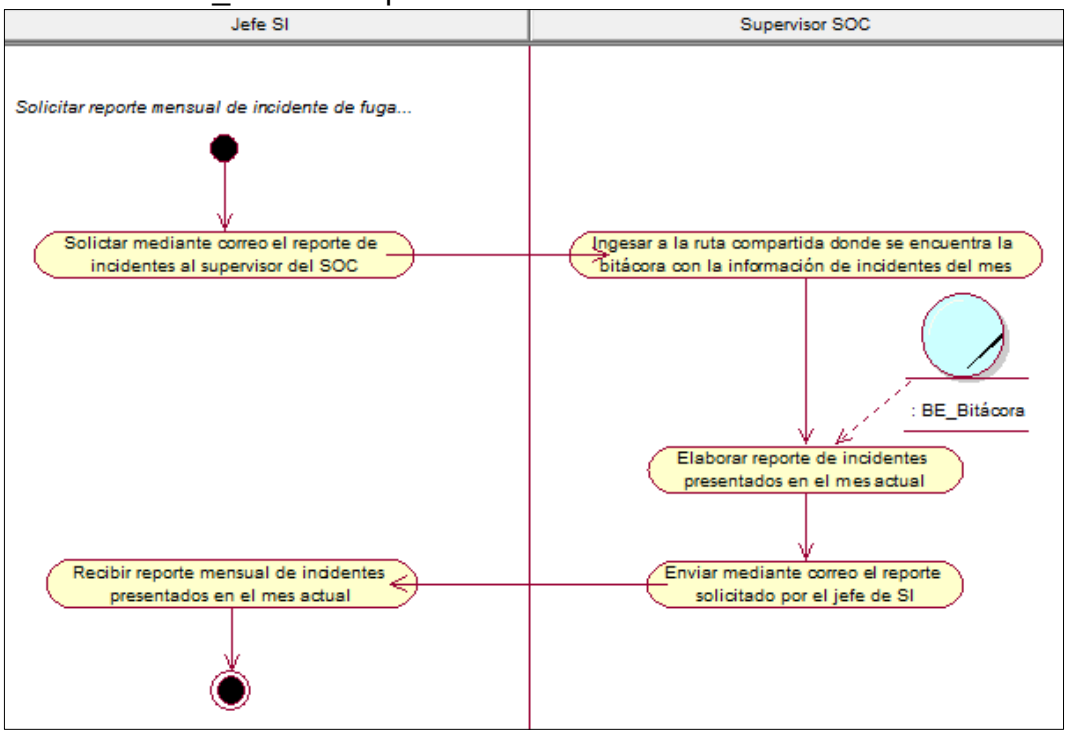



Figura 21. Diagrama de actividades - BUC_SolicitarReporteMensualDeIncidentes
Fuente: Elaboración propia.

## b) Diagrama de Realización de BUC:

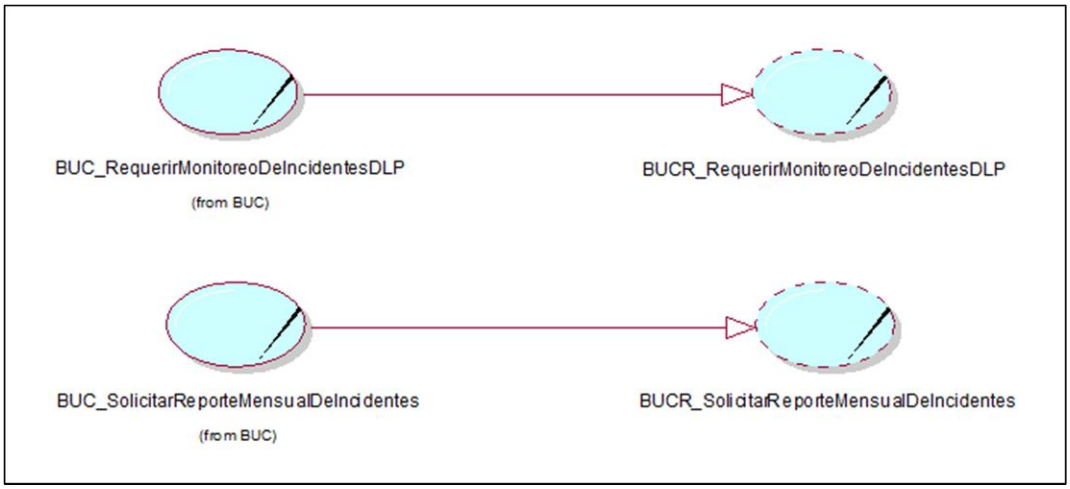



Figura 22. Diagrama de realización de BUC
Fuente: Elaboración propia.

## c) Diagrama de Objetos de Negocio:

- BOD_RequerirMonitoreoDeIncidentesDLP

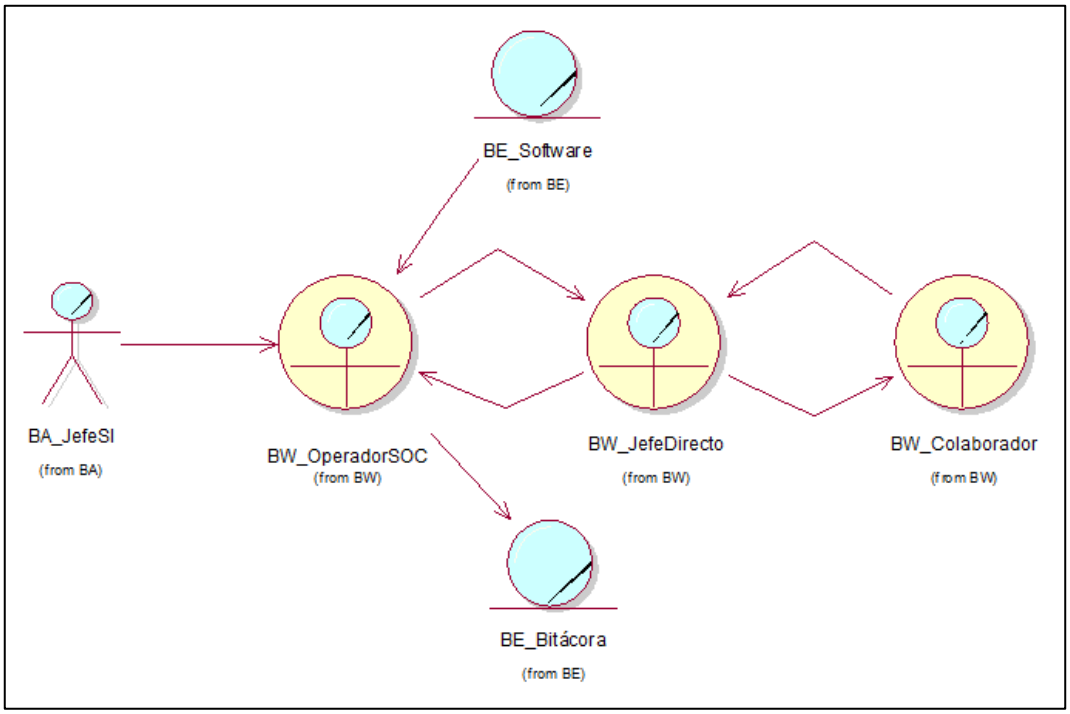



Figura 23. Diagrama de Objeto de Negocio - BOD_RequerirMonitoreoDeIncidentesDLP
Fuente: Elaboración Propia.

- BOD_SolicitarReporteMensualDeIncidentes

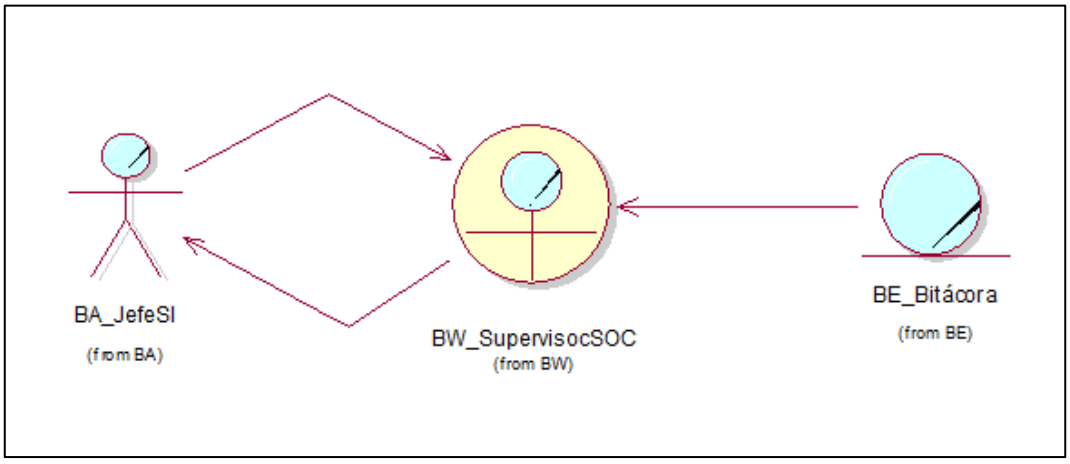



Figura 24. Diagrama de Objeto de Negocio - BOD_SolicitarReporteMensualDeIncidentes
Fuente: Elaboración Propia.

### 3.1.3. Identificación de requerimientos.

Una vez realizado el modelo del negocio se procede a realizar la identificación de requerimientos, para esto generamos la matriz de requerimientos donde se define los requerimientos y el caso de uso que se desarrollará para cada requerimientos y el actor involucrado.

### 3.1.4. Matriz de requerimientos.

| N° | REQUERIMIENTOS | CASOS DE USO | PRIORIDAD | ACTOR |
|---|---|---|---|---|
| 1 | RF01: El sistema debe permitir ver los detalles de los casos del mes. | UC_VerListaGeneralDeIncidentes | 1 | Operador |
| 2 | RF02: El sistema de permitir envía correo de notificación. | UC_NotificarIncidenteDeInformación | 1 | |
| 3 | RF03: El sistema debe permitir registrar datos del incidente presentado. | | | |
| 4 | RF04: El sistema debe permitir Actualizar estado de los incidentes notificados. | UC_ActualizarEstadoDeIncidente | 1 | |
| 5 | RF04: El sistema debe permitir generar informe de incidentes del mes actual. | UC_GenrarInformeDeIncidentes | 1 | Supervisor |
| 6 | RF05: El sistema debe permitir generar Backup de la BD. | UC_GenrarBackupBD | 1 | |
| 7 | RF06: El sistema debe permitir agregar nuevos operadores. | UC_AgregaUsuario | 2 | |
| 8 | RF07: El sistema debe permitir actualizar y eliminar datos de los usuarios. | UC_EditarUsuario | 2 | |
| 9 | RF08: El sistema debe contar con un módulo de seguridad. | UC_AutenticarUsuario | 3 | Usuario |

Tabla 1. Matriz de requerimientos.
Fuente: Elaboración propia.

## 3.2 Análisis y Diseño del Sistema

Con los requerimientos obtenidos de la fase de modelado de negocio comenzaremos a realizar el análisis y diseño del sistema.

Los casos de uso a realizar son:

a) AutenticarUsuario
b) GenerarInformeDeIncidentes
c) GenerarBackupBD
d) AgregarUsuario
e) EditarUsuario
f) ActualizarEstadoDeIncidente
g) VerListaGeneralDeIncidentes
h) NotificarIncidentesDeInformación

Y los actores del sistema que se identificó son:

a) Supervisor
b) Operador

### 3.2.1. Diagrama de caso de uso del sistema

Desarrollaremos el diagrama de caso de uso del sistema donde observaremos la relación de los casos de uso del sistema con los actores del sistema.

## DIAGRAMA DE CASO DE USO DEL SISTEMA

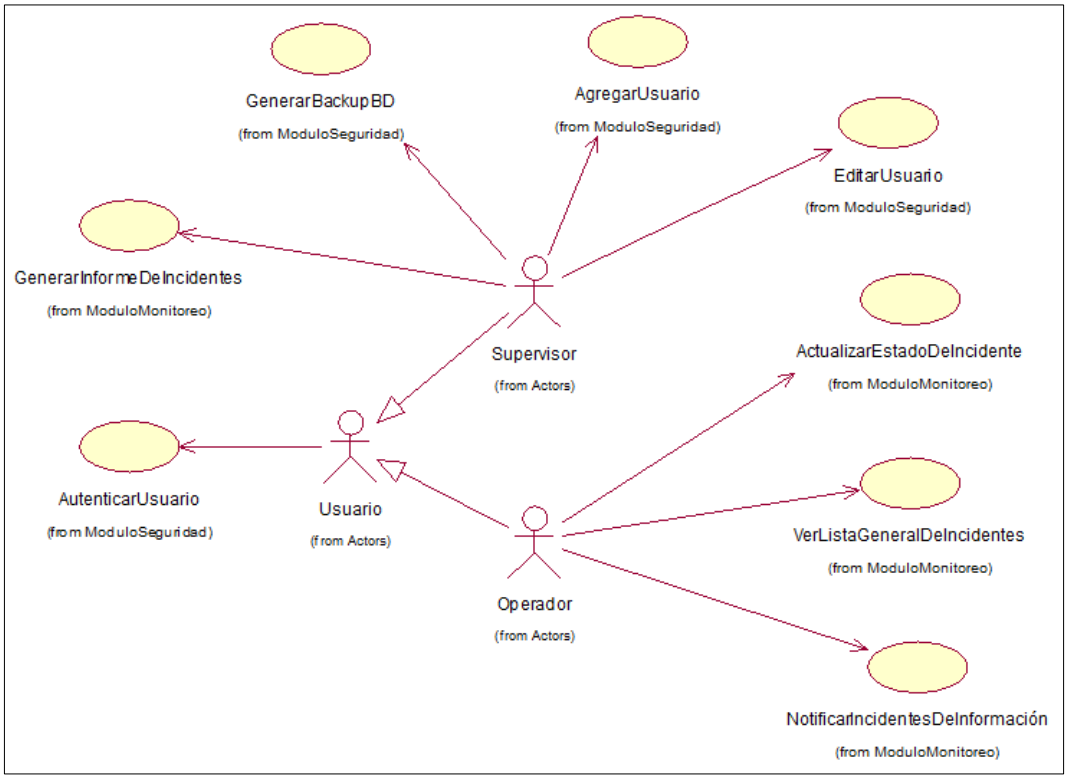



Figura 25. Diagrama de Caso de Uso del Sistema.
Fuente: Elaboración propia.

Una vez realizado el diagrama de casos de uso del sistema, desarrollaremos cada caso de uso con su respectivo diagrama de actividades, diagrama de objetos y diagrama de secuencia.

### 3.2.2. Diagrama de realización de CU

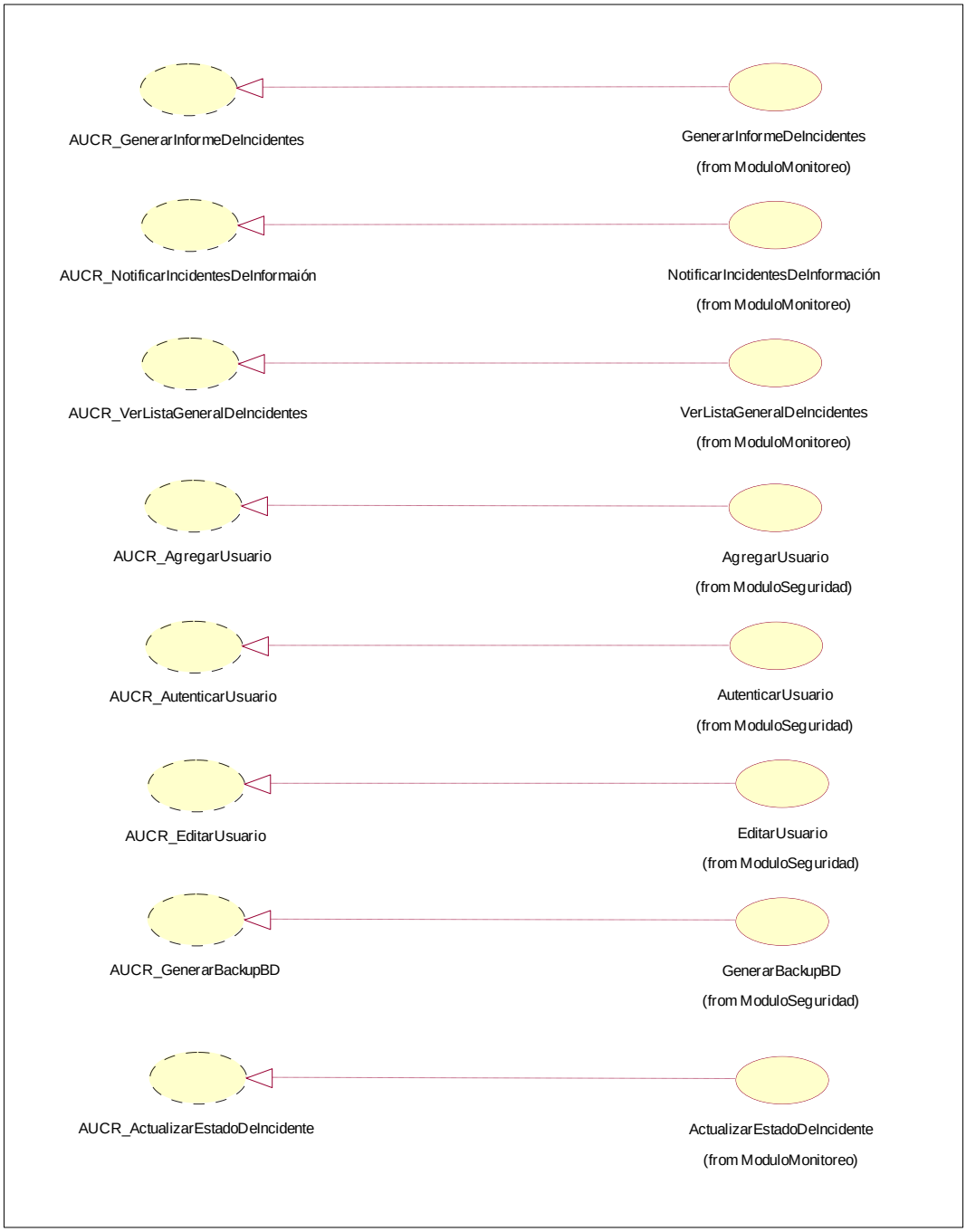



Figura 26. Diagrama de Realización de Caso de Uso del Sistema.
Fuente: Elaboración Propia.

## a) AutenticarUsuario

| | |
|---|---|
| **Nombre:** | AutenticarUsuario. |
| **Descripción:** | Usuario desea ingresar al sistema. |
| **Precondición:** | Usuario registrado. |
| **Secuencia principal:** | 1. Usuario ingresa la URL en la barra de dirección de un navegador.<br>2. Sistema mostrará el formulario de inicio de sesión para ingresar su nombre de usuario y su contraseña.<br>3. El usuario ingresa su nombre de usuario y contraseña.<br>4. El sistema validará que los datos ingresados se encuentren en la base de datos.<br>5. El sistema obtendrá los privilegios según el usuario autenticado.<br>6. El sistema mostrará el menú principal del usuario. |
| **Errores / alternativas** | 1. En caso que el nombre de usuario o contraseña sean incorrectos, el sistema mostrará un mensaje de error “User o password incorrectos”.<br>2. En caso el usuario no cuente con privilegios, el sistema mostrará un mensaje de error “El usuario no tiene privilegios”. |
| **Post condición:** | Ninguna. |
| **Notas** | |

Tabla 2. Especificación de Caso de Uso: AutenticarUsuario
Fuente: Elaboración propia.

## Diagrama de Actividades: AutenticarUsuario

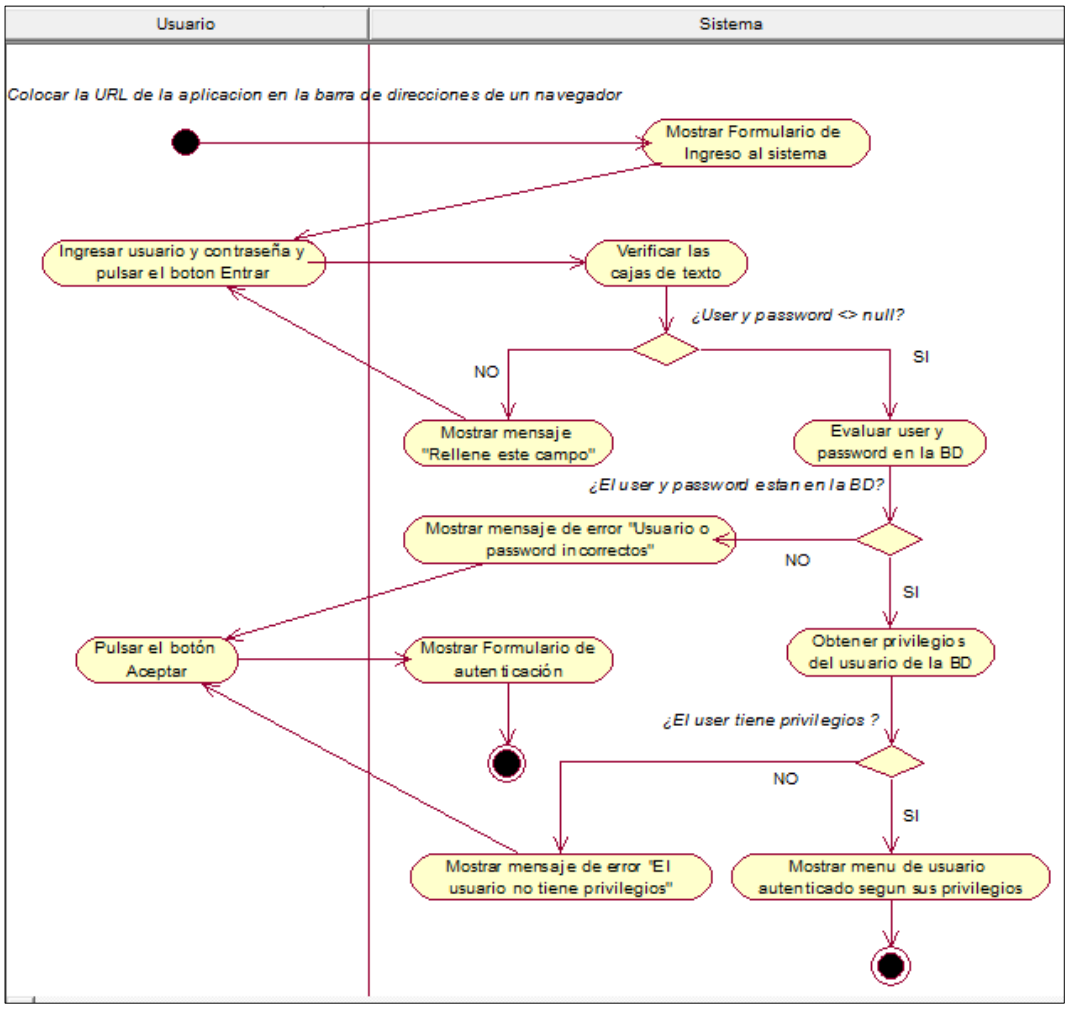



Figura 27. Diagrama de Actividades: AutenticarUsuario
Fuente: Elaboración propia.

## Diagrama de Objetos: AutenticarUsuario

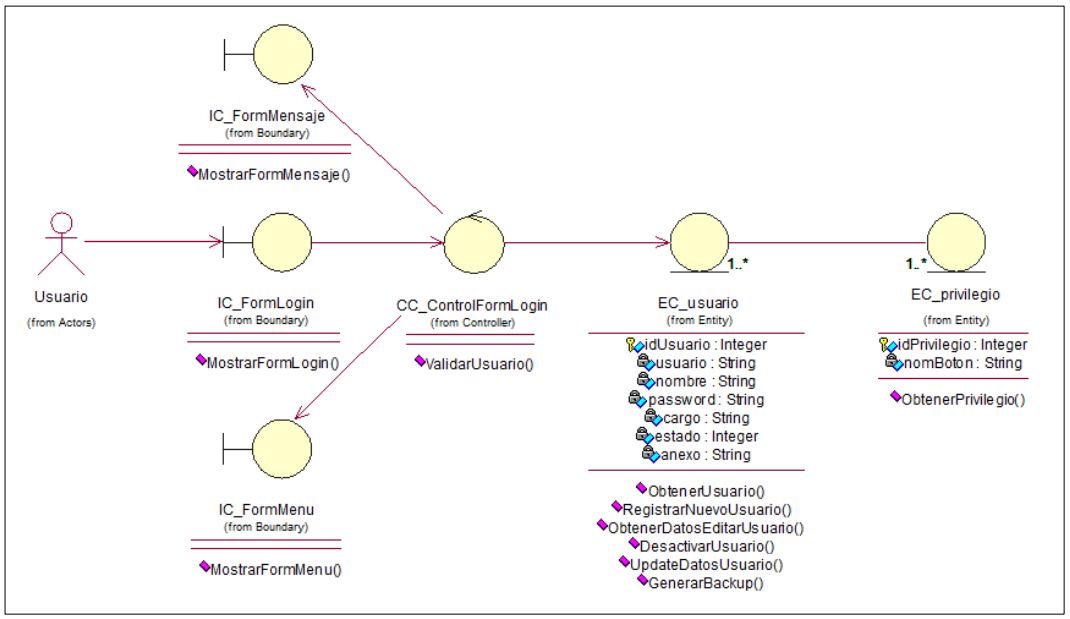



Figura 28. Diagrama de Objetos: AutenticarUsuario
Fuente: Elaboración Propia.

## Diagrama de Secuencia: AutenticarUsuario

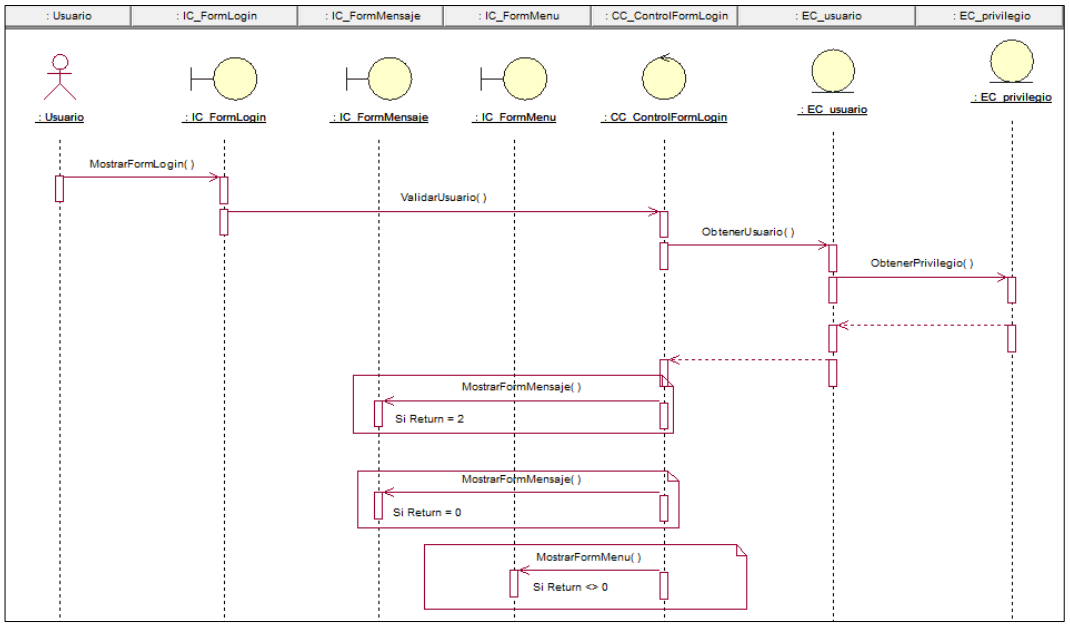



Figura 29. Diagrama de Secuencia: AutenticarUsuario
Fuente: Elaboración propia.

## b) GenerarInformeDeIncidentes

| | |
|---|---|
| **Nombre:** | GenerarInformeDeIncidentes |
| **Descripción:** | El supervisor desea generar informe de incidentes del mes. |
| **Precondición:** | Incidentes registrados |
| **Secuencia principal:** | 1. El supervisor SOC dará clic en el botón Generar Reporte.<br>2. El sistema mostrar combo box con los 12 meses del año.<br>3. El supervisor selecciona el mes que desea generar el reporte.<br>4. El sistema obtiene los datos de los incidentes del mes seleccionado y muestra las gráficas estadísticas y la lista de incidentes.<br>5. El supervisor dará clic en botón Exportar reporte EXCEL.<br>6. El sistema Genera el archivo Excel con la información solicitada. |
| **Errores / alternativas** | 1. En caso de que no exista datos registrados en el mes seleccionado, el sistema mostrará mensaje “No se encontraro datos del mes seleccionado en la BD”. |
| **Post condición:** | Reporte de incidentes creados. |
| **Notas** | |

Tabla 3. Especificación de Caso de Uso: GenerarInformeDeIncidentes
Fuente: Elaboración propia.

## Diagrama de Actividades: GenerarInformeDeIncidentes

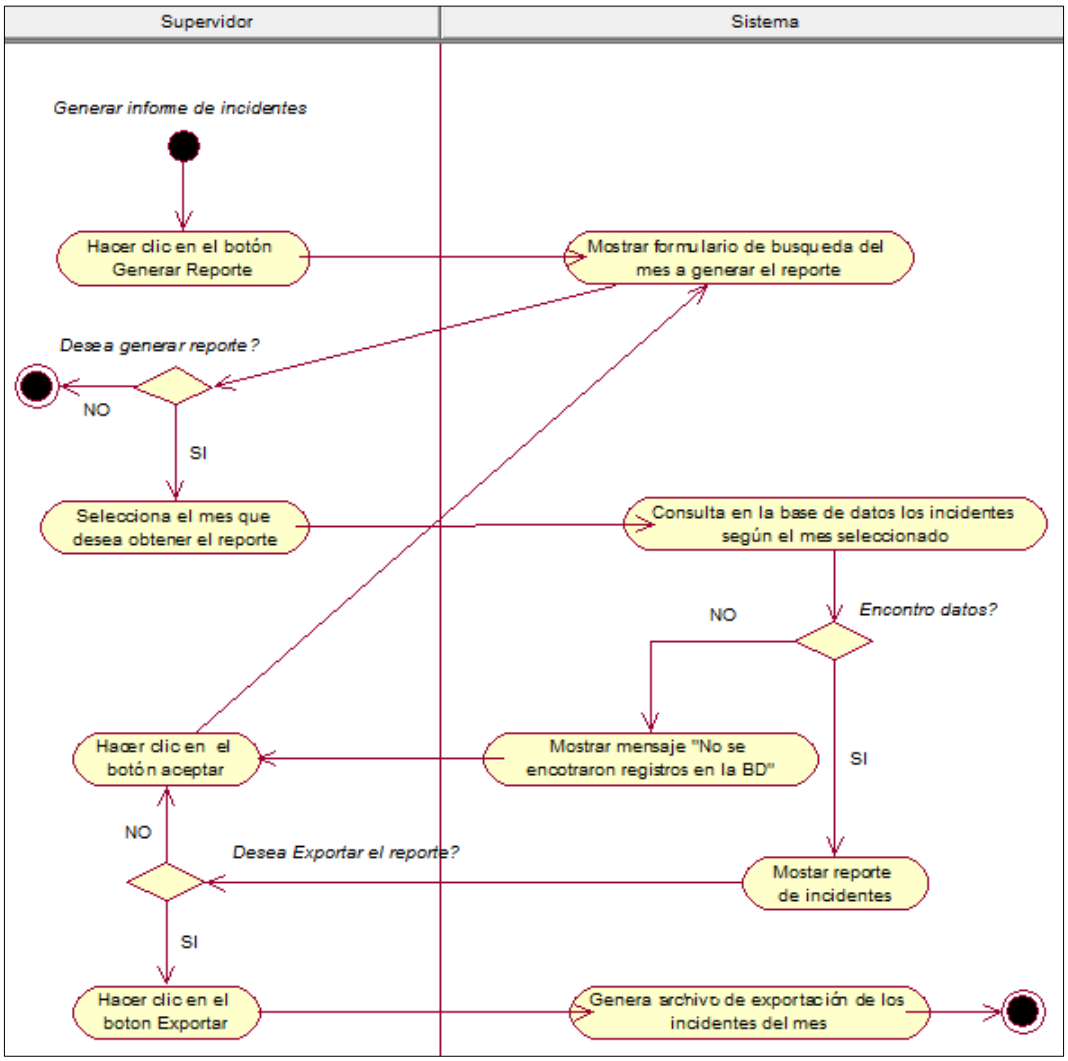



Figura 30. Diagrama de Actividades: GenerarInformeDeIncidentes
Fuente: Elaboración propia.

## Diagrama de Objetos: GenerarInformeDeIncidentes

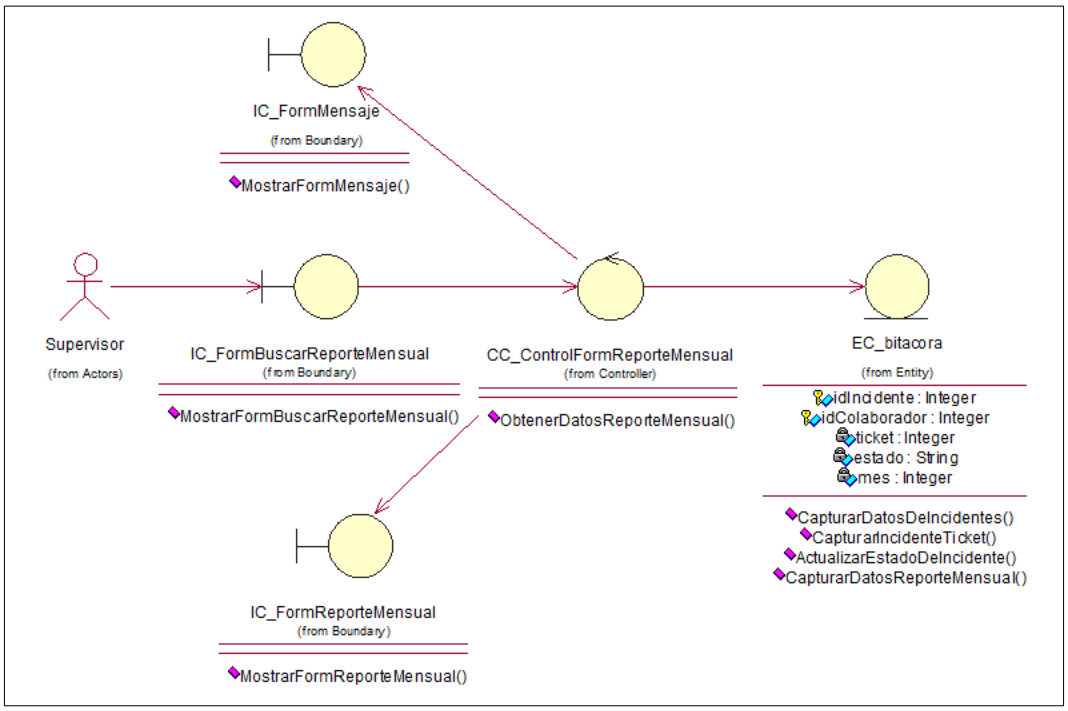



Figura 31. Diagrama de Objetos: GenerarInformeDeIncidentes
Fuente: Elaboración propia.

## Diagrama de Secuencia: GenerarInformeDeIncidentes

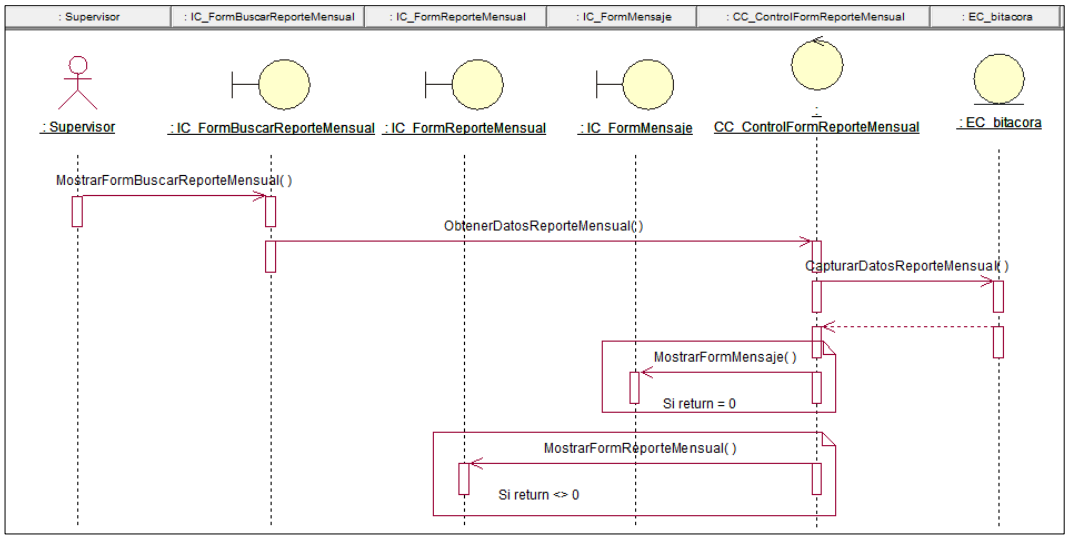



Figura 32. Diagrama de Secuencia: GenerarInformeDeIncidentes
Fuente: Elaboración propia.

## c) GenerarBackupBD

| | |
|---|---|
| **Nombre:** | GenerarBackupBD |
| **Descripción:** | El supervisor SOC desea realizar un Backup de la información registrada en la base de datos. |
| **Precondición:** | Ninguna. |
| **Secuencia principal:** | 1. El Supervisor dará clic en el botón Generar Backup BD.<br>2. El sistema genera archivo de la base de datos (.sql).<br>3. El sistema mostrará mensaje “El Backup se generó correctamente”. |
| **Errores / alternativas** | 1. Ninguna. |
| **Post condición:** | Backup de la BD guardado. |
| **Notas** | Para generar el Backup de la BD se ejecutará un script de código PHP. |

Tabla 4. Especificación de caso de uso: GenerarBackupBD
Fuente: Elaboración propia.

## Diagrama de Actividades: GenerarBackupBD

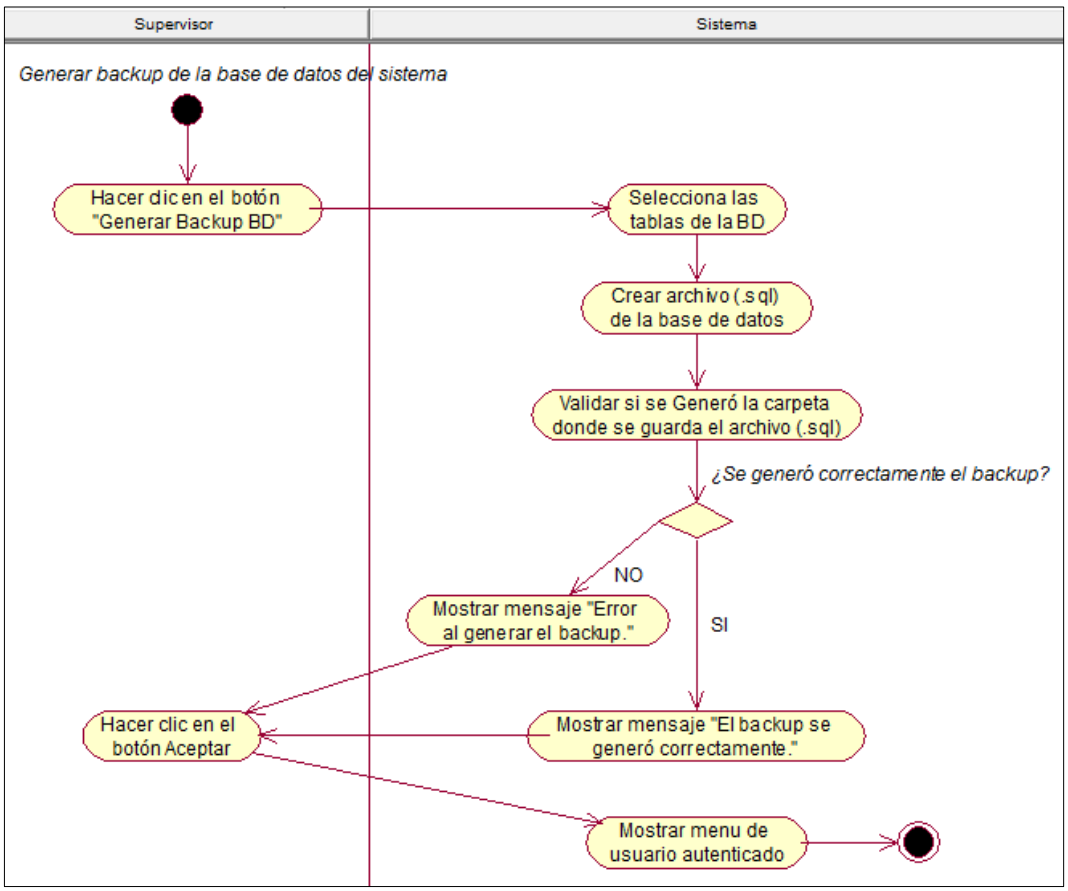



Figura 33. Diagrama de Actividades: GenerarBackupBD
Fuente: Elaboración propia.

## Diagrama de Objetos: GenerarBackupBD

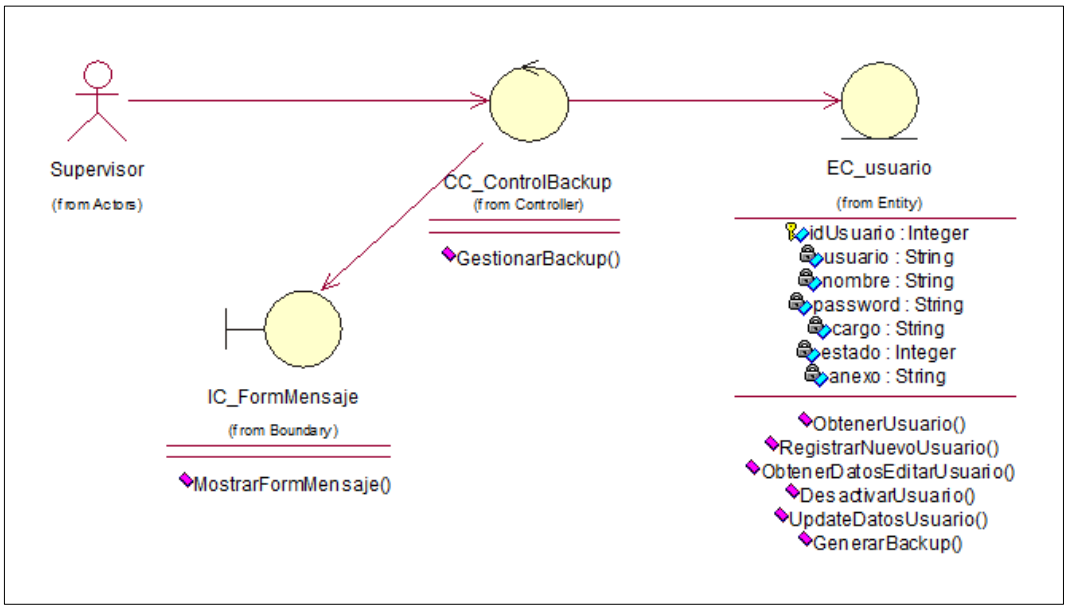



Figura 34. Diagrama de Objetos: GenerarBackupBD
Fuente: Elaboración propia.

## Diagrama de Secuencia: GenerarBackupBD

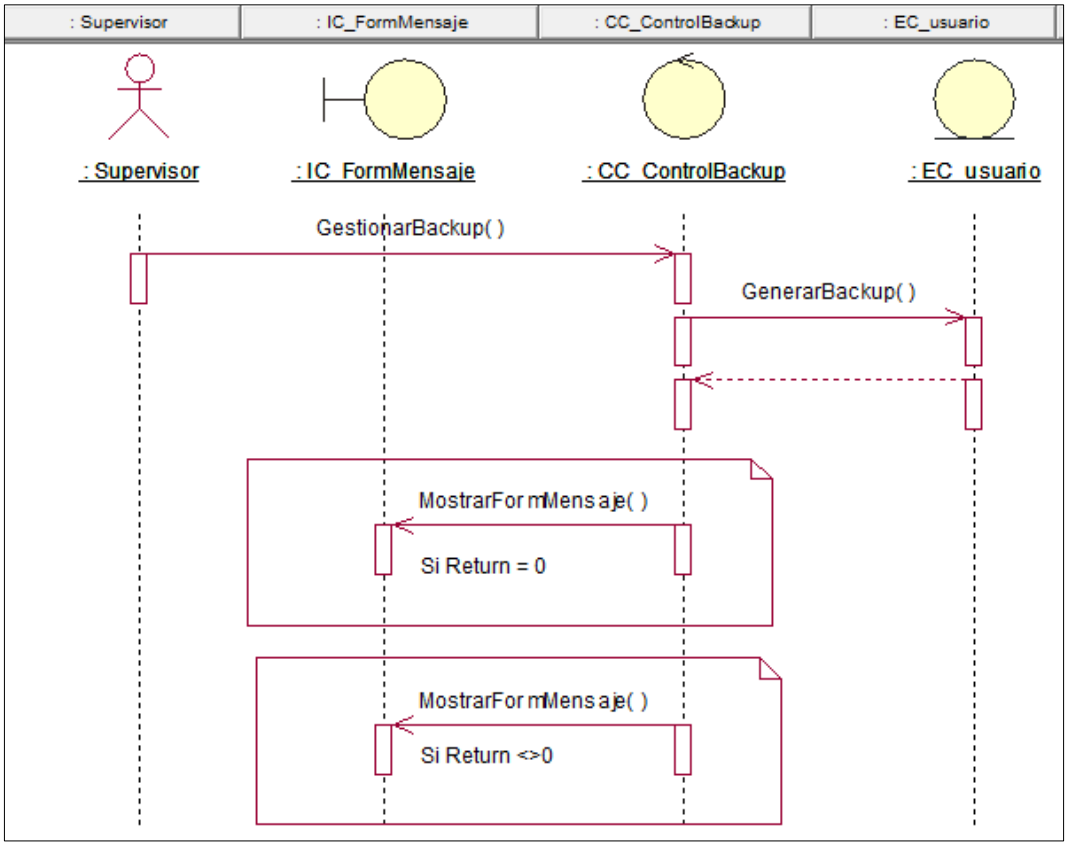



Figura 35. Diagrama de Secuencia: GenerarBackupBD
Fuente: Elaboración propia.

## d) AgregarUsuario

| | |
|---|---|
| **Nombre:** | AgregarUsuario |
| **Descripción:** | El supervisor SOC desea agregar un nuevo usuario al sistema. |
| **Precondición:** | Privilegios registrados. |
| **Secuencia principal:** | 1. El supervisor dará clic en el botón Agregar Usuario.<br>2. El sistema mostrará formulario para registrar los datos del nuevo usuario.<br>3. El supervisor ingresa los datos del usuario.<br>4. El supervisor selecciona los privilegios que tendrá el nuevo usuario.<br>5. El supervisor dará clic en el botón Guardar Usuario.<br>6. El sistema mostrará mensaje “Los datos del usuario se registraron correctamente”. |
| **Errores / alternativas** | 1. El sistema mostrará mensaje de error “Error al registrar nuevo usuario, el usuario debe ser único”. |
| **Post condición:** | Usuario registrado. |
| **Notas** | |

Tabla 5. Especificación de caso de uso: AgregarUsuario
Fuente: Elaboración propia.

## Diagrama de Actividades: AgregarUsuario

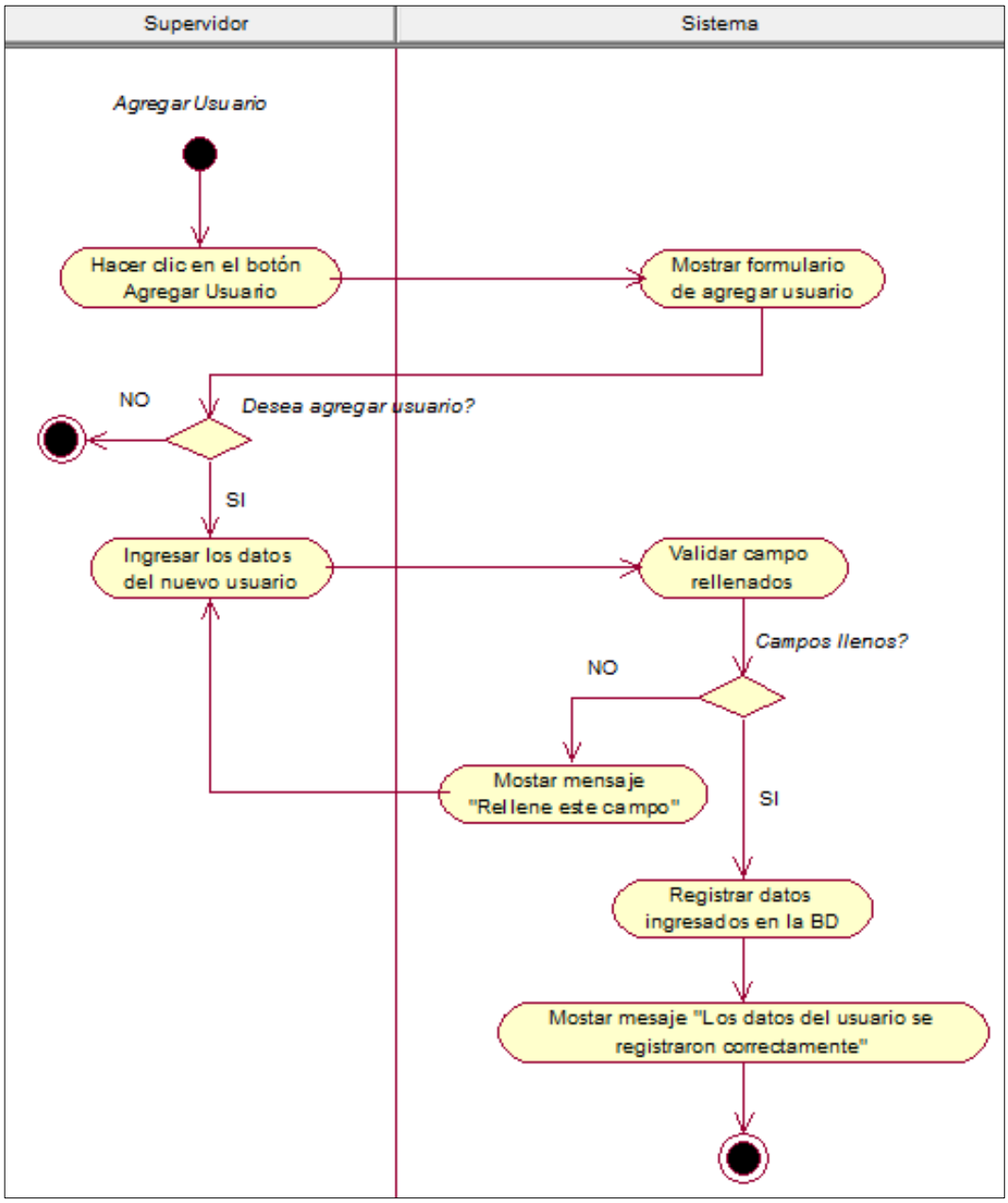



Figura 36. Diagrama de Actividades: AgregarUsuario
Fuente: Elaboración propia.

## Diagrama de Objetos: AgregarUsuario

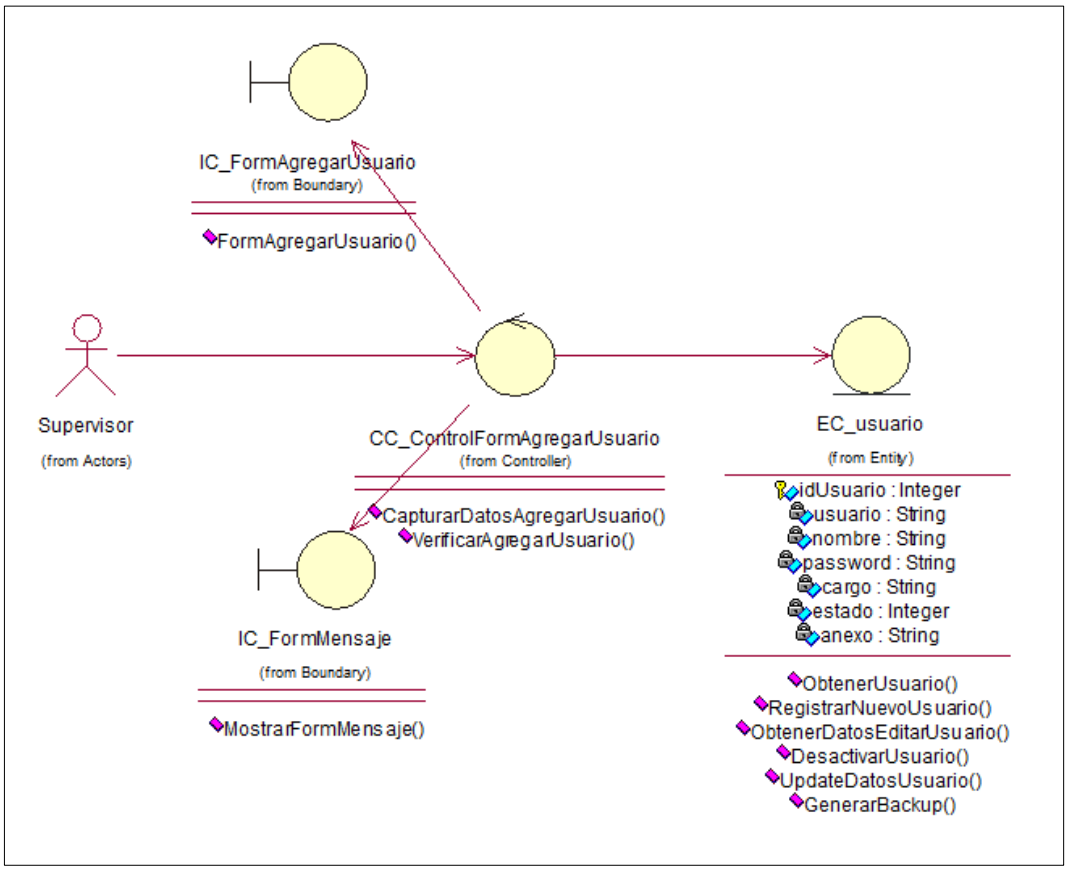



Figura 37. Diagrama de Objetos: AgregarUsuario
Fuente: Elaboración propia.

## Diagrama de Secuencia: AgregarUsuario

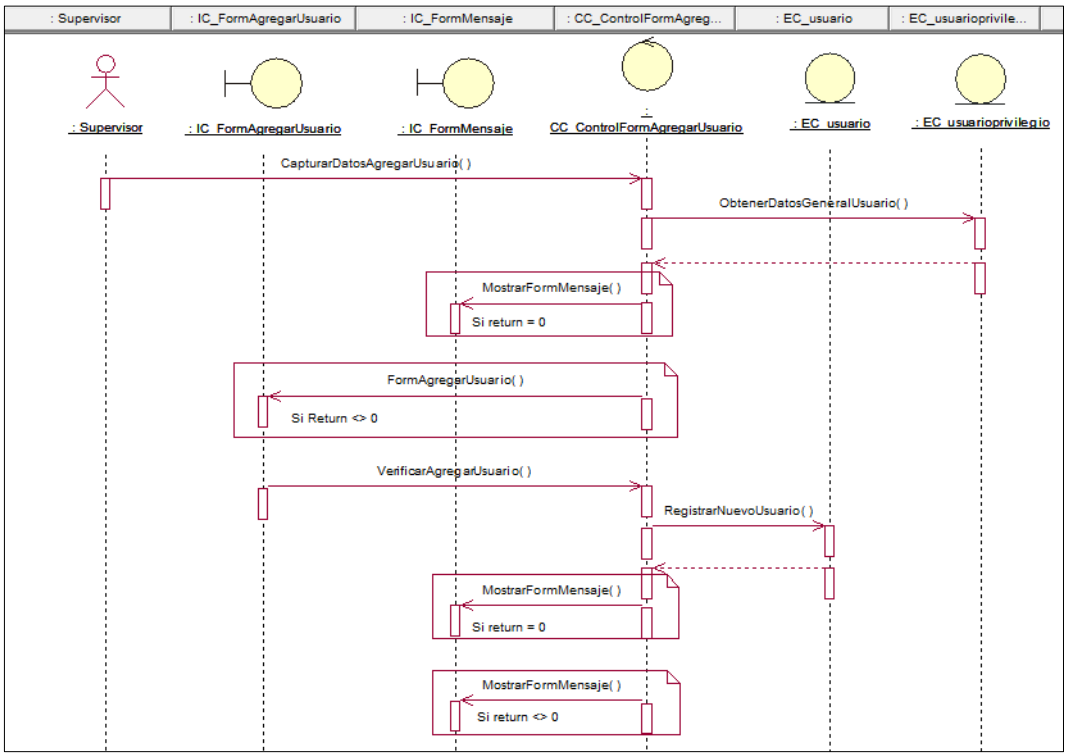



Figura 38. Diagrama de Secuencia: AgregarUsuario
Fuente: Elaboración propia.

## e) EditarUsuario

| | |
|---|---|
| **Nombre:** | EditarUsuario |
| **Descripción:** | El supervisor desea editar datos de los usuarios de sistema. |
| **Precondición:** | Usuario registrado. |
| **Secuencia principal:** | 1. El supervisor dará clic en el botón Editar Usuario.<br>2. El sistema mostrará formulario de búsqueda por nombre o registro del usuario.<br>3. El supervisor ingresa el nombre o registro del usuario a editar.<br>4. El sistema obtiene datos del usuario registrado en la base de datos.<br>5. El supervisor decide actualizar o eliminar usuario.<br>6. El supervisor dará clic en el botón Editar.<br>7. El sistema mostrará formulario con los datos cargados del usuario que se va actualizar sus datos.<br>8. El supervisor modifica los datos que requiere y hace clic en el botón Actualizar Usuario.<br>9. El sistema mostrará mensaje “Los datos del usuario se actualizaron correctamente”.<br>10. Si desea eliminar al usuario del sistema, el supervisor dará clic en el botón Eliminar.<br>11. El sistema actualiza el campo estado en la base de datos.<br>12. El sistema mostrará mensaje “El usuario fue desactivado del sistema”. |
| **Errores / alternativas** | 1. El sistema mostrará mensaje de error “No se encontraron datos similares” cuando no se encuentre en la base de datos el nombre o registro ingresado en la búsqueda. |
| **Post** | Datos del usuario editados. |

| | |
|---|---|
| **condición:** | |
| **Notas** | |

Tabla 6. Especificación de caso de uso: EditarUsuario
Fuente: Elaboración propia.

## Diagrama de Actividades: EditarUsuario (Parte 01)

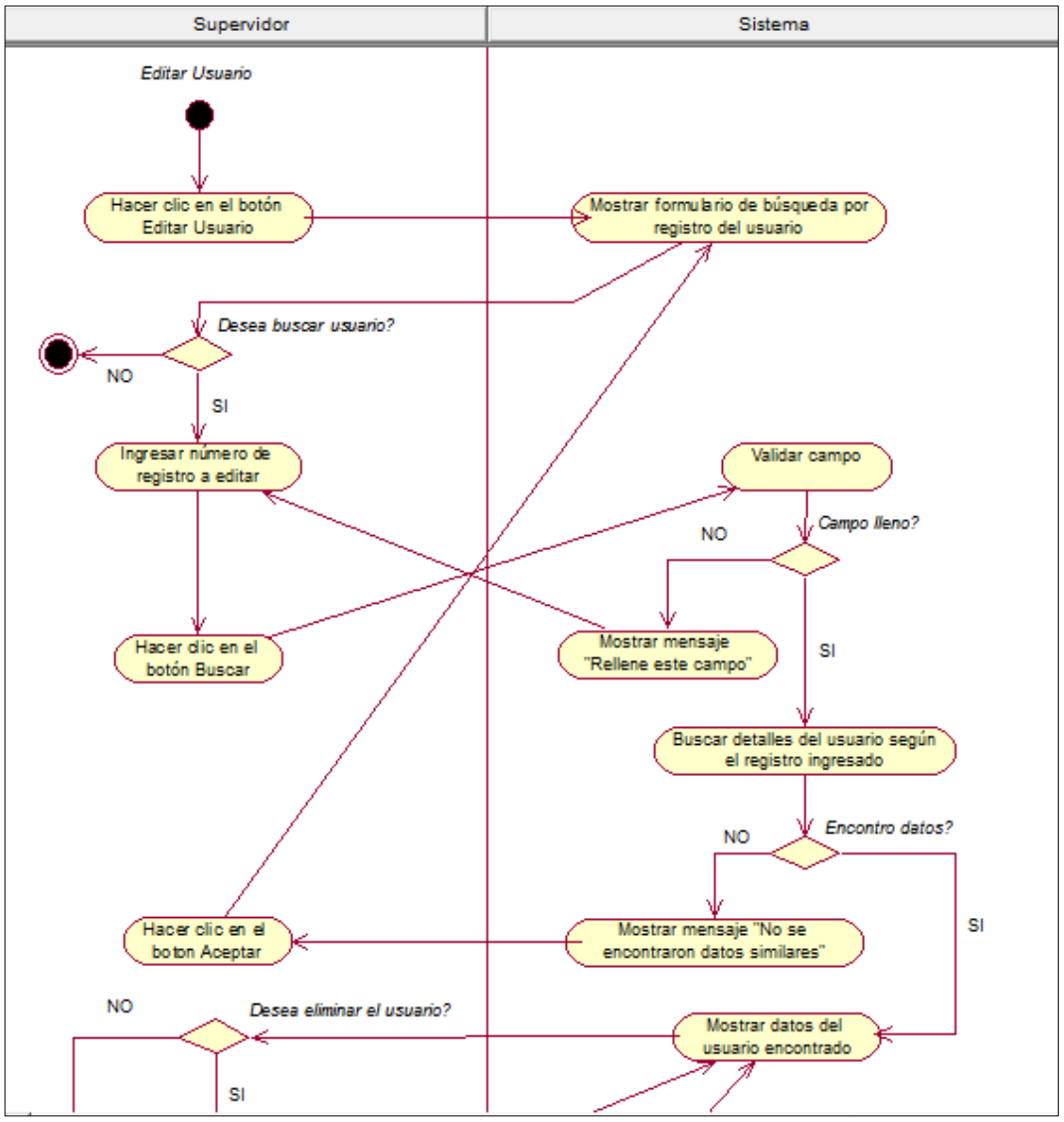



Figura 39. Parte 1, Diagrama de Actividades: EditarUsuario
Fuente: Elaboración propia.

## Diagrama de Actividades: EditarUsuario (Parte 02)

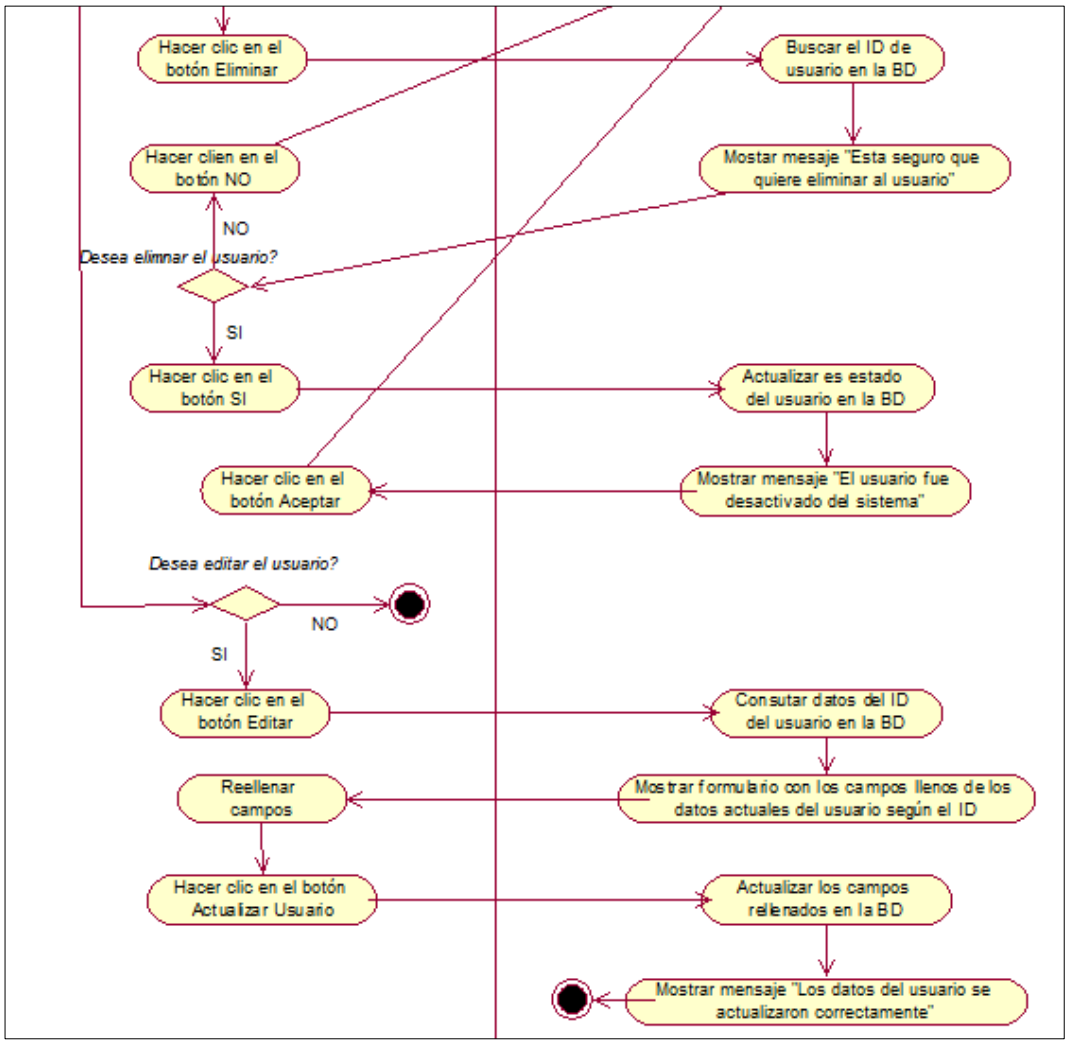



Figura 40. Parte 2, Diagrama de Actividades: EditarUsuario
Fuente: Elaboración propia.

## Diagrama de Objetos: EditarUsuario

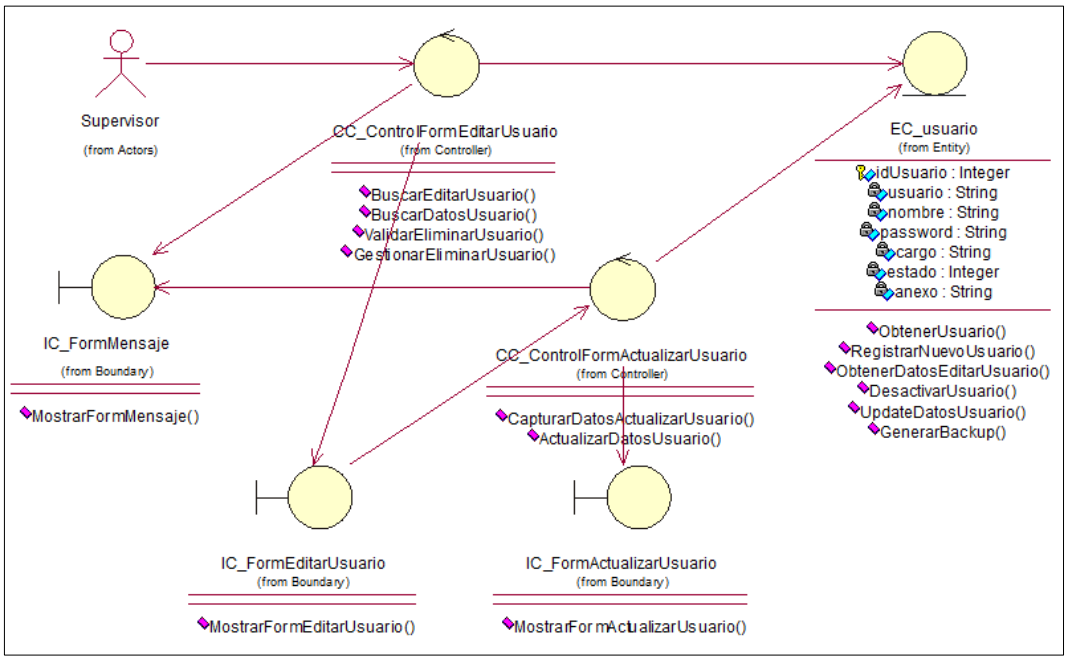



Figura 41. Diagrama de Objetos: EditarUsuairo
Fuente: Elaboración propia.

## Diagrama de Secuencia: EditarUsuario (Parte 01)

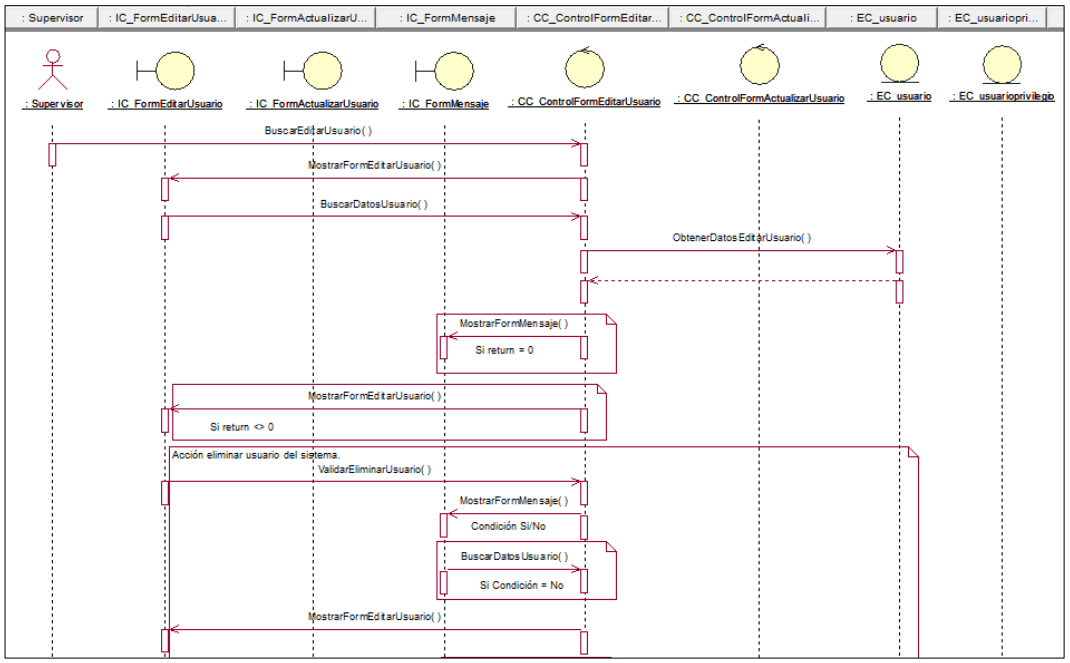



Figura 42. Parte 1, Diagrama de Secuencia: EditarUsuario
Fuente: Elaboración propia.

## Diagrama de Secuencia: EditarUsuario (Parte 02)

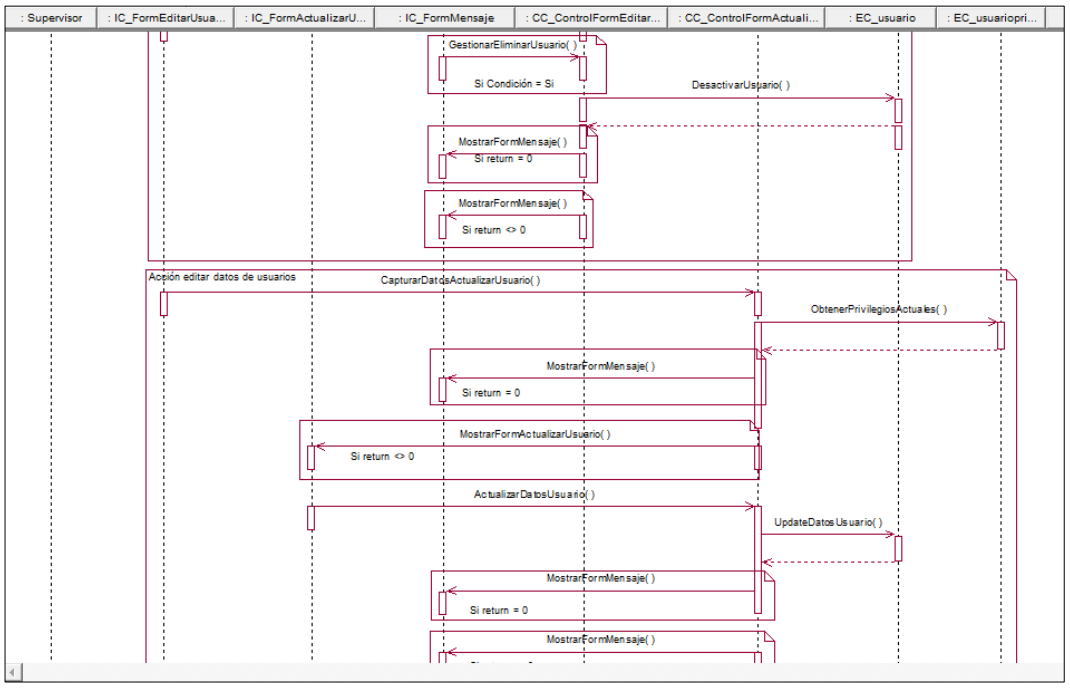



Figura 43. Parte 2, Diagrama de Secuencia: EditarUsuario
Fuente: Elaboración propia.

## f) ActualizarEstadoDeIncidente

| | |
|---|---|
| **Nombre:** | ActualizarEstadoDeIncidente |
| **Descripción:** | El Operador SOC desea actualizar el estado de los incidentes notificados. |
| **Precondición:** | Incidentes registrados. |
| **Secuencia principal:** | 1. El Operador dará clic en el botón Actualizar Estado.<br>2. El sistema mostrará formulario de búsqueda de incidentes por número de ticket.<br>3. El Operador ingresará el número de ticket del incidente.<br>4. El sistema obtiene los datos del incidente según el ticket ingresado.<br>5. El operador decide actualizar el incidente según sea el caso presionando el botón cerrado o incidente.<br>6. El sistema actualiza el campo estado en la base de datos.<br>7. El sistema mostrará mensaje “El estado del incidente se actualizó correctamente”. |
| **Errores / alternativas** | 1. El sistema mostrará mensaje de error “El número de ticket para actualizar, no se encuentra en la BD” cuando el número de ticket sea erróneo. |
| **Post condición:** | Estado de incidente actualizado. |
| **Notas** | |

Tabla 7. Especificación de caso de uso: ActualizarEstadoDeIncidente
Fuente: Elaboración propia.

## Diagrama de Actividades: ActualizarEstadoDeIncidente

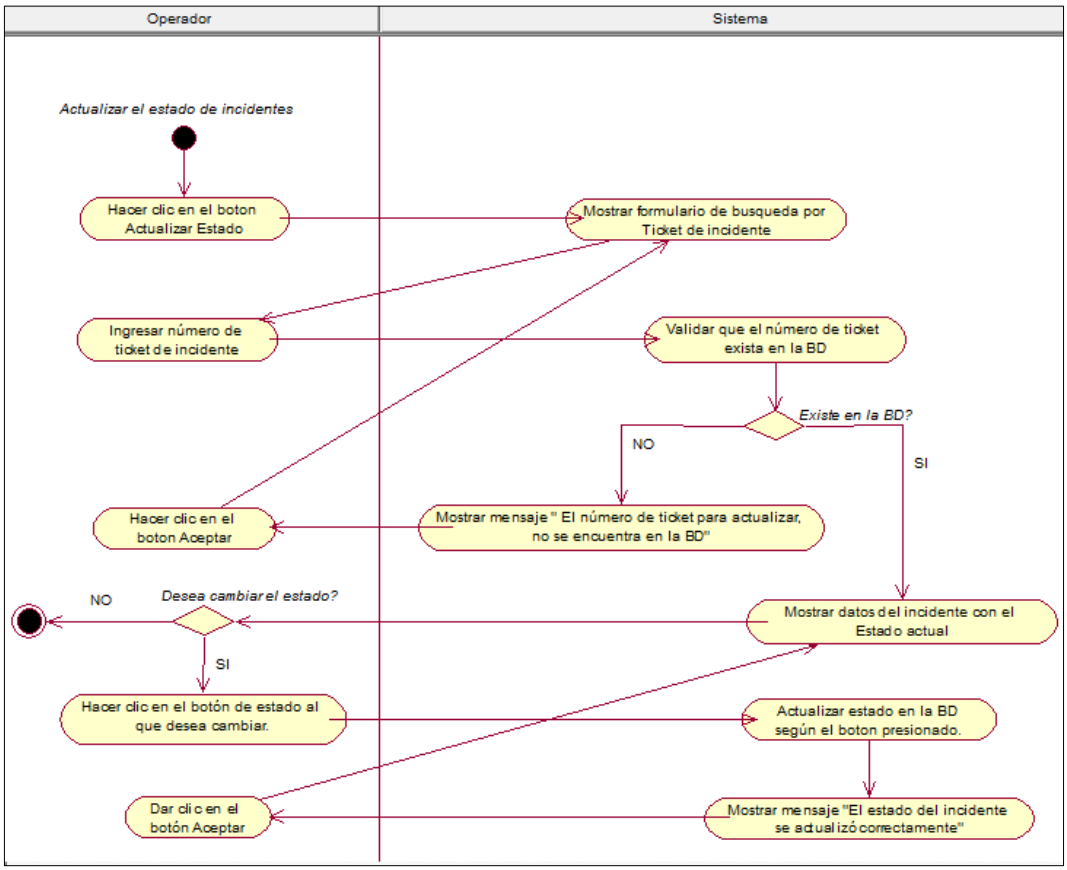



Figura 44. Diagrama de Actividades: ActualizarEstadoDeIncidente
Fuente: Elaboración propia.

## Diagrama de Objetos: ActualizarEstadoDeIncidente

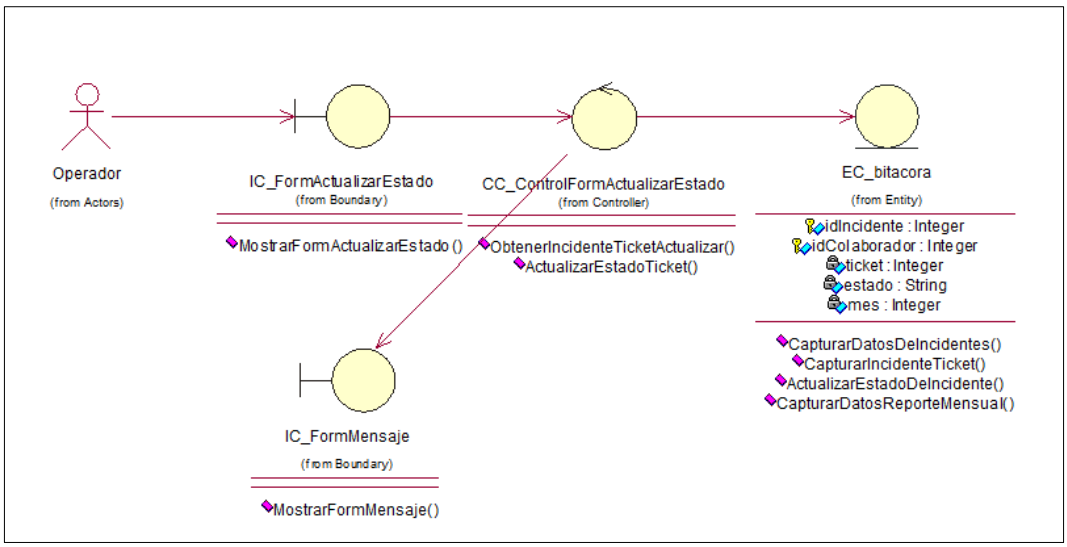



Figura 45. Diagrama de Objetos: ActualizarEstadoDeIncidente
Fuente: Elaboración propia.

## Diagrama de Secuencia: ActualizarEstadoDeIncidente

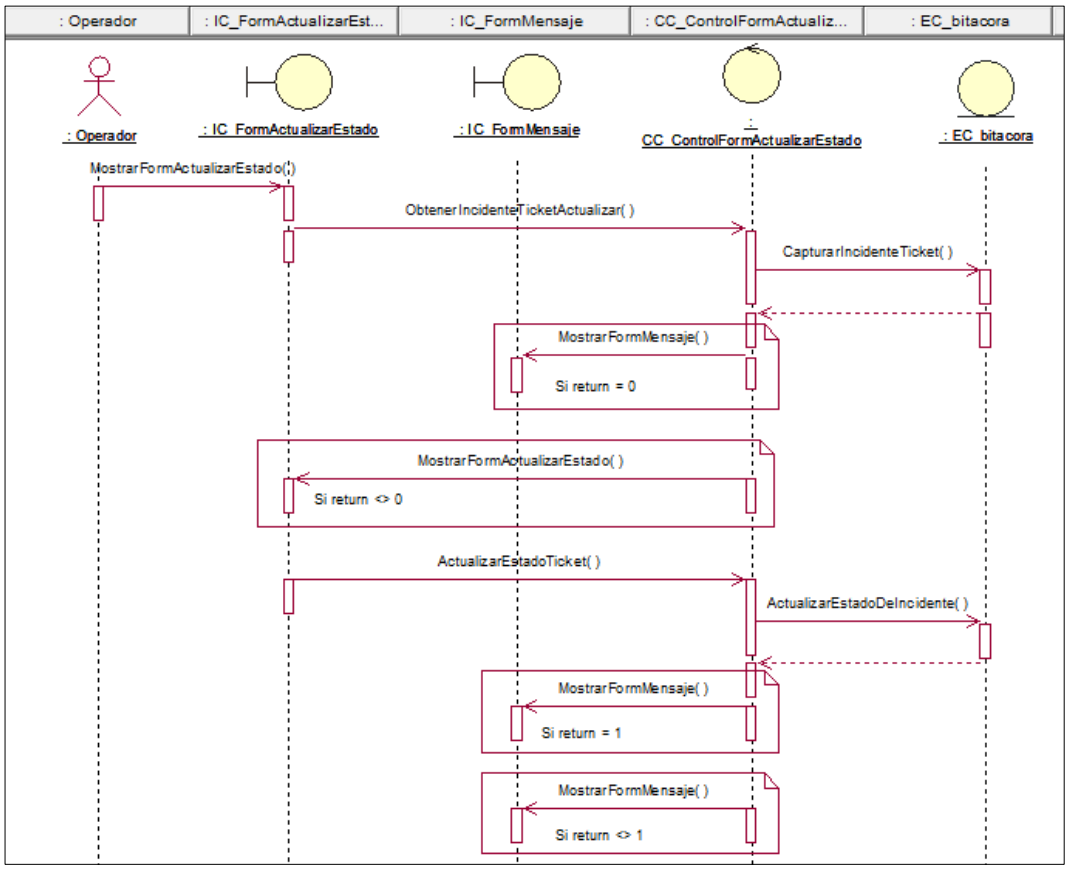



Figura 46. Diagrama de Secuencia: ActualizarEstadoDeIncidente
Fuente: Elaboración propia.

## g) VerListaGeneralDeIncidentes

| | |
|---|---|
| **Nombre:** | VerListaGeneralDeIncidentes |
| **Descripción:** | El Operador SOC desea ver la lista general de incidentes del mes actual. |
| **Precondición:** | Incidentes registrados. |
| **Secuencia principal:** | 1. El Operador dará clic en el botón Lista De Incidentes.<br>2. El sistema obtiene los datos de todos los incidentes registrados del mes actual.<br>3. El sistema muestra la lista general de los incidentes notificados del mes. |
| **Errores / alternativas** | 1. El sistema mostrará mensaje “Error: No se encontraron registros en la BD” en caso de que no se encuentre ningún incidentes registrado en la base de datos del mes actual. |
| **Post condición:** | Ninguna. |
| **Notas** | |

Tabla 8. Especificación de caso de uso: VerListaGeneralDeIncidentes
Fuente: Elaboración propia.

## Diagrama de Actividades: VerListaGeneralDeIncidentes

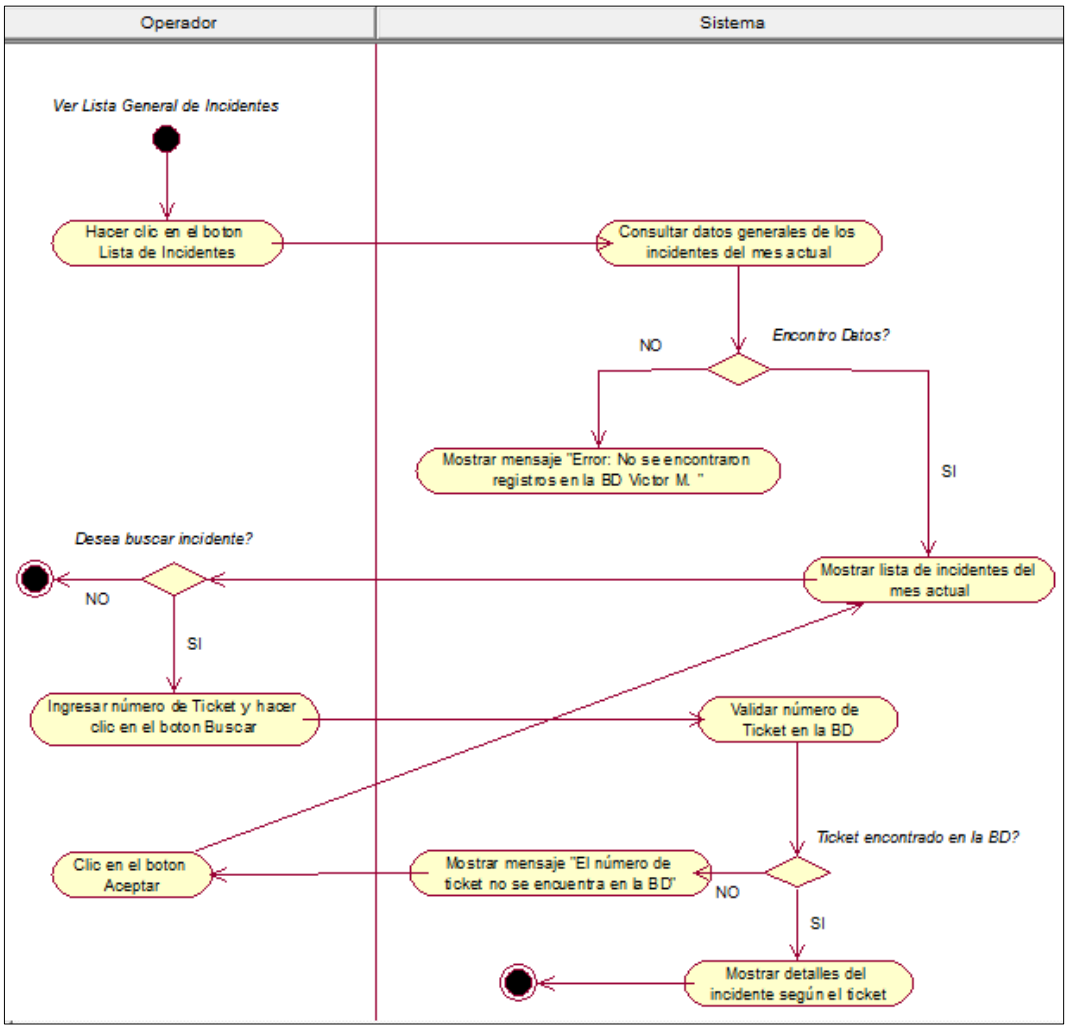



Figura 47. Diagrama de Actividades: VerListaGeneralDeIncidente
Fuente: Elaboración propia.

## Diagrama de Objetos: VerListaGeneralDeIncidentes

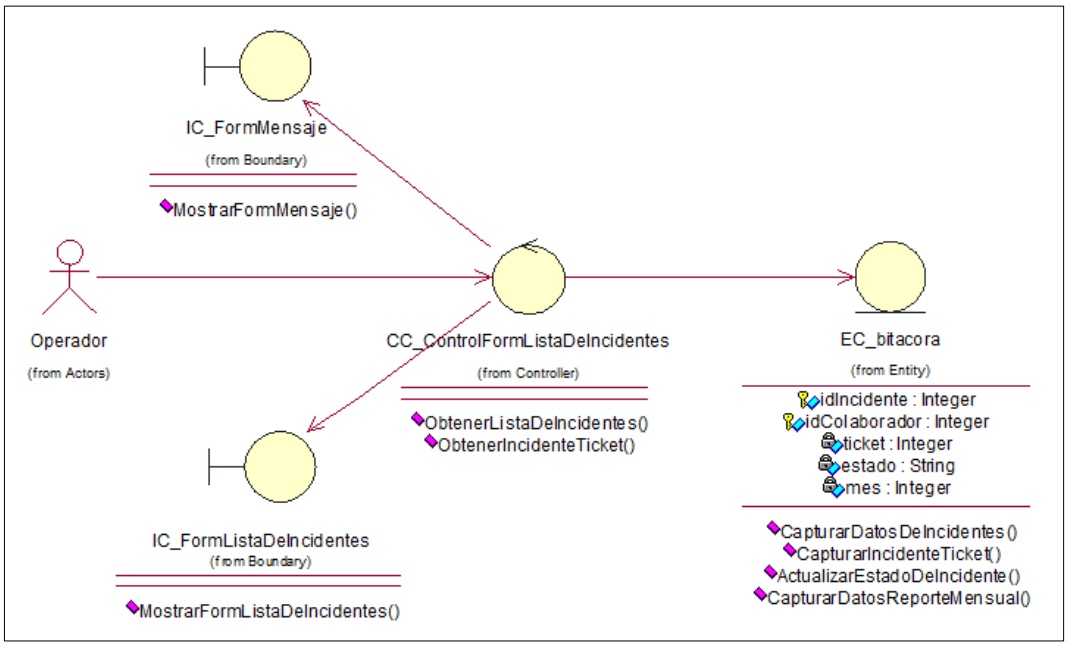



Figura 48. Diagrama de Objetos: VerListaGeneralDeIncidentes
Fuente: Elaboración propia.

## Diagrama de Secuencia: VerListaGeneralDeIncidentes

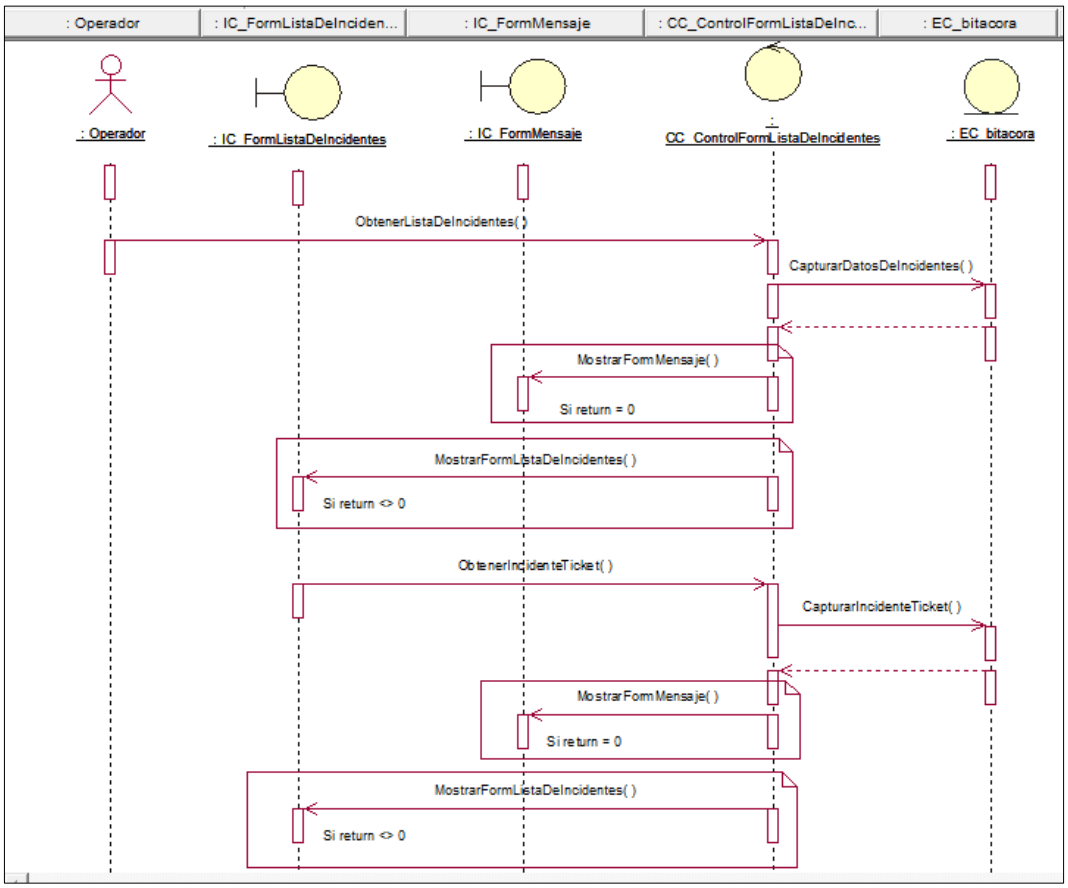



Figura 49. Diagrama de Secuencia: VerListaGeneralDeIncidente
Fuente: Elaboración propia.

## h) NotificarIncidentesDeInformación

| | |
|---|---|
| **Nombre:** | NotificarIncidentesDeInformación |
| **Descripción:** | El Operador SOC desea notificar nuevo incidente. |
| **Precondición:** | Ninguna. |
| **Secuencia principal:** | 1. El Operador dará clic en botón Notificar Incidente.<br>2. El sistema mostrará formulario para registra y notificar nuevo incidente.<br>3. El operador ingresa los datos del incidente y dará clic en el botón Aceptar Incidente.<br>4. El sistema carga los datos complementarios de notificación según el número de registro ingresado del colaborador.<br>5. El sistema mostrará modelo de correo electrónico de notificación.<br>6. El Operador dará clic en el botón Notificar Incidente.<br>7. El sistema registra los datos del incidente y envía correo electrónico de notificación al Jefe directo del colaborador.<br>8. El sistema mostrará mensaje “El correo se envió correctamente”. |
| **Errores / alternativas** | 1. El sistema mostrará mensaje “El número de registro no se encuentra en la BD” cuando el número de registro ingresado del colaborador sea erróneo. |
| **Post condición:** | Correo de notificación enviado. |
| **Notas** | |

Tabla 9. Especificación de caso de uso: NotificarIncidentesDeInformación
Fuente: Elaboración propia.

## Diagrama de Actividades: NotificarIncidentesDeInformación

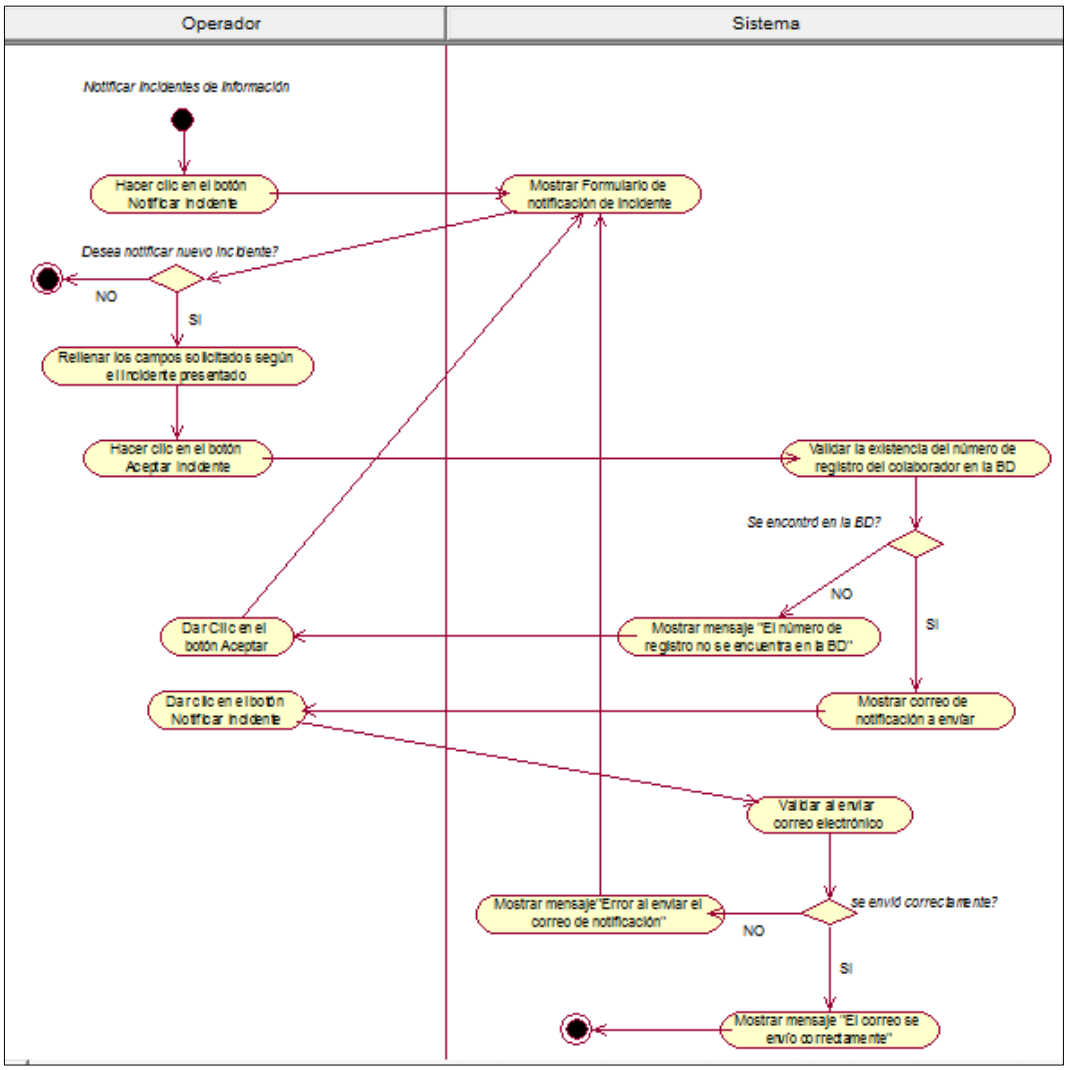



Figura 50. Diagrama de Actividades: NotificarIncidentesDeInformación
Fuente: Elaboración propia.

## Diagrama de Objetos: NotificarIncidentesDeInformación

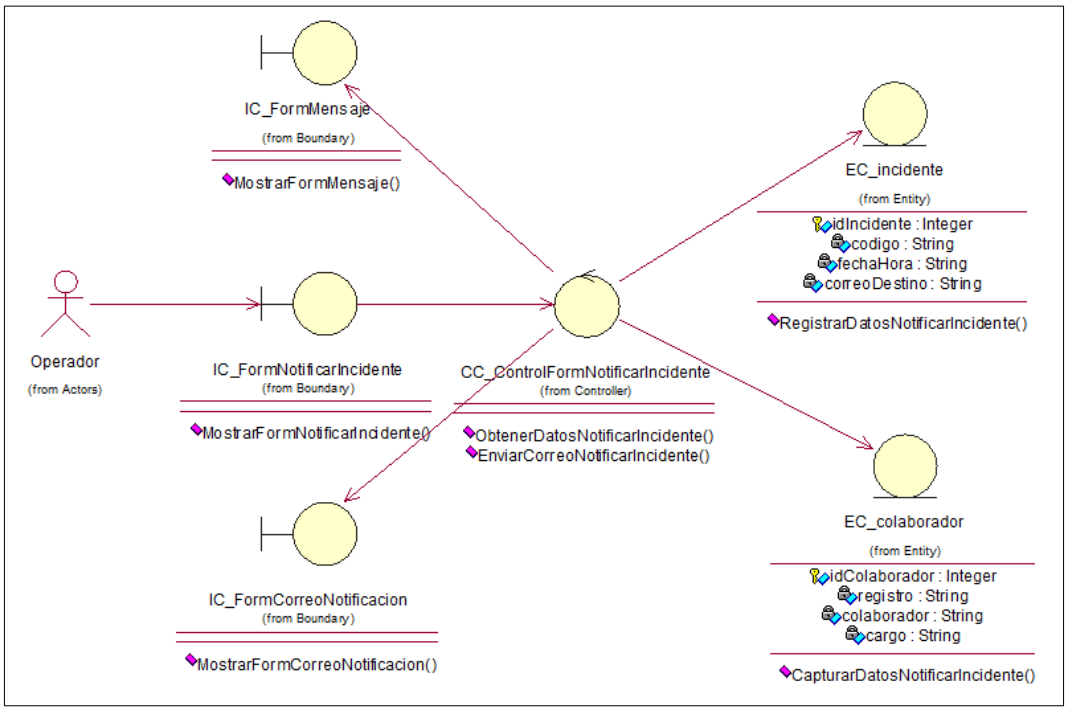



Figura 51. Diagrama de Objetos: NotificarIncidentesDeInformación
Fuente: Elaboración propia.

## Diagrama de Secuencia: NotificarIncidentesDeInformación

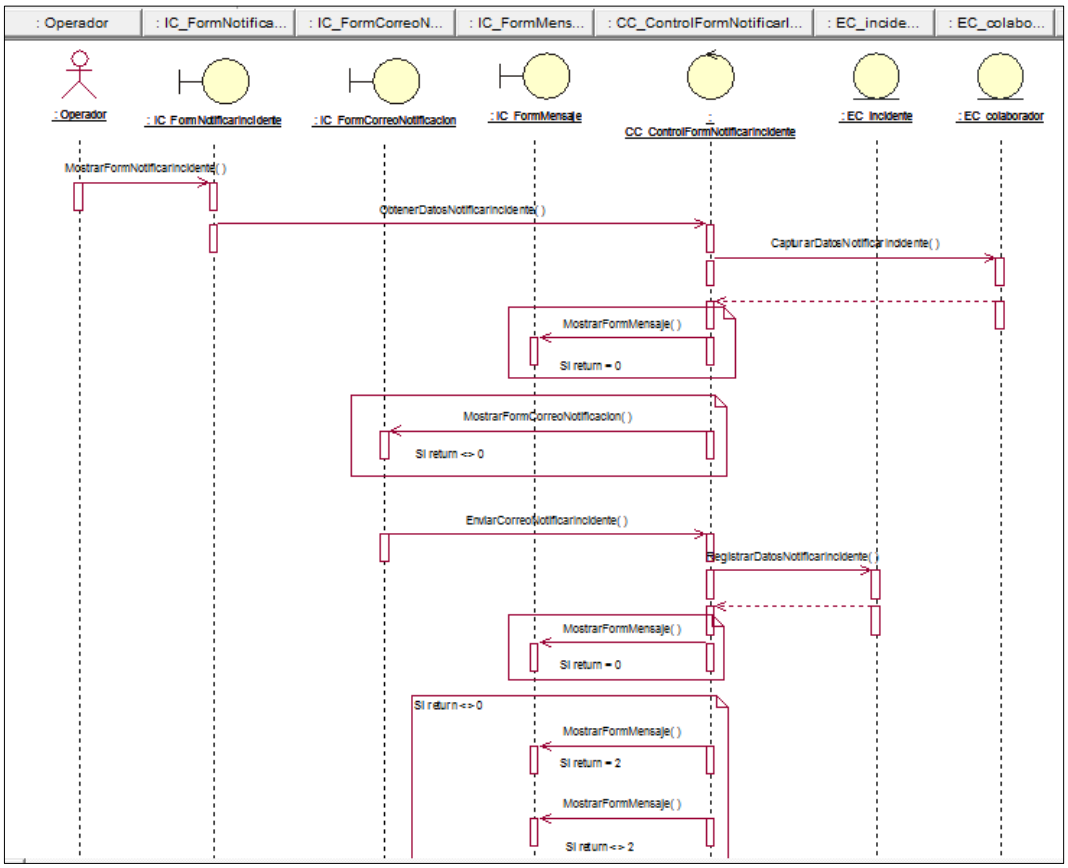



Figura 52. Diagrama de Secuencia: NotificarIncidentesDeInformación
Fuente: Elaboración propia.

### 3.2.3. Diagrama de Clases

En la siguiente figura se describe la estructura del sistema.

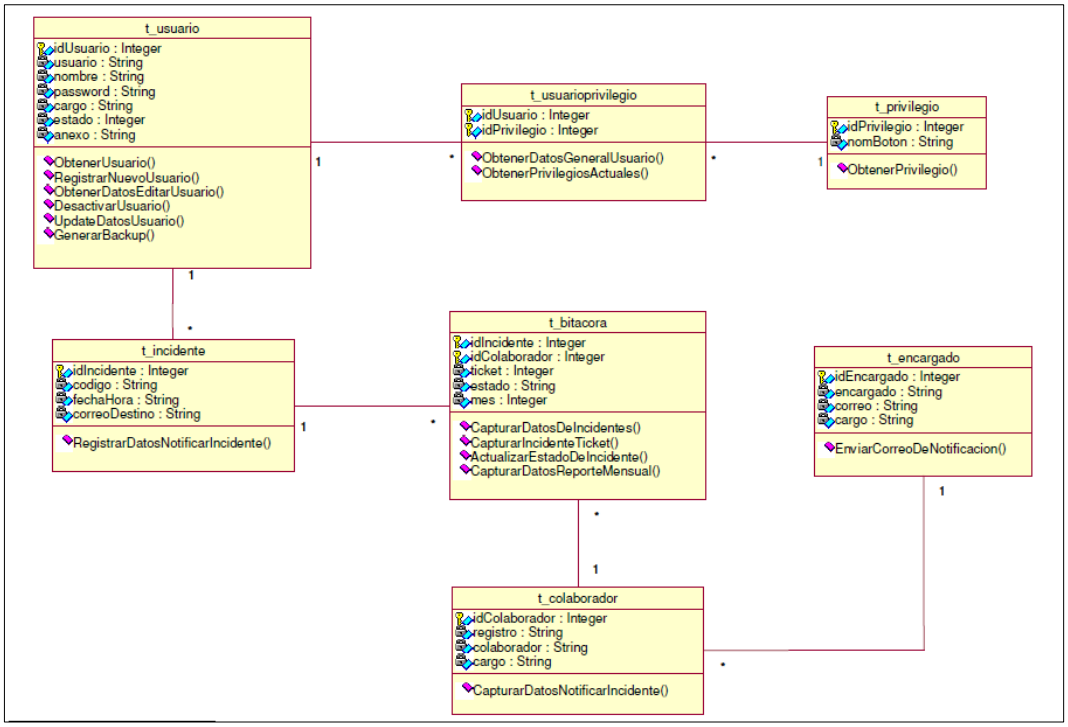



Figura 53. Diagrama de Clases.
Fuente: Elaboración propia.

### 3.2.4. Diagrama de Componentes

En la siguiente figura representa cómo el sistema de software es dividido en componentes y muestra las dependencias entre estos componentes.

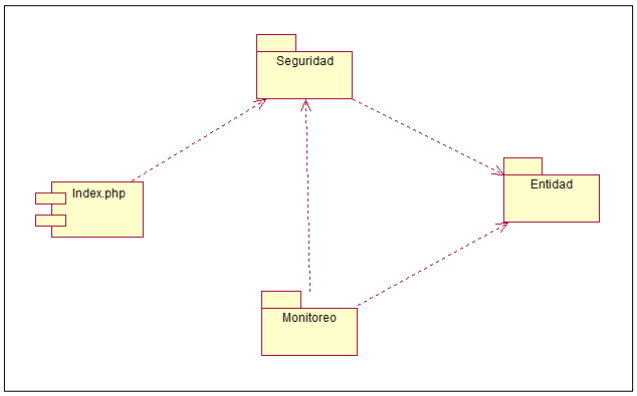



Figura 54. Diagrama de Componentes.
Fuente: Elaboración propia.

### 3.2.5. Diagrama de Despliegue

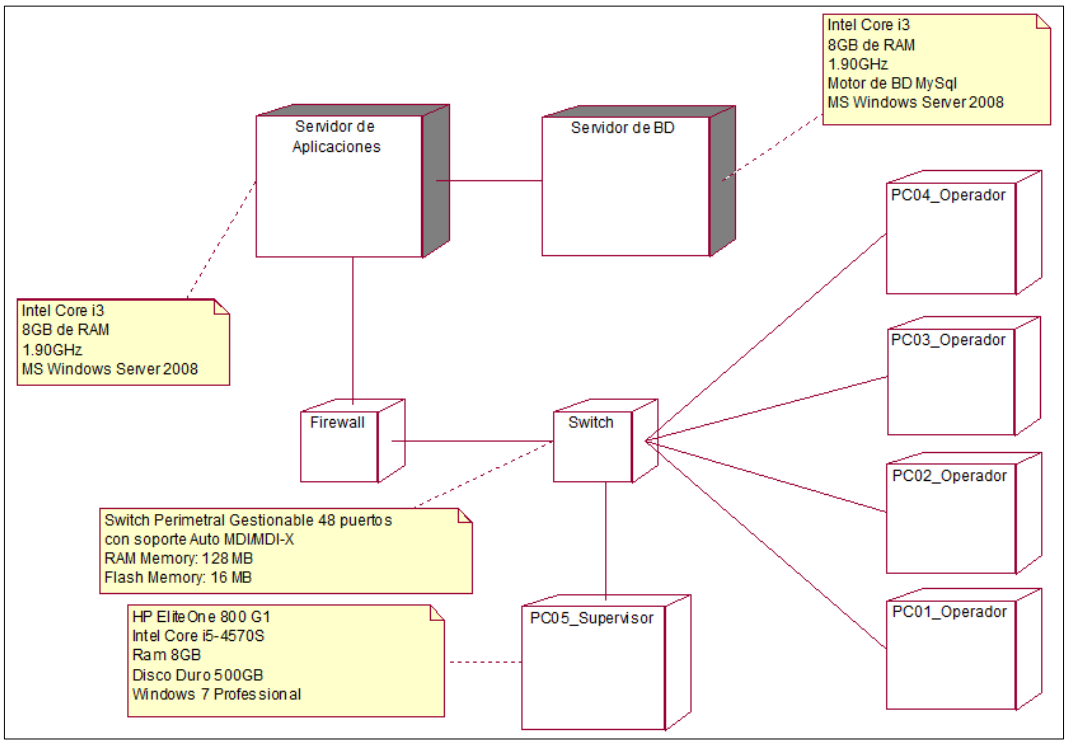



Figura 55. Diagrama de Despliegue del Sistema.
Fuente: Elaboración propia.

### 3.2.6. Modelado de datos del sistema de gestión de incidentes

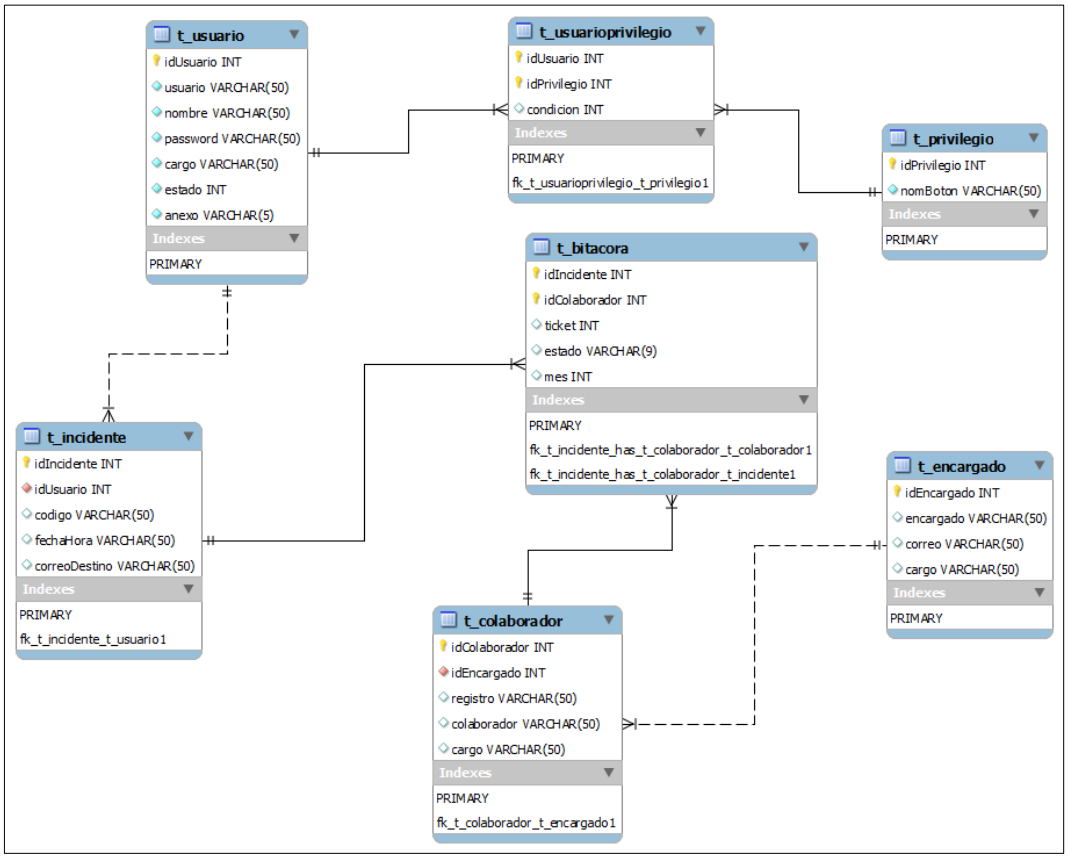



Figura 56. Modelo lógico de la Base de Datos del Sistema de Gestión de Incidentes.
Fuente: Elaboración propia.

La estructura física de cada tabla es mostrada a continuación:

| t_usuario | |
|---|---|
| CAMPO | TIPO |
| idUsuario (PK) | Integer |
| usuario | Varchar(50) |
| nombre | Varchar(50) |
| password | Varchar(50) |
| cargo | Varchar(50) |
| estado | Integer |
| anexo | Varchar(5) |

Tabla 10. Estructura de Tabla: t_usuario
Fuente: Elaboración propia.

| t_usuarioprivilegio | |
|---|---|
| CAMPO | TIPO |
| idUsuario (PK) | Integer |
| idPrivilegio (PK) | Integer |
| condicion | Integer |

Tabla 11. Estructura de Tabla: t_usuarioprivilegio
Fuente: Elaboración propia.

| t_encargado | |
|---|---|
| CAMPO | TIPO |
| idEncargado (PK) | Integer |
| encargado | Varchar(50) |
| correo | Varchar(50) |
| cargo | Varchar(50) |

Tabla 12. Estructura de Tabla: t_encargado
Fuente: Elaboración propia.

| t_incidente | |
|---|---|
| CAMPO | TIPO |
| idIncidente (PK) | Integer |
| idUsuario (FK) | Integer |
| codigo | Varchar(50) |
| fechaHora | Varchar(50) |
| correoDestino | Varchar(50) |

Tabla 13. Estructura de Tabla: t_incidente
Fuente: Elaboración propia.

| t_colaborador | |
|---|---|
| CAMPO | TIPO |
| idColaborador (PK) | Integer |
| idEncargado (FK) | Integer |
| registro | Varchar(50) |
| colaborador | Varchar(50) |
| cargo | Varchar(50) |

Tabla 14. Estructura de Tabla: t_colaborador
Fuente: Elaboración propia.

| t_bitacora | |
|---|---|
| CAMPO | TIPO |
| idIncidente (PK) | Integer |
| idColaborador (PK) | Integer |
| ticket | Integer |
| estado | Varchar(9) |
| mes | Integer |

Tabla 15. Estructura de Tabla: t_bitacora
Fuente: Elaboración propia.

| t_privilegio | |
|---|---|
| CAMPO | TIPO |
| idPrivilegio (PK) | Integer |
| nomBoton | Varchar(50) |

Tabla 16. Estructura de Tabla: t_privilegio
Fuente: Elaboración propia.

### 3.2.7. Interfaces gráficas del sistema de gestión de incidentes

**Pantalla de logeo del sistema de gestión de incidentes.**


Figura 57. Pantalla de inicio de sesión del sistema de gestión de incidentes
Fuente: Elaboración propia.

**Formulario que visualiza el Operador SOC para Notificar Incidentes.**


Figura 58. Pantalla de formulario de notificación de incidentes
Fuente: Elaboración propia.

**Menú del usuario según los privilegios asignados.**

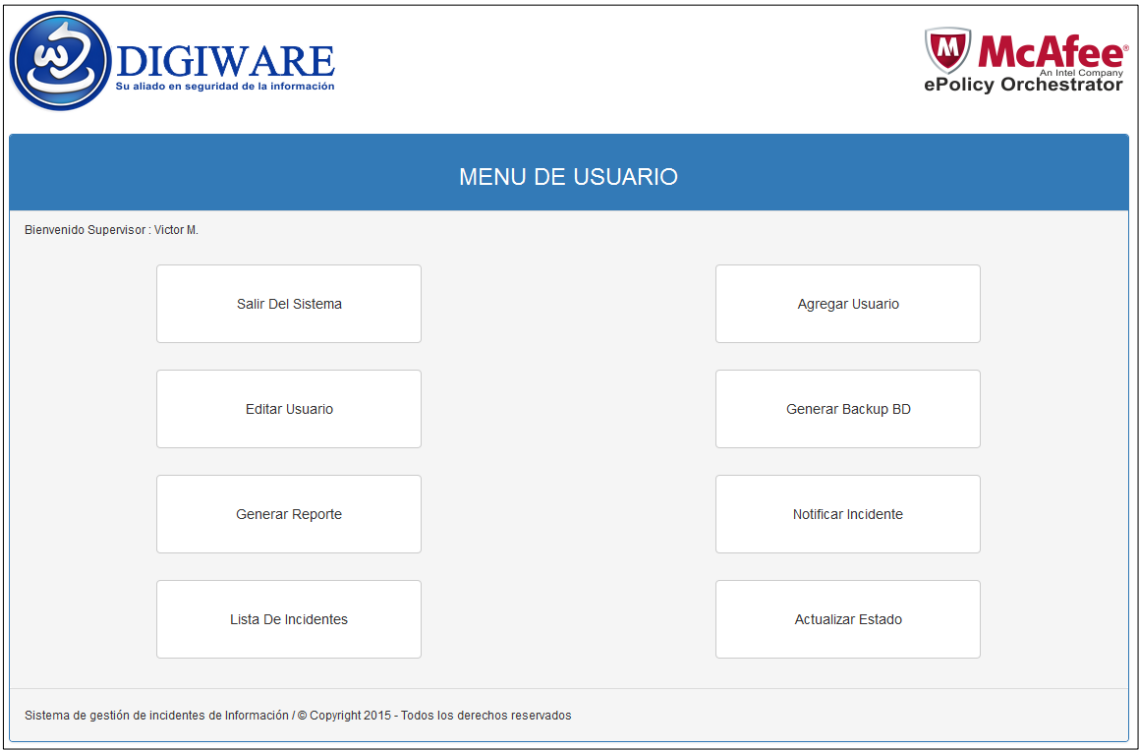



Figura 59. Pantalla de menú de usuario del sistema de gestión de incidentes.
Fuente: Elaboración propia.

**Formulario que visualiza el Operador SOC para actualizar el estado de los casos notificados.**

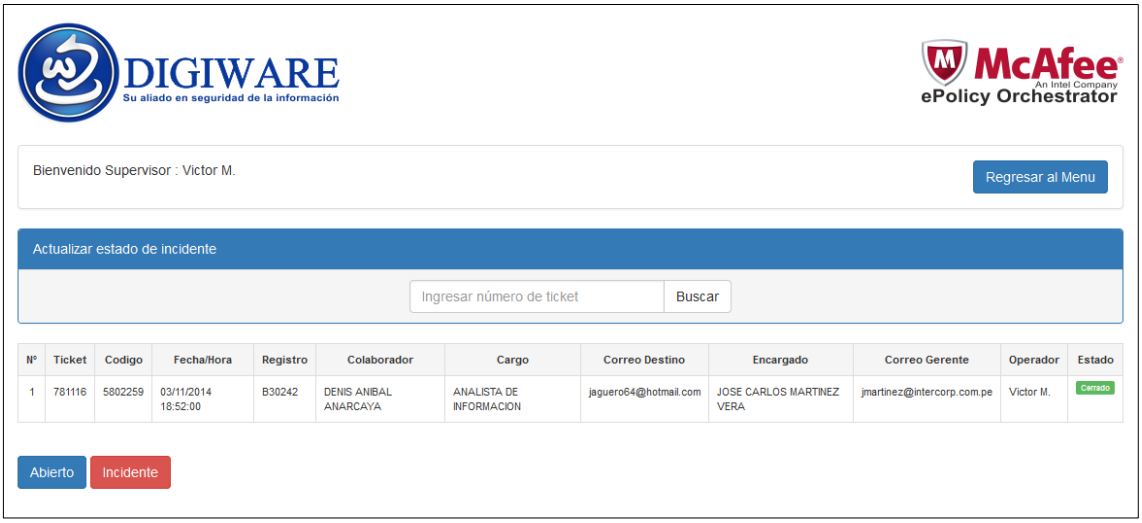



Figura 60. Pantalla de actualización de estado de los casos notificados.
Fuente: Elaboración propia.

**Formulario que visualiza el Operador SOC para notificar al Jefe directo del Colaborador que incurrió en el incidente.**

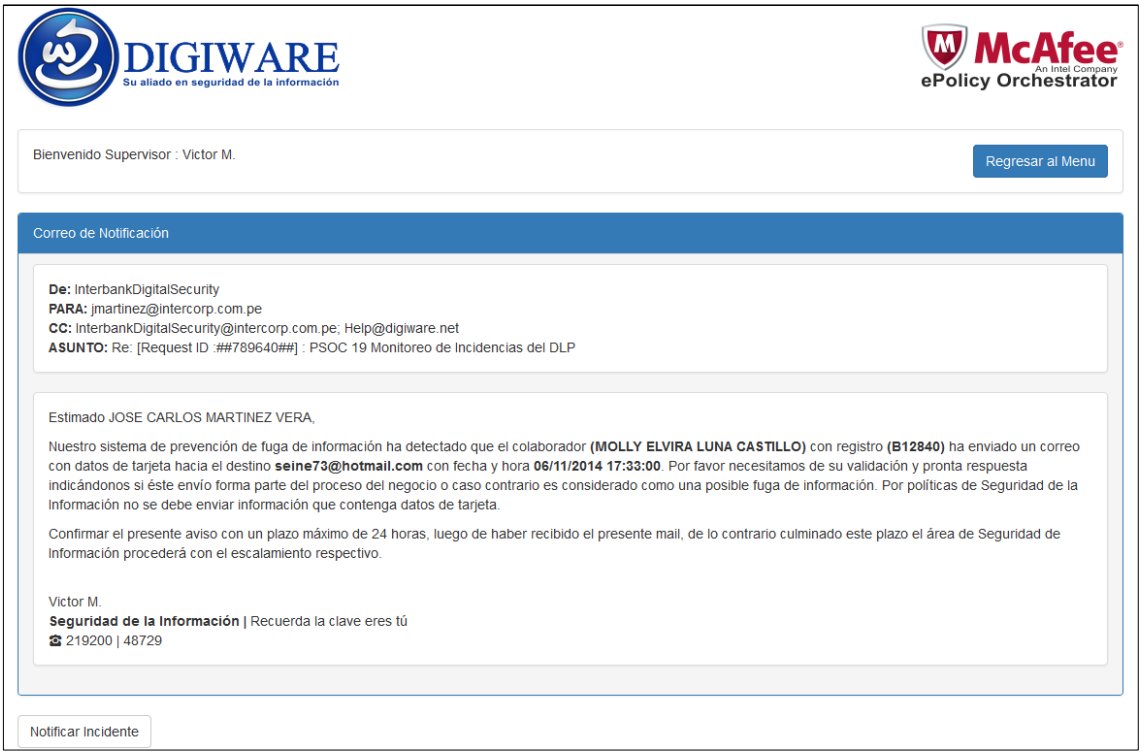
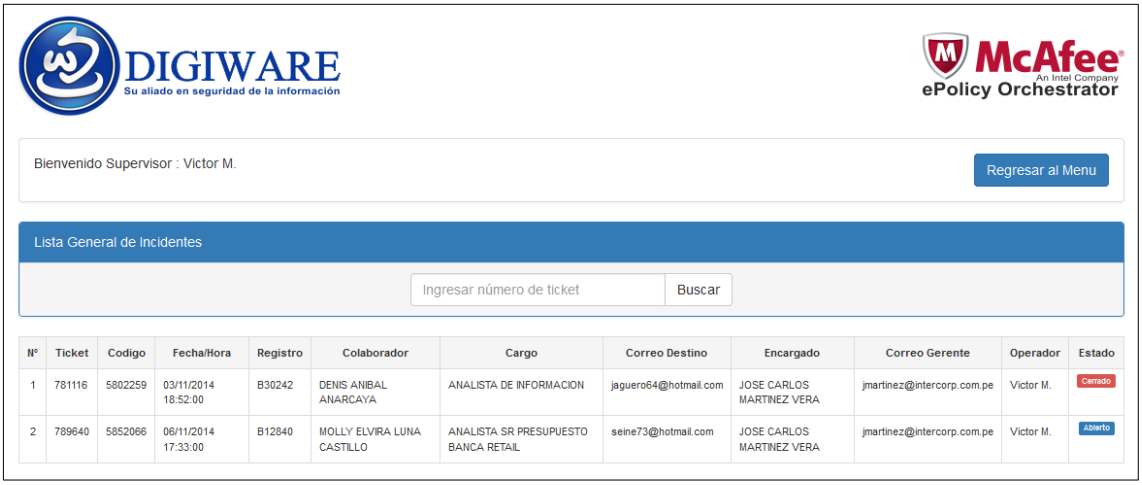



Figura 61. Pantalla de notificación del incidente al jefe directo del colaborador.
Fuente: Elaboración propia.

**Lista general de incidentes del mes actual que visualiza el Operador SOC.**




| N° | Ticket | Codigo | Fecha/Hora | Registro | Colaborador | Cargo | Correo Destino | Encargado | Correo Gerente | Operador | Estado |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 781116 | 5802259 | 03/11/2014 18:52:00 | B30242 | DENIS ANIBAL ANARCAYA | ANALISTA DE INFORMACION | jaguero64@hotmail.com | JOSE CARLOS MARTINEZ VERA | jmartinez@intercorp.com.pe | Victor M. | Cerrado |
| 2 | 789640 | 5852066 | 06/11/2014 17:33:00 | B12840 | MOLLY ELVIRA LUNA CASTILLO | ANALISTA SR PRESUPUESTO BANCA RETAIL | seine73@hotmail.com | JOSE CARLOS MARTINEZ VERA | jmartinez@intercorp.com.pe | Victor M. | Abierto |

Figura 62. Pantalla de lista general de incidentes del mes.
Fuente: Elaboración propia.

**Formulario que visualiza el Supervisor para agregar nuevo usuario.**

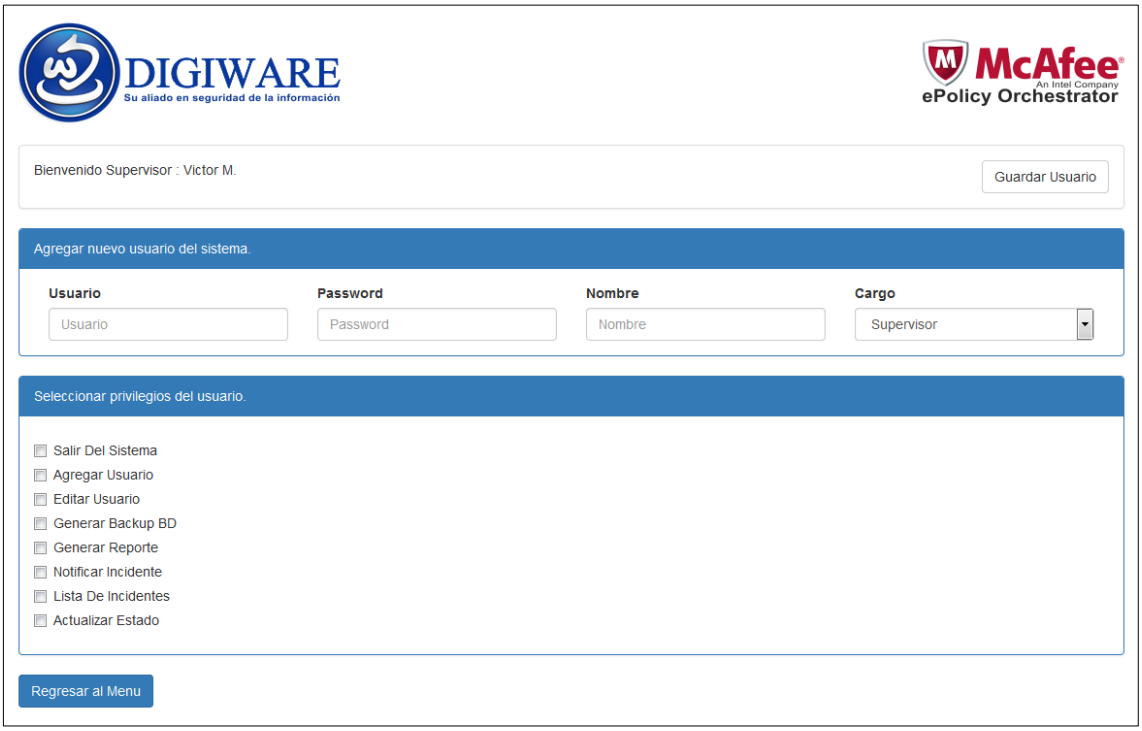



Figura 63. Pantalla de agregar nuevo usuario al sistema de gestión de incidentes.
Fuente: Elaboración propia.

**Formulario que visualiza el supervisor SOC para editar o eliminar a los usuarios del sistema.**

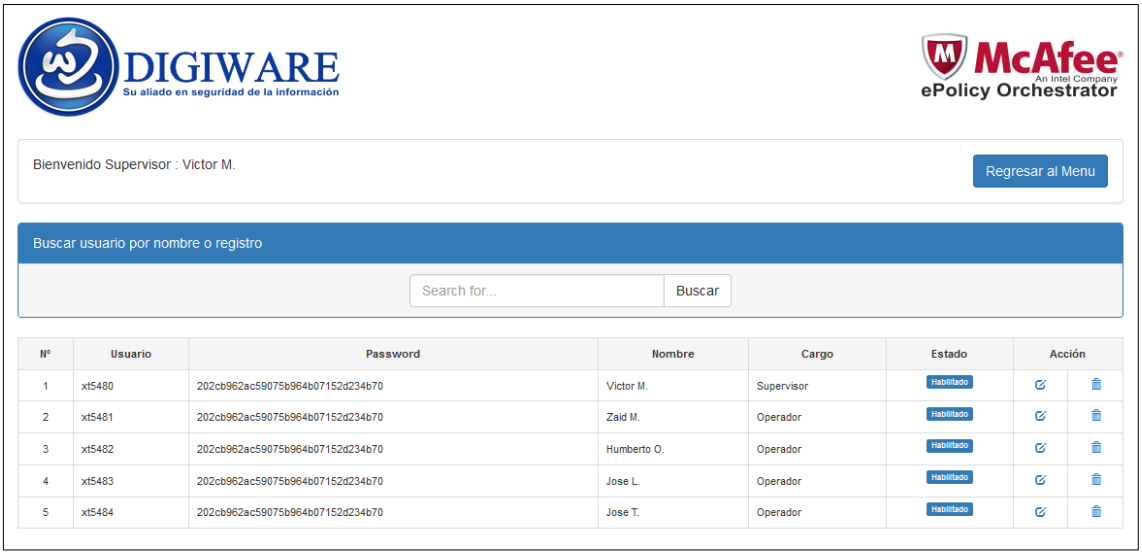



Figura 64. Pantalla de editar o eliminar usuarios del sistema de gestión de incidentes.
Fuente: Elaboración propia.

**Formulario con los datos actuales del usuario del sistema a Editar.**

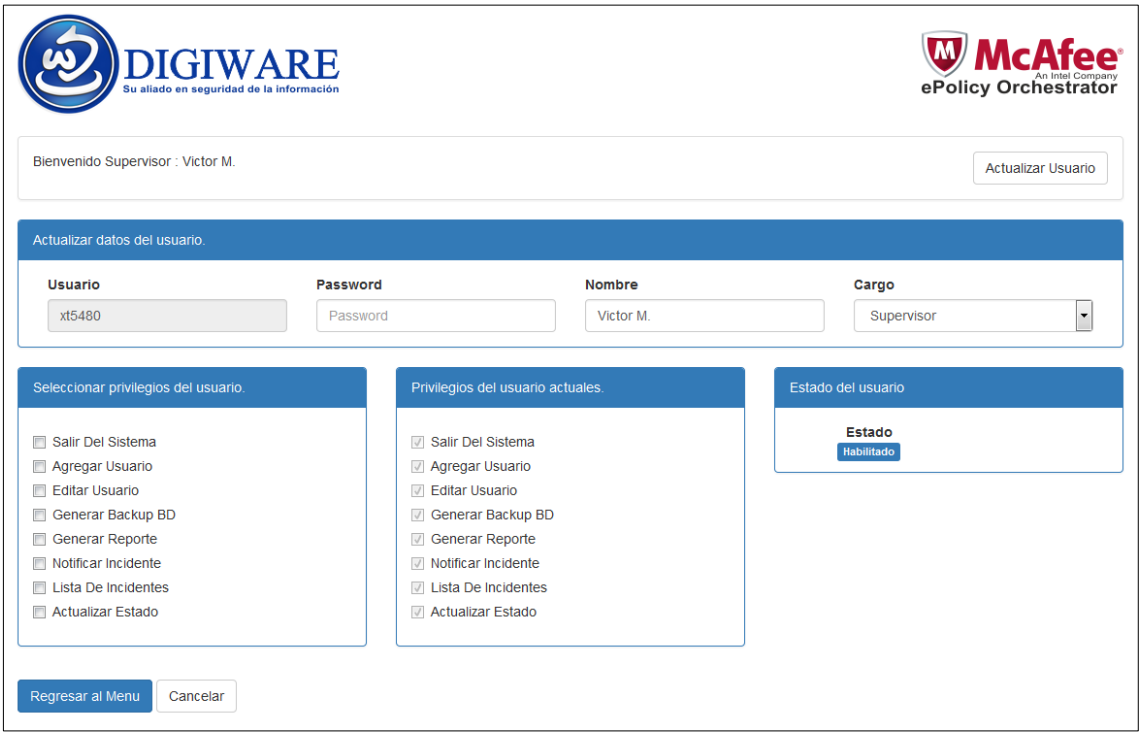
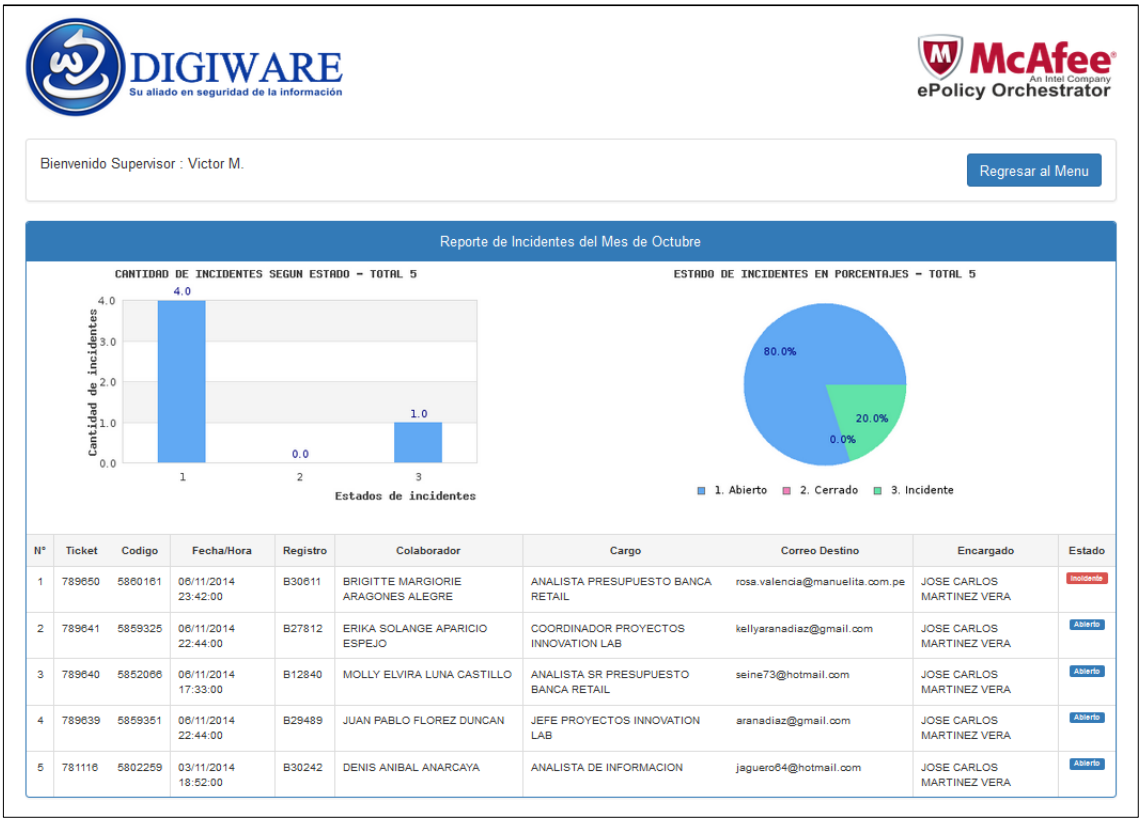



Figura 65. Pantalla de actualizar datos de usuario del sistema de gestión de incidentes.
Fuente: Elaboración propia.

**Consulta del sistema cuando se desea Eliminar un usuario del sistema, visto por el Supervisor SOC.**


Figura 66. Pantalla de consultar la eliminación del usuario del sistema de gestión de incidentes.
Fuente: Elaboración propia.

**Reporte de los casos de incidentes del mes para ser exportado en Excel o PDF, visto por el Supervisor SOC.**




| N° | Ticket | Codigo | Fecha/Hora | Registro | Colaborador | Cargo | Correo Destino | Encargado | Estado |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 789650 | 5860161 | 06/11/2014 23:42:00 | B30611 | BRIGITTE MARGIORIE ARAGONES ALEGRE | ANALISTA PRESUPUESTO BANCA RETAIL | rosa.valencia@manuelita.com.pe | JOSE CARLOS MARTINEZ VERA | Incidente |
| 2 | 789641 | 5859325 | 06/11/2014 22:44:00 | B27812 | ERIKA SOLANGE APARICIO ESPEJO | COORDINADOR PROYECTOS INNOVATION LAB | kellyaranadiaz@gmail.com | JOSE CARLOS MARTINEZ VERA | Abierto |
| 3 | 789640 | 5852066 | 06/11/2014 17:33:00 | B12840 | MOLLY ELVIRA LUNA CASTILLO | ANALISTA SR PRESUPUESTO BANCA RETAIL | seine73@hotmail.com | JOSE CARLOS MARTINEZ VERA | Abierto |
| 4 | 789639 | 5859351 | 06/11/2014 22:44:00 | B29489 | JUAN PABLO FLOREZ DUNCAN | JEFE PROYECTOS INNOVATION LAB | aranadiaz@gmail.com | JOSE CARLOS MARTINEZ VERA | Abierto |
| 5 | 781116 | 5802259 | 03/11/2014 18:52:00 | B30242 | DENIS ANIBAL ANARCAYA | ANALISTA DE INFORMACION | jaguero64@hotmail.com | JOSE CARLOS MARTINEZ VERA | Abierto |

Figura 67. Pantalla de reporte de los casos de incidentes del mes.
Fuente: Elaboración propia.

**Mensaje del sistema al Generar el Backup de la Base de Datos visto por el Supervisor SOC.**

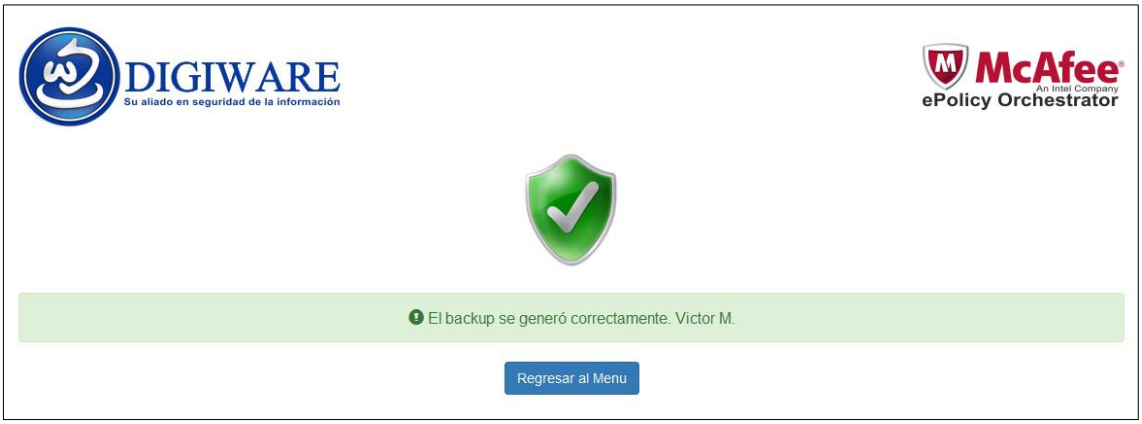



Figura 68. Pantalla de mensaje de confirmación del sistema de gestión de incidentes.
Fuente: Elaboración propia.

**Mensaje de error de Inicio de Sesión al sistema.**


Figura 69. Pantalla de mensaje de error del sistema de gestión de incidentes.
Fuente: Elaboración propia.

### 3.2.8. Implementación del sistema de gestión de incidentes

#### a) Sistema gestor de base de datos Mysql.

MySQL es un sistema gestor de bases de datos relacionales rápido, sólido y flexible. Es idóneo para la creación de bases de datos con acceso desde páginas web dinámicas, así como para la creación de cualquier otra solución que implique el almacenamiento de datos, posibilitando realizar múltiples y rápidas consultas. Está desarrollado en C y C++, facilitando su integración en otras aplicaciones desarrolladas también en esos lenguajes.

Es un sistema cliente/servidor, por lo que permite trabajar como servidor multiusuario y de subprocesamiento múltiple, o sea, cada vez que se crea una conexión con el servidor, el programa servidor establece un proceso para manejar la solicitud del cliente, controlando así el acceso simultáneo de un gran número de usuarios a los datos y asegurando el acceso a usuarios autorizados solamente. Es uno de los sistemas gestores de bases de datos más utilizado en la actualidad, utilizado por grandes corporaciones como Yahoo! Finance, Google, Motorola, entre otras.

**b) Servidor web Apache.**

Apache es software libre y el servidor web más popular. Algunos sondeos realizados demuestran que más del 70% de los sitios web en Internet están manejados por Apache, haciéndolo más extensamente usado que todos los otros servidores web juntos.

Apache es un proyecto de la Fundación de Software Apache, con el objetivo de suministrar un servidor seguro, eficiente, y extensible que proporcione servicios HTTP en sincronía con los estándares HTTP actuales.

Apache se caracteriza por ser un servidor web flexible, rápido y eficiente, continuamente actualizado y adaptado a los nuevos protocolos HTTP.

- Multiplataforma.
- Modular: Puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo que proporciona, y con la API de programación de módulos, para el desarrollo de módulos específicos.
- Extensible: gracias a ser modular se han desarrollado diversas extensiones entre las que destaca PHP, un lenguaje de programación del lado del servidor.

**c) Tecnología PHP**

PHP es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en el documento HTML en lugar de llamar a un archivo externo que procese los datos. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera la página Web resultante.

PHP ha evolucionado por lo que ahora incluye también una interfaz de línea de comandos que puede ser usada en aplicaciones gráficas independientes. Puede ser usado en la mayoría de los servidores web al igual que en casi todos los sistemas operativos y plataformas sin ningún costo.

**d) Rational Rose**

Es una herramienta CASE (Computer – Arded Software Engineering), traducido al español como Ingeniería Asistida por Computadora, desarrollada por Rational Corporation basada en el Lenguaje Unificado de Modelación (UML), que permite crear los diagramas que se van generando durante el proceso de Ingeniería en el Desarrollo del Software.

En la definición de sistemas, esta herramienta permite que el equipo de desarrollo entienda mejor el problema, que identifique las necesidades del cliente en forma más efectiva y comunique la solución propuesta de forma más clara.

Rational permite completar una gran parte de las disciplinas (flujos fundamentales) de RUP tales como:

- Captura de requisitos.
- Análisis y diseño.
- Implementación
- Control de cambios y gestión de configuración.

**e) MySql Workbench**

Es una herramienta visual de diseño de bases de datos que integra desarrollo de software, Administración de bases de datos, diseño de bases de datos, creación y mantenimiento para el sistema de base de datos MySQL.

### 3.2.9. Definición de usuarios del sistema

Definimos los usuarios principales del sistema de gestión de incidentes de acuerdo al rol que desempeña dentro de la empresa.

- **Supervisor**

Tendrá todos los privilegios del sistema para generar los Backup de la base de datos, notificar nuevos incidente de información, ver la lista general de los incidentes presentados en el mes y actualizar el estado los casos notificados.

También podrá administrar los usuarios del sistema como editar, agregar y eliminar, de igual forma podrá obtener los reportes de los casos notificados del mes solicitados por el Jefe del área de Ingeniería de Seguridad de la Información del banco Interbank.

- **Operador**

Tendrá solo los privilegios de ver lista general de incidentes, notificar nuevos incidentes y actualizar el estado de los casos notificados.

## 3.3 Revisión y Consolidación de Resultados

### a) Comparando los indicadores de envío de correos con datos de tarjeta hacia dominios externos No Autorizados.

Número total de correos enviados mensual (TCE)= 120

- **Indicador de envío de correos no autorizados sin uso del sistema de gestión de incidentes:**

  Número de correos enviados No autorizados (CEN)= 32

  Indicador de correos enviados Sin autorización (CEN)/(TCE)*100= 26,67%

- **Indicador de envío de correos no autorizados con uso del sistema de gestión de incidentes:**

  Número de correos enviados No autorizados (CEN)= 14

  Indicador de correos enviados Sin autorización (CEN)/(TCE)*100= 11,67%

Gráfica de comparación entre los indicadores de envío de correos con datos de tarjeta del mes de diciembre del 2014 y julio de 2015.

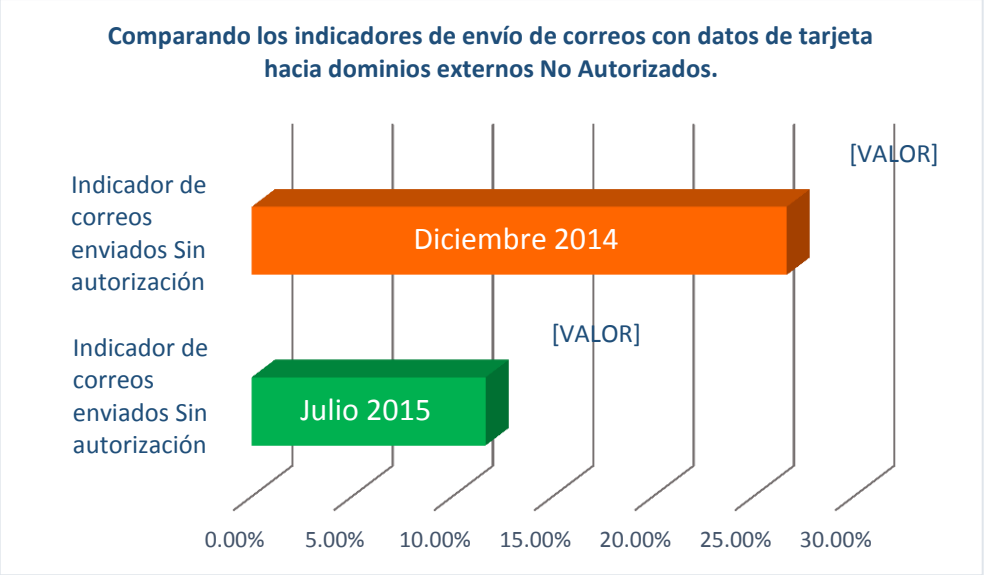



Figura 70. Gráfica de comparación de indicadores del mes de diciembre del 2014 y julio del 2015.
Fuente: Elaboración propia.

Se observa, las cantidades de Incidentes generados por el envío de correos con datos de tarjetas hacia dominios externos se reducen de 32 incidentes a 14 incidentes, se demuestra, que con el uso del sistema de gestión de incidentes los envíos de correos No Autorizados a dominios externos se reducen de un 26,67% a un 11,67%.

## b) Comparando el tiempo promedio de exposición de los incidentes.

Tiempo promedio de exposición de los incidentes notificados sin el uso del sistema de gestión (noviembre del 2014).

| Notificaciones de incidentes del mes de Noviembre del 2014 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Día | Operador - Inic | Ticket Digiware | ID | Hora de envío | DESTINO | Operador - Fin | Condición | Hora de Apertura | Hora de Cierre | Tiempo de Exposición |
| 1 | Jose T. | 773447 | 5779929 | 31/10/2014 23:02 | charo514@hotmail.com | Zaid M. | Cerrado | 01/11/2014 5:17 | 06/11/2014 10:39 | 05 d 05 h 22 min |
| 2 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ |
| 3 | Jose T. | 786820 | 5799367 | 03/11/2014 16:51 | kconta11@hotmail.com | Zaid M. | Cerrado | 06/11/2014 0:00 | 07/11/2014 10:11 | 01 d 10 h 11 min |
| | Jose T. | 781116 | 5802259 | 03/11/2014 18:52 | jaguero64@hotmail.com | Jose T. | Cerrado | 06/11/2014 12:54 | 07/11/2014 11:23 | 22 h 29 min |
| 4 | Jose T. | 784388 | 5815430 | 04/11/2014 16:11 | danicaf@hotmail.com | Jose T. | Cerrado | 07/11/2014 12:15 | 10/11/2014 10:23 | 02 d 22 h 08 min |
| | Jose T. | 784389 | 5822315 | 04/11/2014 18:14 | jccm@cajatrujillo.com.pe | Zaid M. | Cerrado | 05/11/2014 5:15 | 07/11/2014 10:17 | 02 d 05 h 02 min |
| | Jose T. | 784390 | 5826591 | 04/11/2014 22:33 | leandro_21_16@hotmail.com | Jose T. | Cerrado | 05/11/2014 5:35 | 07/11/2014 7:45 | 02 d 02 h 10 min |
| | Jose T. | 784391 | 5827350 | 04/11/2014 21:30 | tania@terrawari.com | Zaid M. | Cerrado | 05/11/2014 5:23 | 13/11/2014 12:14 | 08 d 06 h 51 min |
| | Jose T. | 784392 | 5827351 | 04/11/2014 9:57 | tania@terrawari.com | Zaid M. | Cerrado | 05/11/2014 5:45 | 13/11/2014 10:26 | 08 d 04 h 41 min |
| 5 | Jose T. | 787224 | 5836505 | 05/11/2014 16:04 | kritobh@gmail.com | Zaid M. | Cerrado | 06/11/2014 5:28 | 06/11/2014 10:02 | 04 h 34 min |
| | Jose T. | 787229 | 5846178 | 06/11/2014 0:18 | xmariocux@hotmail.com | Zaid M. | Cerrado | 06/11/2014 5:43 | 06/11/2014 9:57 | 04 h 14 min |
| 6 | Zaid M. | 789636 | 5849744 | 06/11/2014 15:54 | jsanchezgo@mibanco.com.pe | Zaid M. | Cerrado | 07/11/2014 1:06 | 07/11/2014 10:53 | 09 h 47 min |
| | Zaid M. | 789639 | 5850661 | 06/11/2014 16:38 | yssayunis@hotmail.com | Zaid M. | Cerrado | 07/11/2014 2:09 | 07/11/2014 10:24 | 08 h 15 min |
| | Zaid M. | 789640 | 5852066 | 06/11/2014 17:33 | seine73@hotmail.com | Zaid M. | Cerrado | 07/11/2014 2:27 | 07/11/2014 10:26 | 07 h 59 min |
| | Zaid M. | 789641 | 5859325 | 06/11/2014 22:44 | kellyaranadiaz@gmail.com | Zaid M. | Cerrado | 07/11/2014 2:35 | 07/11/2014 10:30 | 07 h 55 min |
| | Zaid M. | 789642 | 5859358 | 06/11/2014 22:58 | tevez.a@hotmail.com | Zaid M. | Cerrado | 07/11/2014 2:45 | 07/11/2014 10:02 | 07 h 17 min |
| | Zaid M. | 789649 | 5859668 | 06/11/2014 21:12 | fabio181255@hotmail.com | Zaid M. | Cerrado | 07/11/2014 3:03 | 07/11/2014 10:08 | 07 h 05 min |
| | Zaid M. | 789650 | 5860161 | 06/11/2014 23:42 | rosa.valencia@manuelita.com.pe | Zaid M. | Cerrado | 07/11/2014 3:14 | 07/11/2014 10:05 | 06 h 51 min |
| | Zaid M. | 789651 | 5860753 | 06/11/2014 21:58 | alvaro-otero@terra.com.pe | Zaid M. | Cerrado | 07/11/2014 3:24 | 13/11/2014 12:21 | 06 d 08 h 57 min |
| 7 | Zaid M. | 789652 | 5868788 | 07/11/2014 14:28 | lorbezo@aasa.com.pe | Zaid M. | Cerrado | 08/11/2014 1:22 | 11/11/2014 11:59 | 03 d 10 h 37 min |
| | Zaid M. | 789654 | 5883677 | 07/11/2014 23:02 | rosme_ri16@hotmail.com | Zaid M. | Cerrado | 08/11/2014 1:27 | 10/11/2014 10:48 | 02 d 09 h 21 min |
| 8 | Zaid M. | 792074 | 5888076 | 08/11/2014 14:31 | kellyaranadiaz@gmail.com | Zaid M. | Cerrado | 09/11/2014 12:35 | 12/11/2014 11:49 | 02 d 23 h 14 min |
| | Zaid M. | 793937 | 5893009 | 08/11/2014 15:55 | fago57@gmail.com | Zaid M. | Cerrado | 09/11/2014 12:43 | 12/11/2014 11:46 | 02 d 23 h 03 min |
| 9 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ |
| 10 | Zaid M. | 798039 | 5899907 | 10/11/2014 14:35 | kellyaranadiaz@gmail.com | Zaid M. | Cerrado | 11/11/2014 12:33 | 11/11/2014 11:56 | 23 h 23 min |
| | Zaid M. | 798042 | 5901781 | 10/11/2014 15:12 | andre.m.castro@marsh.com | Zaid M. | Cerrado | 11/11/2014 12:41 | 12/11/2014 11:59 | 23 h 18 min |
| | Zaid M. | 798043 | 5903682 | 10/11/2014 17:30 | gianchacon@hotmail.com | Zaid M. | Cerrado | 11/11/2014 12:51 | 11/11/2014 11:52 | 23 h 01 min |
| | Zaid M. | 798044 | 5903966 | 10/11/2014 15:41 | liz_4612@hotmail.com | Zaid M. | Cerrado | 11/11/2014 12:59 | 12/11/2014 12:03 | 23 h 04 min |
| 11 | Zaid M. | 799318 | 5918021 | 11/11/2014 16:51 | vanessa.montoya@apdayc.org.pe | Zaid M. | Cerrado | 12/11/2014 12:35 | 13/11/2014 10:30 | 21 h 55 min |
| | Zaid M. | 799319 | 5918809 | 11/11/2014 16:18 | renzo.suito@gmail.com | Zaid M. | Cerrado | 12/11/2014 12:45 | 13/11/2014 10:35 | 21 h 50 min |
| | Zaid M. | 799320 | 5921462 | 11/11/2014 20:40 | danielorellana66@hotmail.com | Zaid M. | Cerrado | 12/11/2014 12:55 | 13/11/2014 10:47 | 21 h 52 min |
| | Zaid M. | 799321 | 5926085 | 11/11/2014 21:47 | jfranco@josfel.com.pe | Zaid M. | Cerrado | 12/11/2014 1:20 | 13/11/2014 12:04 | 01 d 10 h 44 min |
| | Zaid M. | 799322 | 5927214 | 11/11/2014 23:34 | edominguezc@bcp.com.pe | Zaid M. | Cerrado | 12/11/2014 1:36 | 13/11/2014 10:27 | 01 d 08 h 51 min |
| 12 | Zaid M. | 799324 | 5932096 | 12/11/2014 15:29 | mmarino@slb.com | Zaid M. | Cerrado | 13/11/2014 1:35 | 13/11/2014 10:41 | 09 h 06 min |
| | Zaid M. | 801495 | 5934957 | 12/11/2014 20:29 | jfranco@josfel.com.pe | Zaid M. | Cerrado | 13/11/2014 1:51 | 14/11/2014 10:17 | 01 d 08 h 26 min |
| | Zaid M. | 801496 | 5934984 | 12/11/2014 19:31 | alfonsopatron@gmail.com | Zaid M. | Cerrado | 13/11/2014 2:01 | 13/11/2014 10:38 | 08 h 37 min |
| | Zaid M. | 801500 | 5935051 | 12/11/2014 18:25 | jari.coloma@gmail.com | Zaid M. | Cerrado | 13/11/2014 2:12 | 13/11/2014 10:21 | 08 h 09 min |
| | Zaid M. | 801501 | 5935612 | 12/11/2014 18:34 | as_leg_chimbote2@scotiabank.com.pe | Victor | Cerrado | 13/11/2014 2:24 | 18/11/2014 1:30 | 04 d 23 h 06 min |
| | Zaid M. | 801502 | 5943727 | 13/11/2014 0:09 | romar_110@hotmail.com | Zaid M. | Cerrado | 14/11/2014 12:33 | 14/11/2014 10:20 | 21 h 47 min |
| | Humberto O. | 816436 | 5938798 | 13/11/2014 22:37 | cvilela@intercorp.com.pe | Humberto O. | Cerrado | 26/11/2014 6:30 | 28/11/2014 12:58 | 02 d 06 h 28 min |
| 13 | Zaid M. | 801505 | 5946328 | 13/11/2014 16:20 | carmen.burneo@gmail.com | Victor | Cerrado | 14/11/2014 1:08 | 17/11/2014 4:30 | 03 d 03 h 22 min |
| | Zaid M. | 802903 | 5947712 | 13/11/2014 15:14 | alan.cuadra@telefonica.com | Victor | Cerrado | 14/11/2014 1:27 | 18/11/2014 1:34 | 04 d 00 h 07 min |
| | Zaid M. | 802904 | 5947839 | 13/11/2014 16:13 | betty.perez@upn.edu.pe | Victor | Cerrado | 14/11/2014 1:35 | 18/11/2014 1:40 | 04 d 00 h 05 min |
| | Zaid M. | 802906 | 5947957 | 13/11/2014 15:28 | alfredo.paredes@paredesgroup.com.pe | Victor | Cerrado | 14/11/2014 1:45 | 18/11/2014 1:44 | 03 d 23 h 59 min |
| 14 | Zaid M. | 802907 | 5968432 | 14/11/2014 18:01 | amvega@odebrecht.com | Victor | Cerrado | 15/11/2014 1:09 | 18/11/2014 1:47 | 03 d 00 h 38 min |
| 15 | Victor | 802908 | 5983623 | 15/11/2014 17:04 | cristian_ad@hotmail.com | Victor | Cerrado | 16/11/2014 3:00 | 22/11/2014 1:52 | 05 d 22 h 52 min |
| | Victor | 805356 | 5986013 | 15/11/2014 19:27 | kurycor@hotmail.com | Victor | Cerrado | 16/11/2014 3:05 | 20/11/2014 12:47 | 04 d 09 h 42 min |
| 16 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ |

Tabla 17. Parte 1, Tiempo de exposición de los incidentes sin el uso del sistema.
Fuente: Elaboración propia.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 | Victor | 807585 | 5993134 | 17/11/2014 14:31 | elizabeth5_13@yahoo.es | Victor | Cerrado | 18/11/2014 2:23 | 21/11/2014 2:54 | 03 d 00 h 31 min |
| | Victor | 807586 | 6002764 | 17/11/2014 18:38 | cardiles@florisert.com | Victor | Cerrado | 18/11/2014 2:32 | 18/11/2014 11:57 | 09 h 25 min |
| | Victor | 807587 | 6008834 | 17/11/2014 21:44 | rondascam@hotmail.com | Victor | Cerrado | 18/11/2014 2:40 | 20/11/2014 1:04 | 01 d 22 h 24 min |
| 18 | Victor | 808670 | 6019378 | 18/11/2014 15:13 | katya.valencia@natuperu.com | Victor | Cerrado | 19/11/2014 2:24 | 20/11/2014 1:14 | 22 h 50 min |
| | Victor | 808672 | 6022069 | 18/11/2014 16:06 | wrg20@hotmail.com | Victor | Cerrado | 19/11/2014 2:33 | 21/11/2014 3:07 | 02 d 00 h 34 min |
| | Victor | 808673 | 6022276 | 18/11/2014 16:12 | wrg20@hotmail.com | Victor | Cerrado | 19/11/2014 2:53 | 21/11/2014 8:07 | 02 d 05 h 14 min |
| | Victor | 808674 | 6030162 | 18/11/2014 22:22 | rosa.hoyos@rjabogados.com | Victor | Cerrado | 19/11/2014 2:36 | 20/11/2014 1:19 | 22 h 43 min |
| | Victor | 808675 | 6030724 | 18/11/2014 20:19 | rosa.hoyos@rjabogados.com | Victor | Cerrado | 19/11/2014 2:48 | 20/11/2014 1:21 | 22 h 33 min |
| | Victor | 808676 | 6032505 | 18/11/2014 23:02 | zegarral@gmail.com | Victor | Cerrado | 19/11/2014 2:44 | 22/11/2014 1:52 | 02 d 23 h 08 min |
| 19 | Victor | 809462 | 6037792 | 19/11/2014 15:26 | alvaromaurial@gmail.com | Victor | Cerrado | 20/11/2014 3:42 | 21/11/2014 3:15 | 23 h 33 min |
| | Victor | 809463 | 6038660 | 19/11/2014 15:19 | compras3@rokys.pe | Victor | Cerrado | 20/11/2014 4:57 | 22/11/2014 1:54 | 01 d 20 h 57 min |
| | Victor | 809464 | 6041436 | 19/11/2014 19:41 | jorgeparedes1201@yahoo.com.pe | Victor | Cerrado | 20/11/2014 5:09 | 21/11/2014 3:25 | 22 h 16 min |
| | Victor | 809465 | 6044883 | 19/11/2014 20:44 | manu.ortiz.amp@gmail.com | Victor | Cerrado | 20/11/2014 5:24 | 21/11/2014 3:37 | 22 h 13 min |
| | Victor | 809466 | 6046325 | 19/11/2014 22:51 | rosa.hoyos@rjabogados.com | Victor | Cerrado | 20/11/2014 5:58 | 21/11/2014 3:40 | 21 h 42 min |
| | Victor | 809467 | 6050287 | 20/11/2014 0:16 | flescanodlp@hotmail.com | Victor | Cerrado | 20/11/2014 6:10 | 21/11/2014 3:43 | 21 h 33 min |
| 20 | Victor | 810314 | 6054919 | 20/11/2014 17:47 | ferrol.contabilidad@gmail.com | Humberto O. | Cerrado | 21/11/2014 4:58 | 21/11/2014 4:10 | 23 h 12 min |
| | Victor | 810315 | 6058773 | 20/11/2014 20:17 | vicente.valdivia@bbva.com | Humberto O. | Cerrado | 21/11/2014 4:46 | 28/11/2014 12:10 | 07 d 07 h 24 min |
| 21 | Victor | 815496 | 6069157 | 21/11/2014 14:42 | dpedreros@bfu.pe | Humberto O. | Cerrado | 22/11/2014 6:23 | 03/12/2014 12:00 | 11 d 05 h 37 min |
| | Victor | 812082 | 6069502 | 21/11/2014 15:06 | carlos.llerena@saviaperu.com | Victor | Cerrado | 22/11/2014 3:46 | 23/11/2014 1:39 | 21 h 53 min |
| | Victor | 812099 | 6077368 | 21/11/2014 18:29 | claudiamutze@hotmail.com | Zaid M. | Cerrado | 22/11/2014 4:02 | 28/11/2014 10:35 | 06 d 06 h 33 min |
| | Victor | 812104 | 6080717 | 21/11/2014 21:57 | ancafesa@hotmail.com | Humberto O. | Cerrado | 22/11/2014 4:16 | 25/11/2014 4:30 | 03 d 00 h 14 min |
| 22 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ |
| 23 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ |
| 24 | Humberto O. | 815475 | 6100827 | 24/11/2014 13:45 | felr_75@hotmail.com | Humberto O. | Cerrado | 25/11/2014 5:23 | 26/11/2014 4:33 | 23 h 10 min |
| | Humberto O. | 815481 | 6105289 | 24/11/2014 16:14 | rosa.hoyos@rjabogados.com | Humberto O. | Cerrado | 25/11/2014 5:29 | 26/11/2014 4:19 | 22 h 50 min |
| | Humberto O. | 815483 | 6110146 | 24/11/2014 20:49 | elizabethcastanedapena@gmail.com | Humberto O. | Cerrado | 25/11/2014 3:50 | 02/12/2014 11:50 | 07 d 08 h 00 min |
| | Humberto O. | 815485 | 6110589 | 24/11/2014 18:17 | romyco100@hotmail.com | Humberto O. | Cerrado | 25/11/2014 5:43 | 26/11/2014 4:27 | 22 h 44 min |
| | Humberto O. | 815489 | 6112701 | 24/11/2014 21:50 | adamy@hotmail.com | Zaid M. | Cerrado | 25/11/2014 5:34 | 28/11/2014 10:23 | 03 d 04 h 49 min |
| 25 | Humberto O. | 816347 | 6120516 | 25/11/2014 15:21 | terrones741@hotmail.com | Humberto O. | Cerrado | 26/11/2014 10:21 | 28/11/2014 12:38 | 02 d 02 h 17 min |
| | Humberto O. | 816367 | 6121961 | 25/11/2014 15:23 | reyna.cordova@crediscotia.com.pe | Humberto O. | Cerrado | 26/11/2014 3:22 | 09/01/2015 2:28 | 12 d 23 h 06 min |
| | Humberto O. | 816374 | 6124751 | 25/11/2014 19:51 | psalazar@mifarma.com.pe | Zaid M. | Cerrado | 26/11/2014 3:29 | 28/11/2014 10:30 | 02 d 07 h 01 min |
| | Humberto O. | 816378 | 6127556 | 25/11/2014 22:00 | tesoreria@santiagoqueirolo.com | Zaid M. | Cerrado | 26/11/2014 3:37 | 28/11/2014 10:26 | 02 d 06 h 49 min |
| | Humberto O. | 816385 | 6127741 | 25/11/2014 21:27 | kritobh@gmail.com | Humberto O. | Cerrado | 26/11/2014 4:28 | 28/11/2014 12:48 | 02 d 08 h 20 min |
| 26 | Humberto O. | 817239 | 6135036 | 26/11/2014 15:49 | joel.gonzales.m@gmail.com | Humberto O. | Cerrado | 27/11/2014 10:11 | 09/01/2015 1:31 | 11 d 15 h 20 min |
| | Humberto O. | 817242 | 6139250 | 26/11/2014 19:55 | cesarlosan@hotmail.com | Humberto O. | Cerrado | 27/11/2014 2:58 | 28/11/2014 1:15 | 22 h 17 min |
| | Humberto O. | 817246 | 6142590 | 26/11/2014 23:18 | alexa2galy@gmail.com | Humberto O. | Cerrado | 27/11/2014 3:05 | 28/11/2014 4:16 | 01 d 01 h 11 min |
| | Humberto O. | 817249 | 6144006 | 26/11/2014 23:39 | mchang@banbif.com.pe | Zaid M. | Cerrado | 27/11/2014 3:23 | 28/11/2014 10:18 | 01 d 06 h 55 min |
| 27 | Humberto O. | 818300 | 6151857 | 27/11/2014 17:19 | christianvasquezricce@gmail.com | Humberto O. | Cerrado | 28/11/2014 3:01 | 02/12/2014 11:45 | 04 d 08 h 44 min |
| | Humberto O. | 818309 | 6155340 | 27/11/2014 20:52 | segundosabu80@hotmail.com | Humberto O. | Cerrado | 28/11/2014 3:09 | 02/12/2014 11:39 | 04 d 08 h 30 min |
| | Humberto O. | 818322 | 6162168 | 27/11/2014 22:42 | prubin@rree.gob.pe | Zaid M. | Cerrado | 28/11/2014 3:23 | 28/11/2014 10:42 | 07 h 19 min |
| 28 | Zaid M. | 820002 | 6175091 | 28/11/2014 20:21 | camj1112@hotmail.com | Humberto O. | Cerrado | 29/11/2014 2:07 | 02/12/2014 11:34 | 03 d 09 h 27 min |
| | Zaid M. | 819995 | 6179284 | 28/11/2014 21:30 | segundosabu80@hotmail.com | Humberto O. | Cerrado | 29/11/2014 3:53 | 01/12/2014 11:42 | 02 d 07 h 49 min |
| | Zaid M. | 819994 | 6180312 | 28/11/2014 21:12 | consul@peru.ae | Humberto O. | Cerrado | 29/11/2014 6:45 | 01/12/2014 11:47 | 02 d 05 h 02 min |
| 29 | Humberto O. | 821828 | 6185658 | 29/11/2014 14:14 | hannita1206@hotmail.com | Zaid M. | Cerrado | 01/12/2014 1:29 | 02/12/2014 11:39 | 01 d 10 h 10 min |
| | Humberto O. | 821833 | 6185667 | 29/11/2014 14:24 | hannita1206@gmail.com | Zaid M. | Cerrado | 01/12/2014 1:44 | 02/12/2014 8:47 | 01 d 07 h 03 min |
| | Humberto O. | 821834 | 6190179 | 29/11/2014 15:05 | lnmena8@gmail.com | Zaid M. | Cerrado | 01/12/2014 1:58 | 05/12/2014 3:47 | 04 d 01 h 49 min |
| | Humberto O. | 821839 | 6190181 | 29/11/2014 17:12 | charo514@hotmail.com | Zaid M. | Cerrado | 01/12/2014 2:14 | 08/12/2014 9:47 | 07 d 07 h 33 min |
| | Humberto O. | 821840 | 6192430 | 29/11/2014 18:28 | miriamgrabiel@hotmail.com | Humberto O. | Cerrado | 01/12/2014 2:25 | 09/01/2015 2:37 | 08 d 00 h 12 min |
| 30 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ |
| **Tiempo promedio de exposición de los casos de incidentes de información** | | | | | | | | | | 03 d 16 h 14 min |

Tabla 18. Parte 2, Tiempo de exposición de los incidentes sin el uso del sistema.
Fuente: Elaboración propia.

Tiempo promedio de exposición de los incidentes notificados con el uso del sistema de gestión (junio del 2015).

| Notificaciones de incidentes del mes de Junio del 2015 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Día | Operador - Inic | Ticket Digiware | ID | Hora de envío | DESTINO | Operador - Fin | Condición | Hora de Apertura | Hora de Cierre | Tiempo de Exposición |
| 1 | Jose T. | 993339 | 7779929 | 31/10/2014 23:23 | dimas_dr@hotmail.com | Zaid M. | Cerrado | 02/06/2015 4:11 | 06/06/2015 10:39 | 04 d 06 h 28 min |
| 2 | Jose T. | 986825 | 7799387 | 02/06/2015 17:59 | ritapita1@ymail.com | Zaid M. | Cerrado | 03/06/2015 1:23 | 07/06/2015 10:11 | 04 d 08 h 48 min |
| | Jose T. | 980006 | 7802279 | 02/06/2015 13:51 | lihiskasvi@yahoo.com | Jose T. | Cerrado | 03/06/2015 1:55 | 07/06/2015 11:23 | 04 d 09 h 28 min |
| 3 | Jose T. | 983388 | 7817430 | 03/06/2015 14:19 | saif_niloy@hotmail.com | Jose T. | Cerrado | 04/06/2015 1:18 | 10/06/2015 10:23 | 06 d 09 h 05 min |
| | Jose T. | 983389 | 7822317 | 03/06/2015 17:55 | terrence23@comcast.net | Zaid M. | Cerrado | 04/06/2015 5:19 | 07/06/2015 10:17 | 03 d 04 h 58 min |
| | Jose T. | 983395 | 7828791 | 03/06/2015 20:33 | arshad_1601@hotmail.com | Jose T. | Cerrado | 04/06/2015 6:35 | 07/06/2015 7:45 | 03 d 01 h 10 min |
| | Jose T. | 983390 | 7827370 | 03/06/2015 21:42 | sarahfoley.ox@googlemail.com | Zaid M. | Cerrado | 04/06/2015 5:49 | 13/06/2015 12:14 | 09 d 06 h 25 min |
| | Jose T. | 983392 | 7827371 | 03/06/2015 9:19 | joziesbois@yahoo.com | Zaid M. | Cerrado | 04/06/2015 5:58 | 13/06/2015 10:26 | 09 d 04 h 28 min |
| 5 | Zaid M. | 989223 | 7838707 | 05/06/2015 16:04 | craigtmutoko@gmail.com | Zaid M. | Cerrado | 06/06/2015 1:28 | 06/06/2015 10:02 | 08 h 34 min |
| | Zaid M. | 989229 | 7848178 | 05/06/2015 0:18 | brutues_bekoe@yahoo.com | Zaid M. | Cerrado | 06/06/2015 1:45 | 06/06/2015 9:57 | 08 h 12 min |
| | Zaid M. | 989636 | 7849744 | 05/06/2015 16:54 | kevinbalbuena428@gmail.com | Zaid M. | Cerrado | 06/06/2015 1:58 | 07/06/2015 10:53 | 01 d 08 h 55 min |
| | Zaid M. | 989639 | 7870881 | 05/06/2015 11:35 | kevinwilford@hotmail.com | Zaid M. | Cerrado | 06/06/2015 2:13 | 07/06/2015 10:24 | 01 d 08 h 11 min |
| | Zaid M. | 989635 | 7872088 | 05/06/2015 14:31 | qwanis@yahoo.com | Zaid M. | Cerrado | 06/06/2015 2:25 | 07/06/2015 10:26 | 01 d 08 h 01 min |
| | Zaid M. | 989630 | 7879327 | 05/06/2015 12:44 | bilaldahir@hotmail.com | Zaid M. | Cerrado | 06/06/2015 2:40 | 07/06/2015 10:30 | 01 d 07 h 50 min |
| | Zaid M. | 989632 | 7879378 | 05/06/2015 20:23 | sasukeuchiha1293@yahoo.com | Zaid M. | Cerrado | 06/06/2015 3:15 | 07/06/2015 10:02 | 01 d 06 h 47 min |
| | Zaid M. | 989655 | 7879888 | 05/06/2015 20:13 | raw@abv.bg | Zaid M. | Cerrado | 06/06/2015 3:31 | 07/06/2015 10:08 | 01 d 06 h 37 min |
| | Zaid M. | 989650 | 7880181 | 05/06/2015 21:45 | jyeap@yahoo.com.sg | Zaid M. | Cerrado | 06/06/2015 3:49 | 07/06/2015 10:05 | 01 d 06 h 16 min |
| | Zaid M. | 989651 | 7880773 | 05/06/2015 22:42 | peele.steve@gmail.com | Zaid M. | Cerrado | 06/06/2015 4:18 | 13/06/2015 12:21 | 07 d 08 h 03 min |
| 6 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 7 | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 8 | Zaid M. | 989652 | 7888788 | 08/06/2014 11:28 | krrouse71@gmail.com | Zaid M. | Cerrado | 07/06/2015 1:22 | 11/06/2015 11:59 | 04 d 10 h 37 min |
| | Zaid M. | 989653 | 7883877 | 08/06/2015 22:12 | andelka.toto-ormuz@post.t-com.hr | Zaid M. | Cerrado | 07/06/2015 1:37 | 10/06/2015 10:48 | 03 d 09 h 11 min |
| | Zaid M. | 992593 | 7888078 | 08/06/2015 12:35 | bybio12@yahoo.com | Zaid M. | Cerrado | 07/06/2015 1:52 | 12/06/2015 11:49 | 05 d 09 h 57 min |
| | Zaid M. | 993939 | 7893009 | 08/06/2015 13:50 | waveynick@yahoo.com | Zaid M. | Cerrado | 07/06/2015 2:22 | 12/06/2015 11:46 | 05 d 09 h 24 min |
| 9 | Zaid M. | 998532 | 7899907 | 09/06/2015 14:35 | dimmelus@yahoo.com | Zaid M. | Cerrado | 10/06/2015 12:33 | 11/06/2015 11:56 | 23 h 23 min |
| 10 | Zaid M. | 998533 | 7901781 | 10/06/2015 16:13 | alvinjade_007@yahoo.com.ph | Zaid M. | Cerrado | 11/06/2015 1:41 | 12/06/2015 11:59 | 01 d 10 h 18 min |
| | Zaid M. | 999308 | 7903882 | 10/06/2015 15:32 | jasnalabovic@yahoo.com | Zaid M. | Cerrado | 11/06/2015 2:02 | 11/06/2015 11:52 | 09 h 50 min |
| | Zaid M. | 999309 | 7903988 | 10/06/2015 11:42 | djmzi_2010@hotmail.com | Zaid M. | Cerrado | 11/06/2015 2:19 | 12/06/2015 12:03 | 01 d 09 h 44 min |
| 11 | Zaid M. | 999325 | 7918021 | 11/06/2015 11:56 | victoria20nice@yahoo.com | Zaid M. | Cerrado | 12/06/2015 12:35 | 13/06/2015 10:30 | 21 h 55 min |
| | Zaid M. | 999320 | 7918809 | 11/06/2015 19:14 | tonyiverson09@yahoo.com | Zaid M. | Cerrado | 12/06/2015 12:50 | 13/06/2015 10:35 | 21 h 45 min |
| | Zaid M. | 999322 | 7921482 | 11/06/2015 21:41 | micskillz@rocketmail.com | Zaid M. | Cerrado | 12/06/2015 1:35 | 13/06/2015 10:47 | 01 d 09 h 12 min |
| | Zaid M. | 999323 | 7928087 | 11/06/2014 22:47 | nusaibap@yahoo.com | Zaid M. | Cerrado | 12/06/2015 1:42 | 13/06/2015 12:04 | 01 d 10 h 22 min |
| | Zaid M. | 850395 | 7927214 | 11/06/2015 21:33 | internet.brilliant@gmail.com | Zaid M. | Cerrado | 12/06/2015 2:10 | 13/06/2015 10:27 | 01 d 08 h 17 min |
| 12 | Zaid M. | 850396 | 7932098 | 12/06/2015 11:29 | petterwarcraft@hotmail.com | Zaid M. | Cerrado | 13/06/2015 1:35 | 13/06/2015 10:41 | 09 h 06 min |
| | Zaid M. | 850555 | 7934977 | 12/06/2015 21:30 | robanddave@hotmail.co.uk | Zaid M. | Cerrado | 13/06/2015 1:41 | 14/06/2015 10:17 | 01 d 08 h 36 min |
| | Zaid M. | 850550 | 7934984 | 12/06/2015 17:23 | bornalive101@aol.com | Zaid M. | Cerrado | 13/06/2015 1:55 | 13/06/2015 10:38 | 08 h 43 min |
| | Zaid M. | 850552 | 7937071 | 12/06/2015 15:25 | christian122497@yahoo.com | Zaid M. | Cerrado | 13/06/2015 2:10 | 13/06/2015 10:21 | 08 h 11 min |
| | Zaid M. | 806336 | 7937812 | 12/06/2015 17:35 | crouch@memyself.in | Victor | Cerrado | 13/06/2015 2:25 | 18/06/2015 1:30 | 04 d 23 h 05 min |
| | Zaid M. | 852953 | 7943727 | 12/06/2015 12:14 | thabithabby@aol.com | Zaid M. | Cerrado | 13/06/2015 2:43 | 14/06/2015 10:20 | 01 d 07 h 37 min |
| | Zaid M. | 852956 | 7938798 | 12/06/2015 21:37 | josephtraced@yahoo.com | Humberto O. | Cerrado | 13/06/2015 2:58 | 28/06/2015 12:58 | 15 d 10 h 00 min |
| 13 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 14 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 15 | Zaid M. | 852959 | 7948328 | 15/06/2015 17:21 | sdonavaun@yahoo.com | Victor | Cerrado | 16/06/2015 1:08 | 17/06/2015 4:30 | 01 d 03 h 22 min |
| | Zaid M. | 852958 | 7947712 | 15/06/2015 14:18 | soniamorales@windowslive.com | Victor | Cerrado | 16/06/2015 1:23 | 18/06/2015 1:34 | 02 d 00 h 11 min |
| | Zaid M. | 855356 | 7947839 | 15/06/2015 18:13 | kimfin3000@aol.com | Victor | Cerrado | 16/06/2015 1:36 | 18/06/2015 1:40 | 02 d 00 h 04 min |
| | Zaid M. | 859585 | 7947977 | 15/06/2015 11:28 | katte_lov3@hotmail.com | Victor | Cerrado | 16/06/2015 1:57 | 18/06/2015 1:44 | 01 d 23 h 47 min |

Tabla 19. Parte 1, Tiempo de exposición de los incidentes con el uso del sistema.
Fuente: Elaboración propia.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 16 | Victor | 859586 | 7988432 | 16/06/2015 15:06 | egzooni@msn.com | Victor | Cerrado | 17/06/2015 1:09 | 18/06/2015 1:47 | 01 d 00 h 38 min |
| | Victor | 859589 | 7983823 | 16/06/2015 19:13 | mandira.db@gmail.com | Victor | Cerrado | 17/06/2015 1:24 | 22/06/2015 1:52 | 05 d 00 h 28 min |
| | Victor | 858695 | 7988013 | 16/06/2015 18:32 | rushemjo@hotmail.com | Victor | Cerrado | 17/06/2015 1:44 | 20/06/2015 12:47 | 03 d 11 h 03 min |
| 17 | Victor | 858692 | 7993134 | 17/06/2015 15:31 | jamesbreezy123@gmail.com | Victor | Cerrado | 18/06/2015 2:23 | 21/06/2015 2:54 | 03 d 00 h 31 min |
| | Victor | 858693 | 8002784 | 17/06/2015 17:40 | nathanhoskins92@yahoo.com | Victor | Cerrado | 18/06/2015 2:39 | 18/06/2015 11:57 | 09 h 18 min |
| | Victor | 858696 | 8008834 | 17/06/2015 22:41 | sammijay96@aol.com | Victor | Cerrado | 18/06/2015 2:59 | 20/06/2015 1:04 | 01 d 22 h 05 min |
| 18 | Victor | 859362 | 8019378 | 18/06/2015 11:18 | Blake.condon@yahoo.com | Victor | Cerrado | 19/06/2015 2:24 | 20/06/2015 1:14 | 22 h 50 min |
| | Victor | 859363 | 8022089 | 18/06/2015 14:32 | afiq.hazazi@yahoo.com | Victor | Cerrado | 19/06/2015 2:39 | 21/06/2015 3:07 | 02 d 00 h 28 min |
| | Victor | 859366 | 8030182 | 18/06/2015 21:22 | rhotboyl88@hotmail.com | Victor | Cerrado | 19/06/2015 3:12 | 20/06/2015 1:19 | 22 h 07 min |
| | Victor | 859369 | 8030724 | 18/06/2015 21:21 | wjaime41@yahoo.com | Victor | Cerrado | 19/06/2015 3:25 | 20/06/2015 1:21 | 21 h 56 min |
| | Victor | 805303 | 8032707 | 18/06/2014 19:21 | alex_12_ere@hotmail.co.uk | Victor | Cerrado | 19/06/2015 3:42 | 22/06/2015 1:52 | 02 d 22 h 10 min |
| 19 | Victor | 805305 | 8037792 | 19/06/2015 16:26 | ericseaverns@gmail.com | Victor | Cerrado | 20/06/2015 1:12 | 21/06/2015 3:15 | 01 d 02 h 03 min |
| | Victor | 805396 | 8038880 | 19/06/2015 16:21 | buchobailor@yahoo.com | Victor | Cerrado | 20/06/2015 1:27 | 22/06/2015 1:54 | 02 d 00 h 27 min |
| | Victor | 802582 | 8041438 | 19/06/2015 20:41 | dariusburkett@yahoo.com | Victor | Cerrado | 20/06/2015 1:59 | 21/06/2015 3:25 | 01 d 01 h 26 min |
| | Victor | 802599 | 8044883 | 19/06/2015 21:04 | bozkurtplayer44@hotmail.de | Victor | Cerrado | 20/06/2015 2:15 | 21/06/2015 3:37 | 01 d 01 h 22 min |
| | Victor | 802053 | 8048327 | 19/06/2015 21:49 | mailmon2@yahoo.com | Victor | Cerrado | 20/06/2015 2:36 | 21/06/2015 3:40 | 01 d 01 h 04 min |
| | Victor | 805395 | 8070287 | 19/06/2015 21:29 | humblewildcats@ymail.com | Victor | Cerrado | 20/06/2015 2:49 | 21/06/2015 3:43 | 01 d 00 h 54 min |
| 20 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 21 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 22 | Victor | 805380 | 8074919 | 22/06/2015 18:47 | 22st.cb@gmail.com | Humberto O. | Cerrado | 23/06/2015 12:25 | 25/06/2015 4:10 | 01 d 15 h 45 min |
| | Victor | 805383 | 8078773 | 22/06/2015 19:17 | Ashleyerin93@msn.com | Humberto O. | Cerrado | 23/06/2015 12:40 | 28/06/2015 12:10 | 04 d 23 h 30 min |
| | Victor | 806339 | 8077388 | 22/06/2015 19:30 | ryan23228@yahoo.com | Zaid M. | Cerrado | 23/06/2015 1:31 | 28/06/2015 10:35 | 05 d 09 h 04 min |
| | Victor | 806369 | 8080717 | 22/06/2015 19:53 | kennethballard07@yahoo.com | Humberto O. | Cerrado | 23/06/2015 1:48 | 25/06/2015 4:30 | 02 d 02 h 42 min |
| 23 | Victor | 806393 | 8080717 | 23/06/2015 21:59 | chickenpies@live.com | Humberto O. | Cerrado | 24/06/2015 2:16 | 25/06/2015 4:30 | 01 d 02 h 14 min |
| | Victor | 806398 | 8080717 | 23/06/2015 19:57 | patrickgosselin@live.com | Humberto O. | Cerrado | 24/06/2015 2:36 | 25/06/2015 4:30 | 01 d 01 h 54 min |
| 24 | Humberto O. | 806385 | 8100827 | 24/06/2015 12:45 | fukinis@yahoo.co.uk | Humberto O. | Cerrado | 25/06/2015 1:23 | 26/06/2015 4:33 | 01 d 03 h 10 min |
| | Humberto O. | 809239 | 8107289 | 24/06/2015 15:11 | marsouellet83@hotmail.com | Humberto O. | Cerrado | 25/06/2015 1:38 | 26/06/2015 4:19 | 01 d 02 h 41 min |
| | Humberto O. | 809232 | 8110148 | 24/06/2015 21:48 | kicks-coco@hotmail.com | Humberto O. | Cerrado | 25/06/2015 1:53 | 26/06/2015 11:50 | 01 d 09 h 57 min |
| | Humberto O. | 809236 | 8110789 | 24/06/2015 11:21 | megaman_98@mail.ru | Humberto O. | Cerrado | 25/06/2015 2:13 | 26/06/2015 4:27 | 01 d 02 h 14 min |
| | Humberto O. | 808355 | 8112701 | 24/06/2015 19:22 | kamildakrekos@gmail.com | Zaid M. | Cerrado | 25/06/2015 2:38 | 28/06/2015 10:23 | 03 d 07 h 45 min |
| 25 | Humberto O. | 808359 | 8120718 | 25/06/2015 19:21 | deadzone@hotmail.it | Humberto O. | Cerrado | 26/06/2015 1:21 | 28/06/2015 12:38 | 02 d 11 h 17 min |
| | Humberto O. | 808322 | 8121981 | 25/06/2015 16:13 | craig-simmons@hotmail.co.uk | Humberto O. | Cerrado | 26/06/2015 1:35 | 28/06/2015 2:28 | 02 d 00 h 53 min |
| | Humberto O. | 825552 | 8124771 | 25/06/2015 20:52 | youngspitta912@yahoo.com | Zaid M. | Cerrado | 26/06/2015 1:46 | 28/06/2015 10:30 | 02 d 08 h 44 min |
| | Humberto O. | 809995 | 8127778 | 25/06/2015 20:23 | iiid0m1n4t0riii@live.it | Zaid M. | Cerrado | 26/06/2015 2:03 | 28/06/2015 10:26 | 02 d 08 h 23 min |
| | Humberto O. | 809993 | 8127741 | 25/06/2015 23:55 | marymamet@yahoo.com | Humberto O. | Cerrado | 26/06/2015 2:24 | 28/06/2015 12:48 | 02 d 10 h 24 min |
| 26 | Humberto O. | 820828 | 8137038 | 26/06/2015 14:50 | malcomTV2@hotmail.com | Humberto O. | Cerrado | 27/06/2015 1:11 | 28/06/2015 1:31 | 01 d 00 h 20 min |
| | Humberto O. | 820833 | 8139270 | 26/06/2015 23:55 | bryan_vergara01@yahoo.com | Humberto O. | Cerrado | 27/06/2015 1:29 | 28/06/2015 1:15 | 23 h 46 min |
| | Humberto O. | 820839 | 8142790 | 26/06/2015 21:21 | yoga_ady_samudra@yahoo.co.id | Humberto O. | Cerrado | 27/06/2015 1:46 | 28/06/2015 4:16 | 01 d 02 h 30 min |
| | Humberto O. | 820835 | 8144008 | 26/06/2015 21:46 | casperondalow@hotmail.co.uk | Zaid M. | Cerrado | 27/06/2015 1:09 | 28/06/2015 10:18 | 01 d 09 h 09 min |
| 27 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 28 | ------ | | ------ | ------ | ------ | ------ | ------ | ------ | ------ | |
| 29 | Zaid M. | 820835 | 8171877 | 29/06/2015 19:46 | sk8_mafia7@live.com | Humberto O. | Cerrado | 28/06/2015 1:01 | 02/07/2015 11:45 | 04 d 10 h 44 min |
| | Zaid M. | 820836 | 8177340 | 29/06/2015 16:52 | liammerritt@live.com | Humberto O. | Cerrado | 28/06/2015 1:18 | 02/07/2015 11:39 | 04 d 10 h 21 min |
| | Zaid M. | 820839 | 8182188 | 29/06/2015 14:46 | Levi.Lee.93@gmail.com | Zaid M. | Cerrado | 28/06/2015 1:33 | 28/06/2015 10:42 | 09 h 09 min |
| | Zaid M. | 820841 | 8177091 | 29/06/2014 21:49 | moose1985@hotmail.com | Humberto O. | Cerrado | 28/06/2015 1:48 | 28/06/2015 11:34 | 09 h 46 min |
| | Zaid M. | 820845 | 8179284 | 29/06/2015 20:32 | sufiyanmohd_96@yahoo.com | Humberto O. | Cerrado | 28/06/2015 2:05 | 01/07/2015 11:42 | 03 d 09 h 37 min |
| | Zaid M. | 820860 | 8180312 | 29/06/2015 22:51 | rchy777@hotmail.co.uk | Humberto O. | Cerrado | 28/06/2015 2:22 | 01/07/2015 11:47 | 03 d 09 h 25 min |
| 30 | Humberto O. | 820875 | 8187878 | 30/06/2015 17:15 | jayson_samonteza@yahoo.com | Zaid M. | Cerrado | 01/07/2015 1:29 | 02/07/2015 11:39 | 01 d 10 h 10 min |
| | Humberto O. | 820876 | 8187887 | 30/06/2015 19:25 | jennyluvvsmen@aol.com | Zaid M. | Cerrado | 01/07/2015 1:44 | 02/07/2015 8:47 | 01 d 07 h 03 min |
| | Humberto O. | 820877 | 8190179 | 30/06/2015 18:47 | alisonangel99@rediffmail.com | Zaid M. | Cerrado | 01/07/2015 2:03 | 06/07/2015 3:47 | 05 d 01 h 44 min |
| | Humberto O. | 820878 | 8190181 | 30/06/2015 19:36 | lordjoshmac93@hotmail.com | Zaid M. | Cerrado | 01/07/2015 2:29 | 08/07/2015 9:47 | 07 d 07 h 18 min |
| | Humberto O. | 820879 | 8192430 | 30/06/2015 11:52 | bybio12@yahoo.com | Humberto O. | Cerrado | 01/07/2015 2:43 | 08/07/2015 2:37 | 06 d 23 h 54 min |
| **Tiempo promedio de exposión de los casos de incidentes de información** | | | | | | | | | | 02 d 13 h 26 min |

Tabla 20. Parte 2, Tiempo de exposición de los incidentes con el uso del sistema.
Fuente: Elaboración propia.

Gráfica de comparación del tiempo promedio de exposición de los incidentes notificados a los jefes directo de los colaboradores.

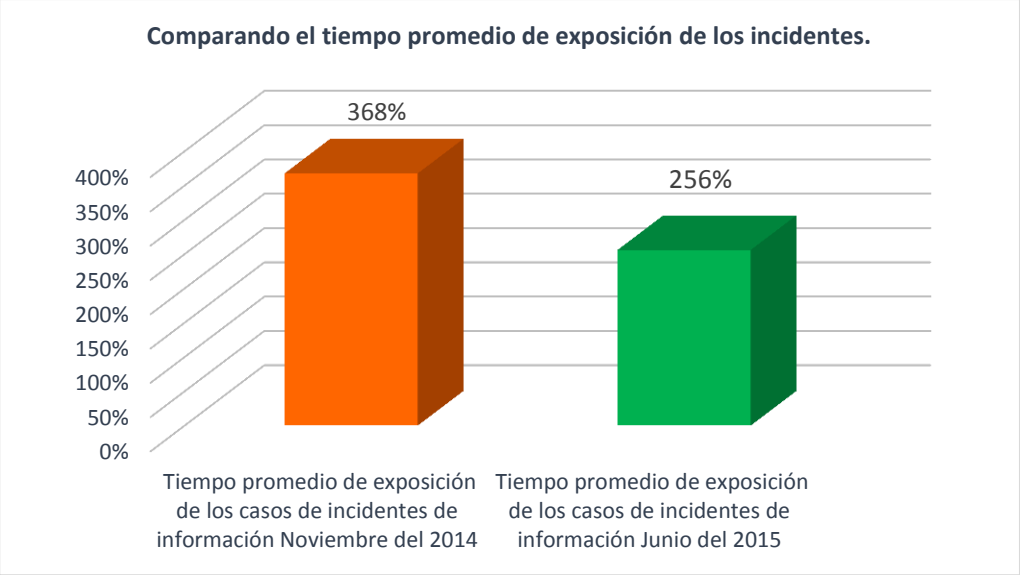



Figura 71. Gráfica de comparación del tiempo promedio de exposición de los incidentes.
Fuente: Elaboración propia.

De los cuadros mostrados, se observa, que el tiempo promedio de exposición de los casos de incidentes del mes de noviembre del 2014 es de 3 días 14 horas 16 min. Y en el mes de junio es de 2 días 13 horas 26 min. El cual, demuestra que con el uso del sistema de gestión de incidentes el tiempo promedio de exposición de los casos se reduce de un 368% a un 256%.

**c) Comparando el tiempo promedio de ejecución de procedimiento por cada evento notificado.**

Tiempo máximo para notificar un incidente de información= 20 minutos.

Tiempo promedio que se demora un operador en notificar el incidentes sin el uso del sistema de gestión de incidente de información.

| OPERADOR | TIEMPO DE EJECUCION X CADA EVENTO |
|---|---|
| Operador 01 | 15 min. |
| Operador 02 | 15 min. |
| Operador 03 | 16 min. |
| Operador 04 | 14 min. |
| Operador 05 | 14 min. |
| Operador 06 | 15 min. |
| Operador 07 | 15 min. |
| Operador 08 | 13 min. |
| Operador 09 | 15 min. |
| Operador 10 | 14 min. |
| Operador 11 | 15 min. |
| Operador 12 | 15 min. |
| Operador 13 | 14 min. |
| Operador 14 | 13 min. |
| Operador 15 | 14 min. |
| Operador 16 | 15 min. |
| Operador 17 | 15 min. |
| Operador 18 | 17 min. |
| Operador 19 | 15 min. |
| Operador 20 | 14 min. |
| Tiempo promedio | 15 minutos. |

Tabla 21. Tiempo de ejecución del procedimiento sin el uso del sistema de gestión.
Fuente: Elaboración propia.

Tiempo promedio que se demora un operador en notificar el incidentes con el uso del sistema de gestión de incidente de información.

| OPERADOR | TIEMPO DE EJECUCION X CADA EVENTO |
|---|---|
| Operador 01 | 5 min. |
| Operador 02 | 5 min. |
| Operador 03 | 5 min. |
| Operador 04 | 5 min. |
| Operador 05 | 5 min. |
| Operador 06 | 5 min. |
| Operador 07 | 5 min. |
| Operador 08 | 5 min. |
| Operador 09 | 5 min. |
| Operador 10 | 5 min. |
| Operador 11 | 5 min. |
| Operador 12 | 5 min. |
| Operador 13 | 5 min. |
| Operador 14 | 5 min. |
| Operador 15 | 5 min. |
| Operador 16 | 5 min. |
| Operador 17 | 5 min. |
| Operador 18 | 5 min. |
| Operador 19 | 5 min. |
| Operador 20 | 5 min. |
| Tiempo promedio | 5 minutos. |

Tabla 22. Tiempo de ejecución del procedimiento con el uso del sistema de gestión. Fuente: Elaboración propia.

Gráfica de comparación del tiempo promedio de ejecución del procedimiento por cada evento notificado.

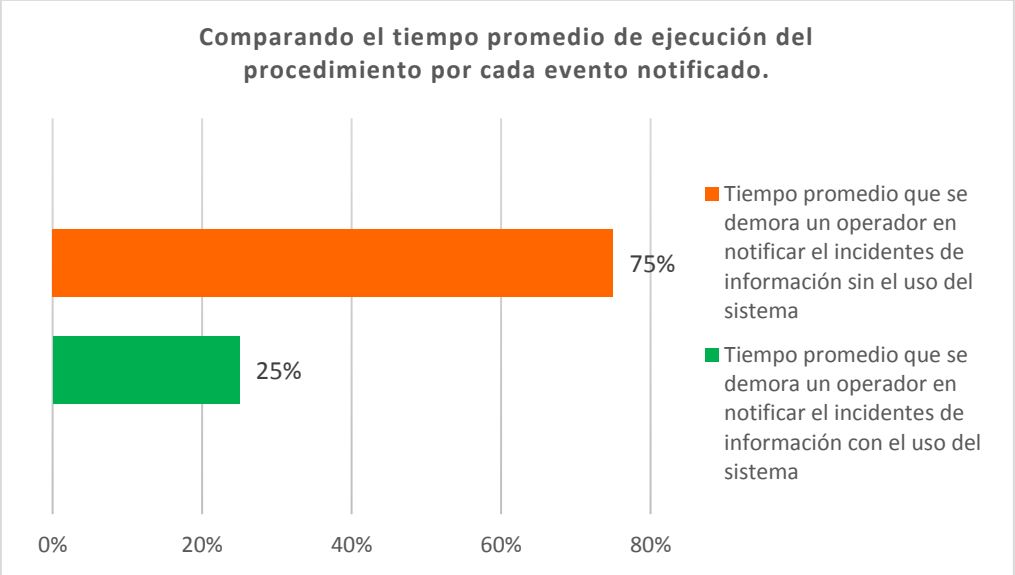


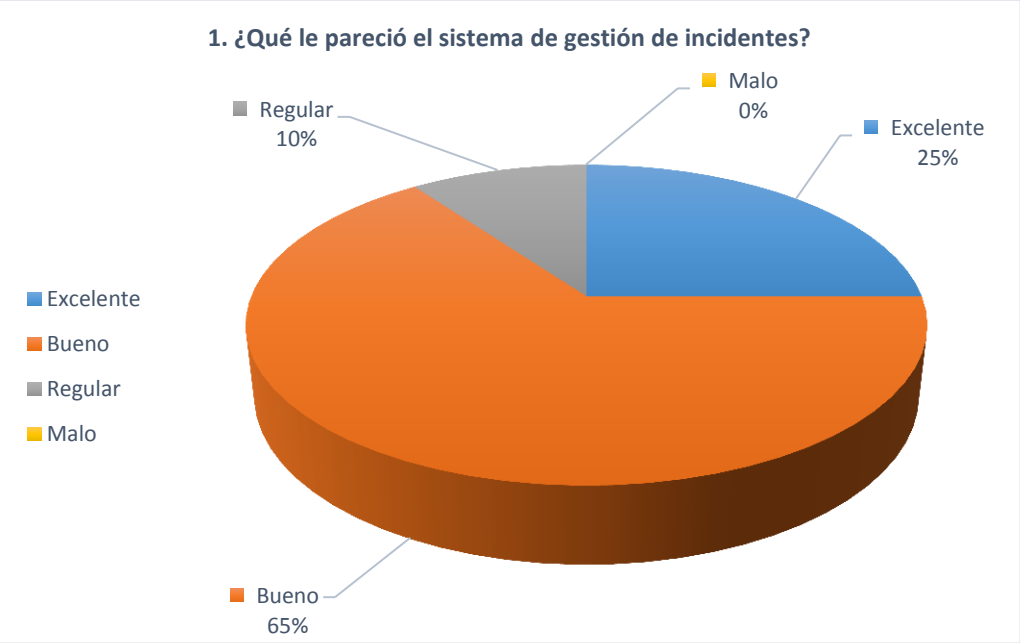

Figura 72. Gráfica de comparación del tiempo promedio de ejecución del procedimiento por cada evento.
Fuente: Elaboración propia.

De los cuadros mostrados, se observa, que el tiempo de ejecución del proceso de notificar un incidente de información es el 75% del tiempo máximo sin el uso del sistema de gestión y en la tabla 22 nos muestra una reducción de tiempo a 25%. El cual, demuestra que con el uso del sistema de gestión de incidente de información, el tiempo promedio de notificar un incidente de información se reduce en un 50% del tiempo máximo.

**d) Encuesta realizada a los usuarios beneficiados del sistema de gestión de incidentes.**

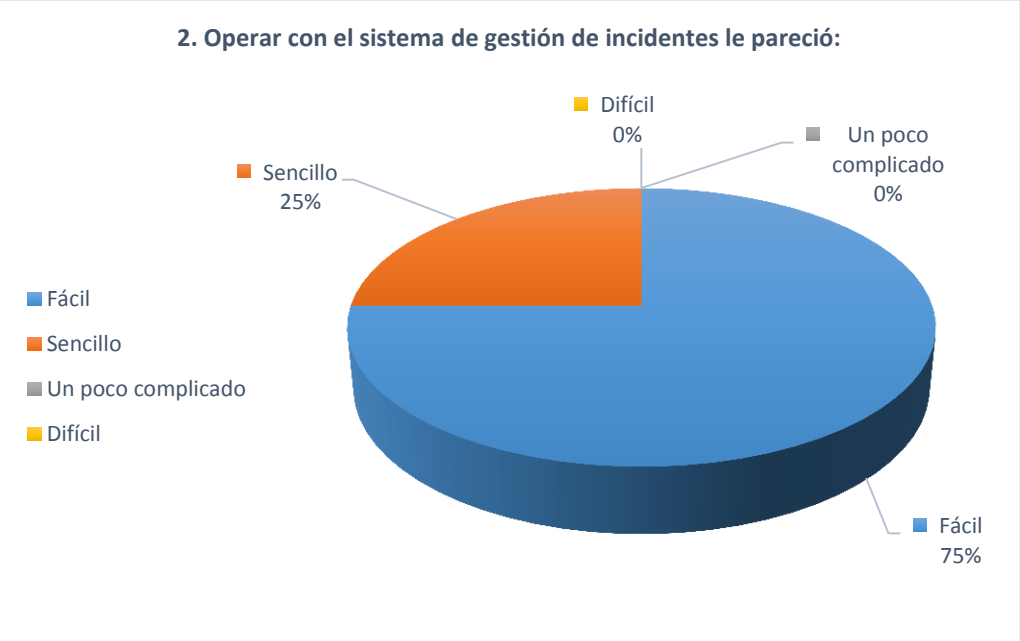
Para poder saber la satisfacción de los operadores SOC con el sistema de gestión de incidentes, se realizó una encuesta a 20 personas. El modelo de la encuesta se encuentra en el Anexo 19 con las 8 preguntas realizadas. Luego los datos de la encuesta fueron procesados dando los siguientes resultados.

**Resultado N°01:**



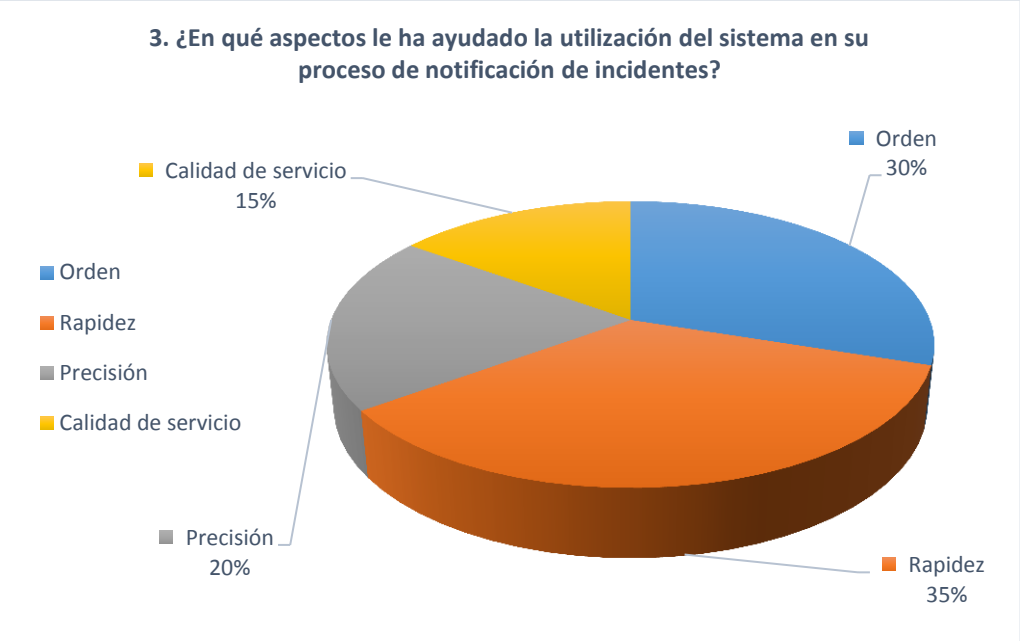

**Interpretación:** Según los datos al 25% le pareció Excelente y al 65% Bueno, es decir al 90% lo aprueba y el resto que es el 10% lo desaprueba. Este resultado es un favorable ya que nos indica que se va por buen camino, pero lo óptimo debería ser Excelente y solo es el 25% en conclusión se debe ir mejorando algunos aspectos del sistema, pero como inicio está más que aceptable.

**Resultado N°02:**



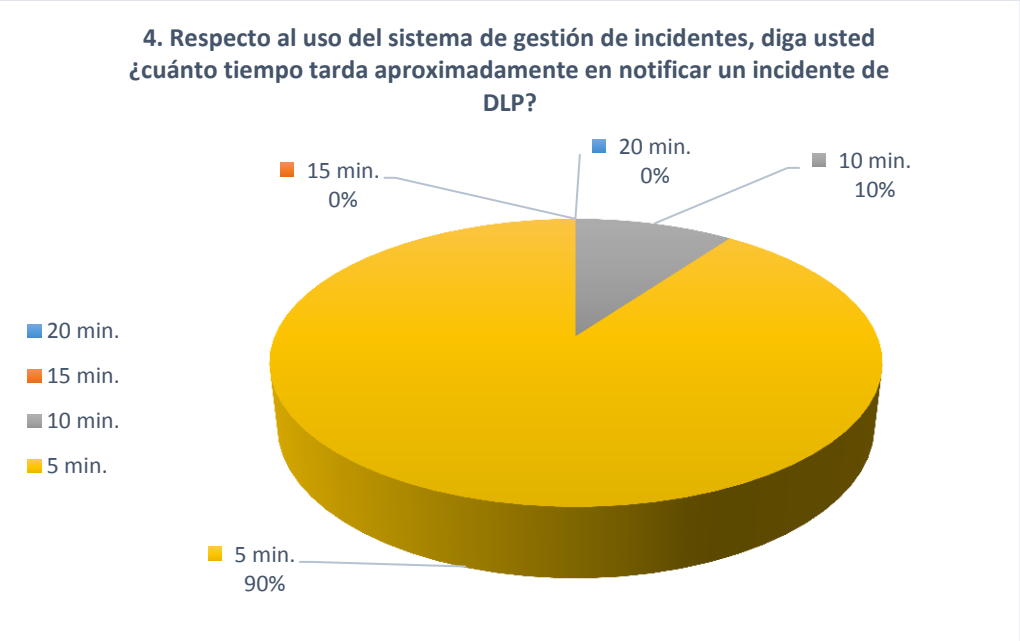

**Interpretación:** Según los datos al 75% le pareció Fácil y al 25% sencillo, es decir el 100% le pareció un sistema manejable y a ninguno le pareció complejo. Este resultado es un buen indicador ya que de esta manera se cumple con el objetivo de mejorar las operaciones de la empresa.

**Resultado N°03:**



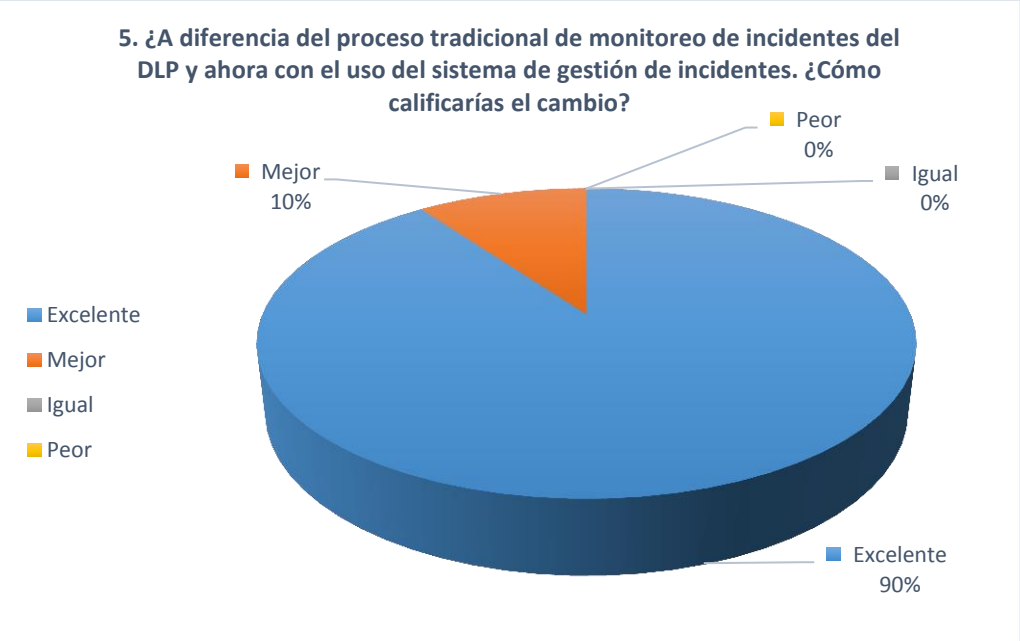

**Interpretación:** Según los datos el 30% le ayudó en el Orden, al 35% en la Rapidez, al 15% en la Calidad de Servicio y al 20% Precisión. El porcentaje de cada uno de los aspectos, nos indica que se cumple con el objetivo de mejora de las operaciones, por consiguiente, el beneficio obtenido para la empresa Digiware será una óptima imagen institucional por el servicio brindado.

**Resultado N°04:**



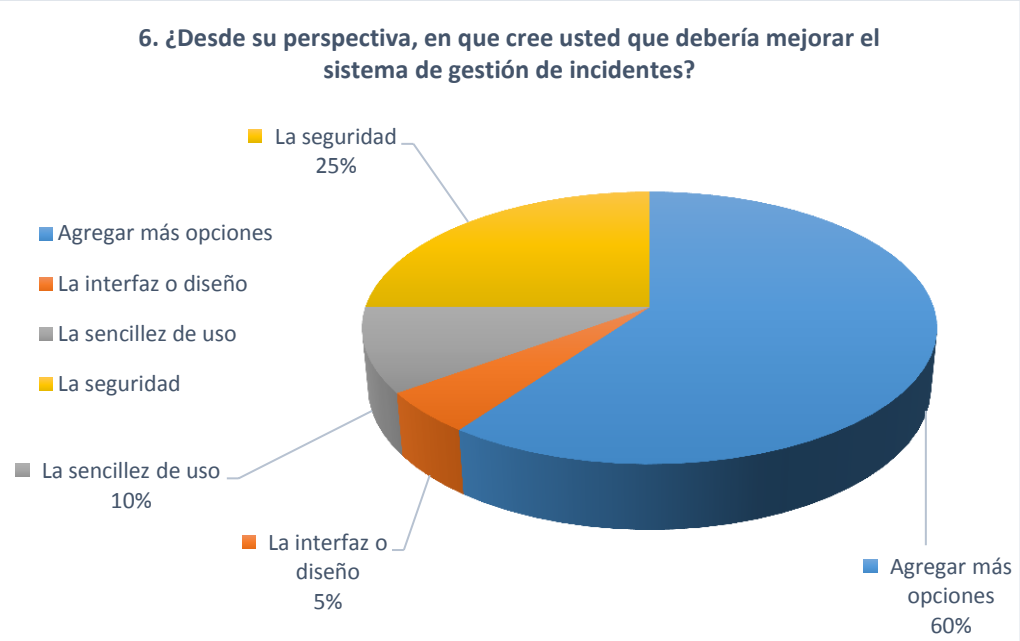

**Interpretación:** Según los datos el 90% tarda en notificar un incidente de información en 5 min y el 10% tarda 10 min, Estos indicadores son favorables ya que demuestran que el tiempo de ejecución del proceso de notificación de incidentes del DLP se ha reducido con respecto a la notificación sin el uso del sistema.

**Resultado N°05:**



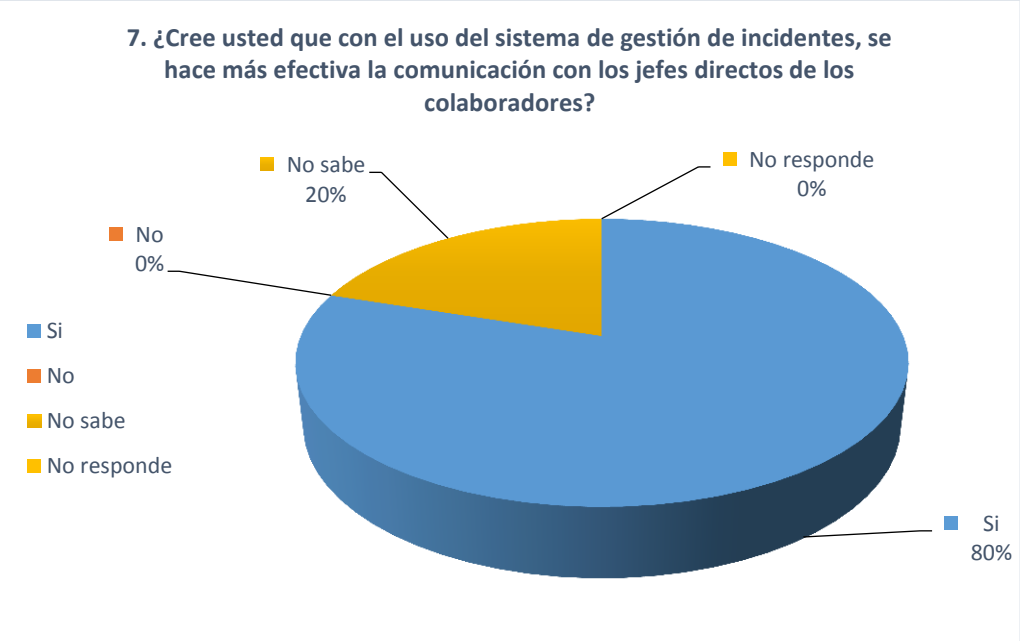

**Interpretación:** Según los datos para el 10% el proceso mejoró, al 90% fue Excelente es decir para el 100% se vio un cambio positivo, este resultado es un buen indicador de que el sistema está aportando al proceso de notificación de incidentes del DLP.

**Resultado N°06:**



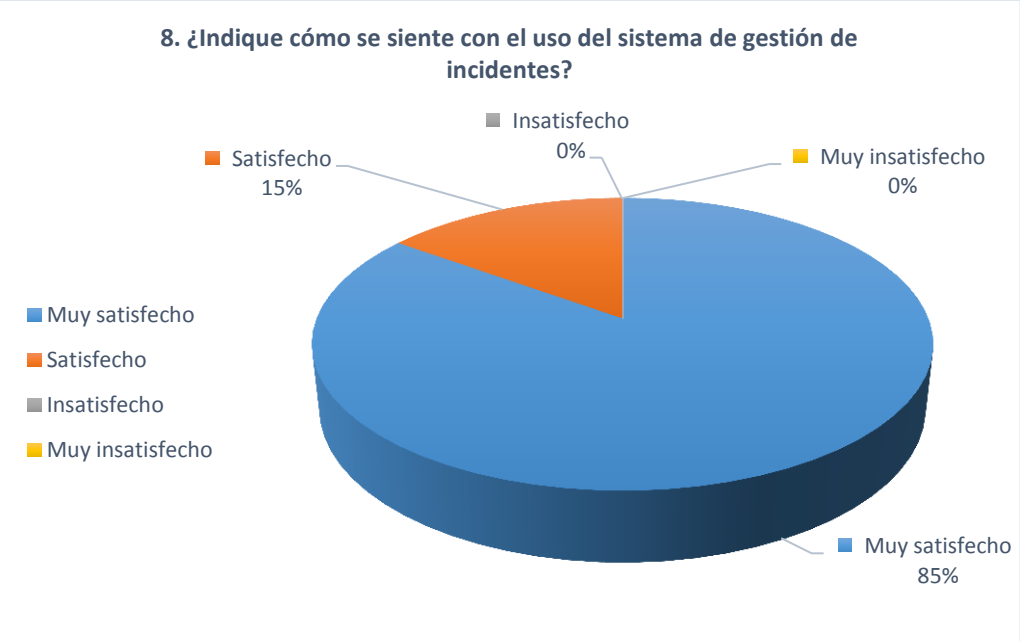

**Interpretación:** Según los datos el 60% desean que se agregue más funcionalidades al sistema relacionado a derivar los casos de fuga de información a otras área, solo un 5% la interfaz, el cual nos indica que el diseño fue bien elaborado, un 25% la seguridad, que siempre es bueno y 10% la sencillez de uso, que será parte de la mejora.

**Resultado N°07:**




**Interpretación:** Según los datos el 80% mencionó que SI, Este resultado es un buen indicador ya que de esta manera se cumple con el objetivo de mejorar las Comunicaciones de la empresa, mientras que el 20% No sabe, este indicador tiene que ver con los usuarios que no se adatan al sistema es por ello que no observan algún cambio.

**Resultado N°08:**




**Interpretación:** Finalmente la pregunta que nos resume todo, donde el 15% se siente satisfecho con el uso del sistema de gestión de incidentes mientras que el 15% se siente satisfecho, este resultado es un buen indicador que demuestra que los operadores están conforme con la automatización del proceso de monitoreo de incidencias del DLP, y que a su vez mejoró las comunicaciones y operaciones de la empresa Digiware.

# CONCLUSIONES

A lo largo del todo el proyecto, se realizó un seguimiento de cada uno de los objetivos específicos los cuales influyeron de forma directa en el objetivo general.

En consecuencia se determinaron las siguientes conclusiones:

1. Mediante el análisis previo del procedimiento de prevención de pérdida de datos (DLP) del banco Interbank, se logró adquirir la información necesaria que permitió establecer los requerimientos funcionales, el cual, fueron considerados en la construcción del sistema de gestión de incidentes.

2. Posteriormente a la obtención de los requerimientos se continuó con el diseño la interfaz gráfica del sistema de gestión de incidentes y el diseño de la base de datos, para ello se utilizó la tecnología PHP y el sistema gestor de base de datos Mysql por pertenecer a la rama de software libre, el cual, es un beneficio para la empresa la mitigación de costos adicionales.

3. El adecuado manejo de la información de los incidentes notificados a los jefes directo de los colaboradores, el cual, se encuentran almacenados en la base de datos, mejoró la generación de los reportes estadísticos, así mismo, ayudó a conocer el estado actual de los casos reportados, a su vez, ayudará a los futuros procesos de auditoria.

4. Comparando los indicadores de envío de correos con datos de tarjeta hacia dominios externos “No Autorizados”, se observa una reducción de 26,67% a 11,67% demostrando así que con el uso del sistema de gestión de incidentes contribuye en la mitigación de pérdida de datos de tarjeta por correo electrónico en 15%.

5. De los tiempos promedios de exposición de los incidentes, se observa que en el mes de noviembre del 2014 su obtuvo en términos de porcentaje un tiempo promedio de 368% y en el mes de junio del 2015 se obtuvo un tiempo promedio de 256% teniendo como resultado una reducción de 12% del lapso de tiempo promedio de los incidentes notificados sin respuesta de los jefes directos.

6. Mediante el uso del sistema de gestión de incidentes se logró reducir el tiempo de ejecución del proceso de notificación en un 50% del tiempo máximo, ya que se demuestra que los operadores SOC sin el uso del sistema de gestión realizaban la notificación en un tiempo promedio de 15 min por evento y con el uso del sistema de gestión el tiempo de notificación por evento es de 5 min.

7. La ejecución del procedimiento de Prevención de Pérdida de Datos (DLP) mediante el uso del sistema de gestión de incidentes, mejoró las Comunicaciones y Operaciones en la empresa Digiware ya que se optimizó el proceso de notificación, a su vez, se verificó la satisfacción de los operadores que utilizaron el sistema de gestión de incidentes permitiendo un mejor control y calidad de servicio.

# RECOMENDACIONES

- Realizar una correcta presentación del sistema de gestión de incidentes al supervisor y todos los operadores SOC. Ya que de esta manera, se informará el qué y para qué se realizó la implementación del sistema.

- Se recomienda a la empresa Digiware, continuar el desarrollo de este proyecto, a fin de implementar nuevas funciones que solucione necesidades que se puedan presentarse en el futuro, ya que el sistema está construido bajo el patrón de arquitectura de software MVC, el cual, permite agregar nuevas funcionalidades.

- Realizar periódicamente mantenimientos preventivos y correctivos al sistema y asignar tareas de mantenimiento a los encargados del cuidado del mismo.

- Elaborar un plan de respaldo (Backup) con frecuencia, de toda la información de sistema. De igual forma, se recomienda almacenar dichos Backups en lugares seguros y de fácil acceso en caso de emergencia.

- Se recomienda al Supervisor y Operadores del área de Seguridad de la Información actualizar el documento de ejecución del procedimiento de prevención de pérdida de datos (DLP), ya que los operadores utilizarán el sistema de gestión de incidentes para la notificación de los eventos, esto servirá para los nuevos operadores que se integren posteriormente al área de trabajo de la empresa.

# BIBLIOGRAFÍA


1. Vilma Crist, Palli Apaza. (2014), "*Modelo de gestión de incidencias basado en ITIL para reducir el tiempo de diagnóstico de incidentes del servicio de soporte técnico en la Universidad Nacional del Altiplano Puno - 2014*" Universidad Nacional del Altiplano, Puno – Perú.

2. José, Buenaño Quintana y Marcelo Alfonso, Granda Luces. (2009), "*Planeación y Diseño de un Sistema de Gestión de seguridad de la Información basado en la norma ISO/IEC 27001 – 27002*", Universidad Politécnica Salesiana, Guayaquil – Ecuador.

3. Arnaldo José, Añez Araujo y Marco Antonio, Rodríguez Henríquez. (2011) "*Implantación de un sistema de gestión de incidencias para la empresa Servicios Fv Venezuela 2010*", Universidad Nueva Esparta, Caracas – Venezuela.

4. Cobo Ángel, Gómez Patricia, Pérez Daniel y Rocha Roció. (2005), "*PHP y MySql Tecnologías para el desarrollo de aplicaciones web"*. Extraído el 24 de Septiembre del 2015, de: https://books.google.es/books?id=zMK3GOMOpQ4C&printsec=frontcover&hl=es#v=onepage&q&f=false

5. Serna Barrera Juan Alberto. (2010), *"Desarrollo de un sistema de base de datos para la administración de un gimnasio mediante la metodología de proceso unificado racional (RUP)".* Extraído el 24 de septiembre del 2015, de: http://proyectosport.freeiz.com/archivos_de_categorias/proyecto_Sport_Byke/1PROY1_METODOLOGIA_RUP.docx

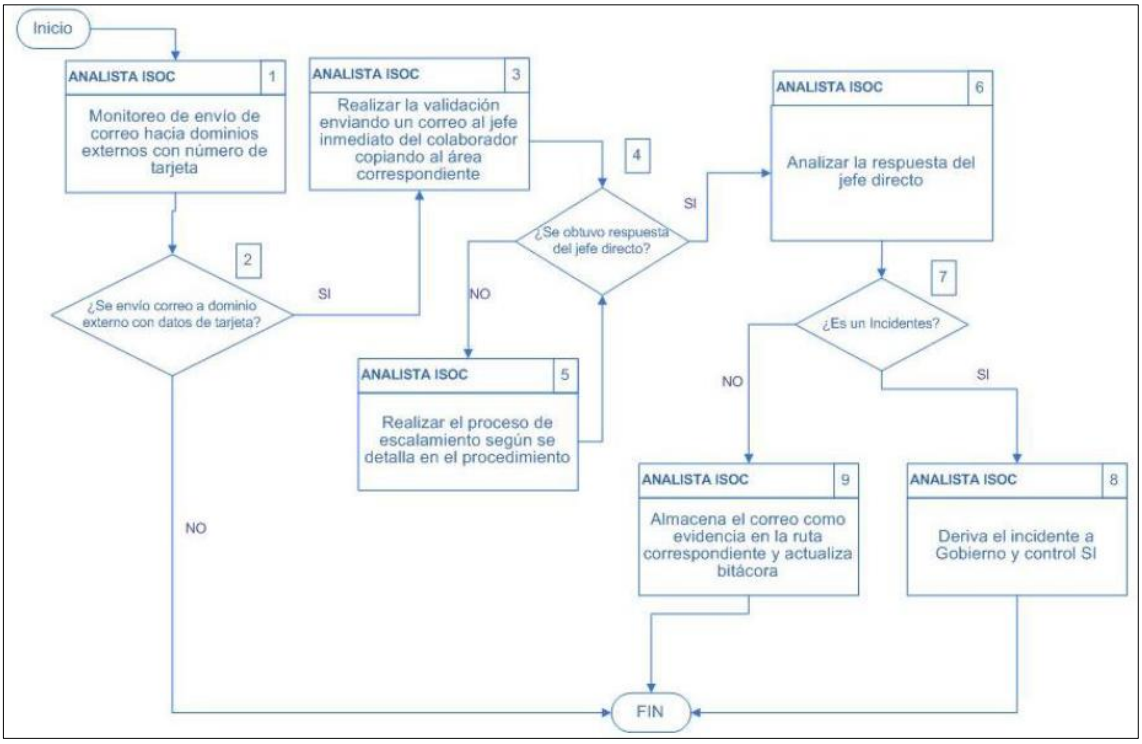
6. Xavier Ferré Grau, María Isabel Sánchez Segura. (2011), *"Desarrollo Orientado a Objetos con UML".* Extraído el 02 de Octubre del 2015, de: http://www.uv.mx/personal/maymendez/files/2011/05/umlTotal.pdf

7. Gestión de Calidad. (2009), "ISO 27002:2005 (Anterior ISO 17799:2005)". Extraído el 24 de Septiembre del 2015, de: http://www.gestion-calidad.com/iso-27002.html

8. Leonardo Camelo. (2010), "ISO 27001 e ISO 27002: Dominio 10 - Gestión de Comunicaciones y Operaciones". Extraído el 20 de Agosto del 2015, de: http://seguridadinformacioncolombia.blogspot.pe/search/label/Comunicaciones%20y%20Operaciones

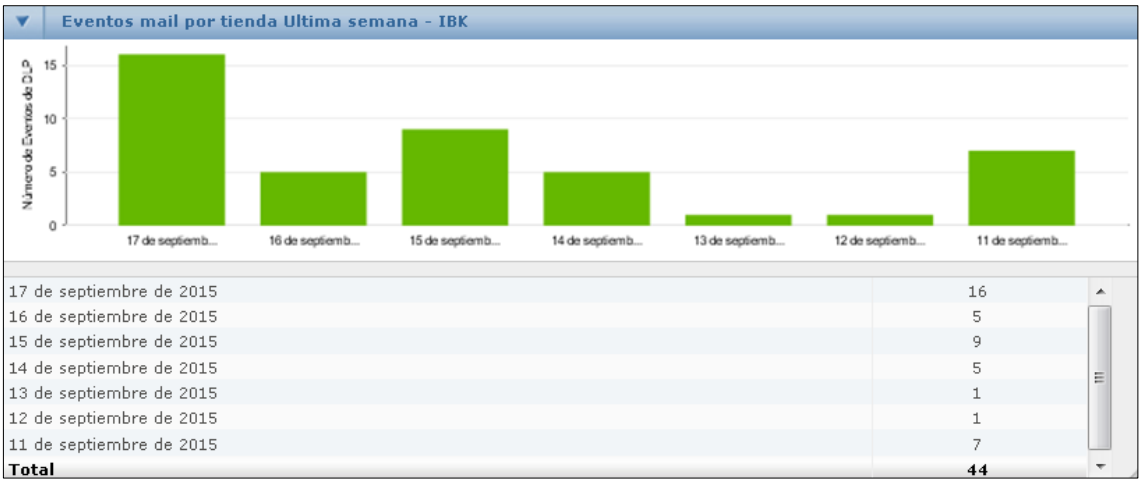
# ANEXOS

**Anexo 01:** Diagrama de actividades del procedimiento monitoreo de incidencias de prevención de pérdida de datos de tarjeta.

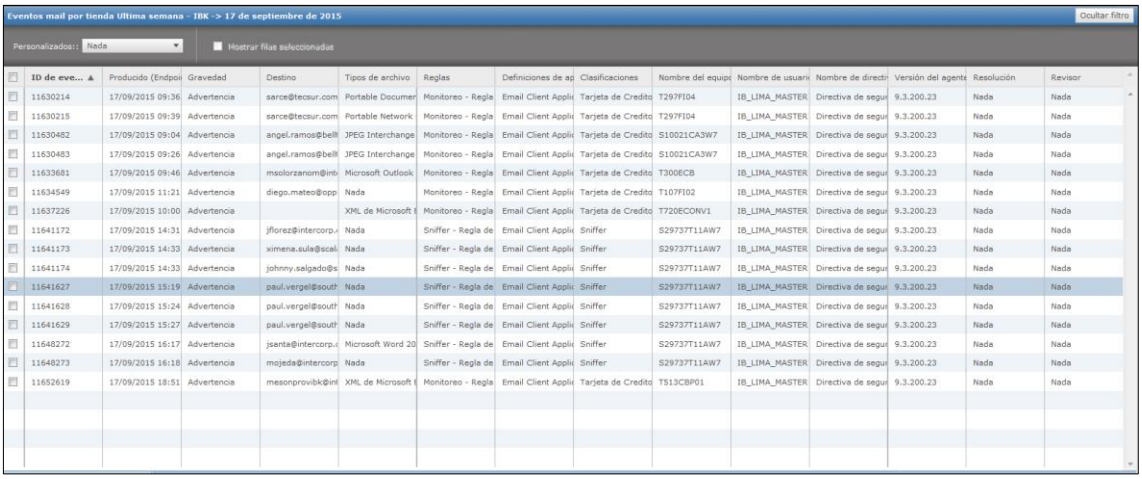


**Anexo 02:** Ventana de logeo de inicio de sesión en la herramienta de monitoreo ePolice Orchestrator (McAfee).

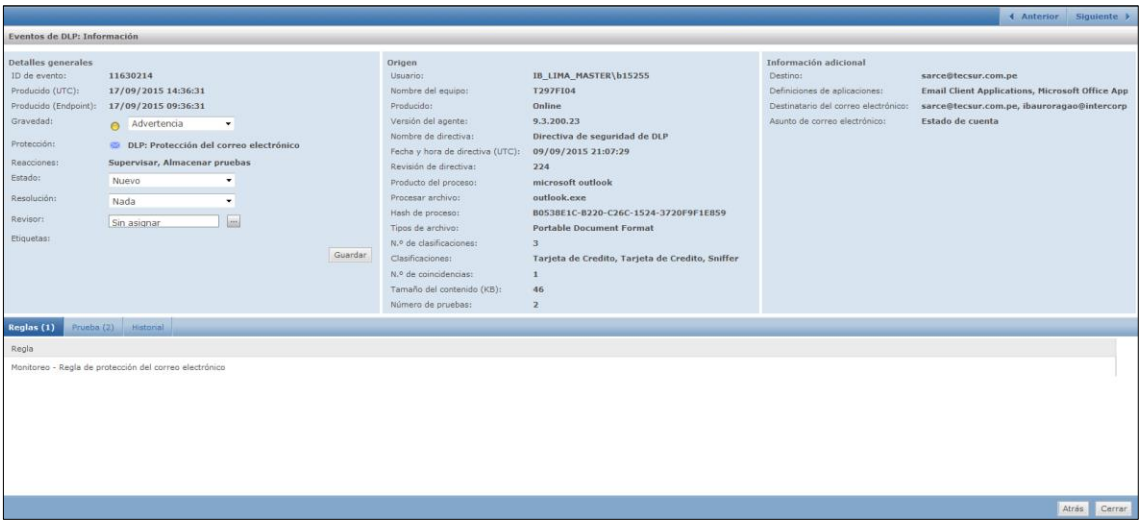

**Anexo 03:** Panel de monitoreo con “Eventos email por tienda”. Correos enviados a dominios externos conteniendo datos de tarjetas.



**Anexo 04:** Lista de eventos de correos enviados desde el dominio del banco hacia dominios externos.




**Anexo 05:** Detalle del evento producido por el envío de correo con datos de tarjeta hacia un dominio externo.



**Anexo 06:** Encuesta realizada a todos los usuarios beneficiados del sistema.

## ENCUESTA

Agradecemos dar respuesta con la mayor trasparecía y veracidad a las diversas preguntas del cuestionario.

1. ¿Qué le pareció el sistema de gestión de incidentes?
   a) Excelente
   b) Bueno
   c) Regular
   d) Malo

2. Operar con el sistema de gestión de incidentes le pareció:
   a) Fácil
   b) Sencillo
   c) Un poco complicado
   d) Difícil

3. ¿En qué aspectos le ha ayudado la utilización del sistema en su proceso de notificación de incidentes?
   a) Orden
   b) Rapidez
   c) Seguridad
   d) Calidad de servicio

4. Respecto al uso del sistema de gestión de incidentes, diga usted ¿cuánto tiempo tarda aproximadamente en notificar un incidente de DLP?
   a) 20 min.
   b) 15 min.
   c) 10 min.
   d) 5 min.

5. ¿A diferencia del proceso tradicional de monitoreo de incidentes del DLP y ahora con el uso del sistema de gestión de incidentes. ¿Cómo calificarías el cambio?
   a) Excelente
   b) Mejor
   c) Igual
   d) Peor

6. ¿Desde su perspectiva, en que cree usted que debería mejorar el sistema de gestión de incidentes?
   a) Agregar más opciones
   b) La interfaz o diseño
   c) La sencillez de uso
   d) La seguridad

7. ¿Cree usted que con el uso del sistema de gestión de incidentes, se hace más efectiva la comunicación con los jefes directos de los colaboradores?
   a) Si
   b) No
   c) No sabe
   d) No responde

8. ¿Indique cómo se siente con el uso del sistema de gestión de incidentes?
   a) Muy satisfecho
   b) Satisfecho
   c) Insatisfecho
   d) Muy insatisfecho

Ha terminado su encuesta, muchas gracias por su opinión.