ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA INFORMÁTICA CON ÉNFASIS EN DESARROLLO DE SOFTWARE

SISTEMA AUTOMATIZADO DE EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO PARA EL ÁREA DE TECNOLOGÍA DE INFORMACIÓN DEL BANCO DE COSTA RICA

Sustentante: José Ricardo Chinchilla Méndez

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE

LICENCIADO EN INGENIERÍA INFORMÁTICA

San José – Costa Rica

JUNIO 2005

Índice de Contenido

Índice de Cuadros

Índice de Gráficos

INTRODUCCIÓN

Siguiendo las disposiciones que sobre supervisón bancaria ha emitido el Comité de Basilea, el Consejo Nacional de Supervisión Financiera (CONASIF), a través de la Superintendencia General de Entidades Financieras (SUGEF), ha establecido una serie de normativas prudenciales, tendientes a mantener la salud financiera del Sistema Financiero Nacional, con el fin de proteger razonablemente los intereses de los depositantes.

Por tal razón, SUGEF utiliza cuestionarios de autoevaluación con el fin de que las instituciones bajo su fiscalización, reporten lo más objetivamente posible, tanto su estado de la gestión como su estado de administración de los recursos. Parte de esta evaluación, incluye un módulo o modelo propiamente diseñado para el área de Tecnología de Información (TI), que dado su naturaleza, es totalmente diferente al modelo de *Autoevaluación de la Gestión*, el cual comprende la parte administrativa y funcional de las entidades. Sin embargo, su metodología de evaluación es muy similar.

Con el propósito de cumplir con las directrices de la SUGEF enunciadas en la *Normativa de Tecnología de Información Para las Entidades Fiscalizadas*, publicada en el diario oficial *La Gaceta* en enero del 2003; el Banco de Costa Rica utilizó la herramienta Microsoft Excel para desarrollar un modelo de autoevaluación de la gestión para el área de Tecnología de Información, adaptado a los parámetros establecidos que permitió a la Institución presentar su calificación del área a la Superintendencia.

Sin embargo, esta herramienta no cumple con las expectativas de oportunidad, integridad y disponibilidad de la información que se requieren. A pesar de haber facilitado en cierta parte el proceso de evaluación, no administra la información en forma confiable ni oportuna, lo cual contradice los principios de la *Ley General de Control Interno No. 8292* (bajo la cual se rigen las instituciones estatales), correspondientes tanto al manejo eficiente y eficaz de los recursos, como a la disponibilidad y confiabilidad de la información.

Además, carece de un proceso automático de generación de estadísticas específicas para la toma de decisiones, situación que genera gran trabajo para la Oficina de Riesgo y Control Interno del Banco de Costa Rica, la cual es la encargada de aplicar dicha evaluación, disminuyendo el tiempo de atención hacia otras situaciones pendientes.

Con esta investigación, se pretende analizar el modelo de *Autoevaluación de la Gestión Para el Área de Tecnología de Información del Banco de Costa Rica*, con el propósito de diseñar un Sistema de Información que incremente la productividad de aplicación de dicha evaluación. Se analizará aspectos como la normativa que sustenta este modelo, así como su estructura y metodología de calificación y clasificación de las entidades.

Esta evaluación del área de Tecnología de Información, está compuesta por los siguientes factores:

1- Administración de TI
2- Seguridad lógica y acceso a datos
3- Seguridad física
4- Sistemas de información
5- Software y bases de datos
6- Hardware, redes y comunicaciones
7- Continuidad de las operaciones
8- Servicios financieros por Internet
9- Descentralización de procesamiento en el exterior

También, se evaluarán aspectos como el tiempo requerido para realizar completamente la evaluación, cantidad y duración de las tareas manuales y las automatizadas, estado actual del control interno, controles concernientes a Tecnología de Información, satisfacción de los usuarios, entre otros.

.

En resumen, se detallará la forma o el modelo de aplicación de evaluación del sistema de control interno para el área de Tecnología de Información del Banco de Costa Rica. Se determinará el cómo, el porqué y el qué evalúa este modelo de evaluación exigido por la SUGEF para las entidades bajo su fiscalización; y se propondrá el diseño de un Sistema de Información Automatizado que incremente la productividad de la metodología actual de evaluación.

JUSTIFICACIÓN

Como parte de la evaluación que debe realizar la Superintendencia General de Entidades Financieras (SUGEF) al Banco de Costa Rica, de conformidad con las disposiciones del Consejo Nacional de Supervisión Financiera (CONASIF), se aplica un cuestionario con formato de autoevaluación, para que la Institución reporte su estado al ente fiscalizador. Este modelo contiene los lineamientos generales que la SUGEF utiliza para evaluar la administración, los sistemas, los equipos, la seguridad, la utilización y los controles aplicados al Área de Tecnología de Información (TI) de las entidades fiscalizadas, con el fin de velar por la estabilidad y la eficiencia de la entidad y el sistema financiero nacional.

La plataforma informática del Banco de Costa Rica permite el desarrollo de un Sistema de Información que incluya todas las variables y parámetros contemplados en el modelo anteriormente citado, generando información oportuna, confiable y precisa para la toma de decisiones gerenciales.

Actualmente, el gran volumen de información que se requiere procesar con el objetivo de evaluar el área de Tecnología de Información del Banco, se administra con la herramienta Microsoft Excel, la cual resta efectividad a la hora de la retroalimentación de información gerencial, ya que la hoja electrónica es poco versátil, poco segura y requiere invertir mucho tiempo en el ingreso de información, mismo que podría utilizarse en labores del análisis de ésta, además de limitar la oportunidad de la información como se indicó anteriormente.

La información almacenada en esta herramienta debe ser analizada rigurosamente para determinar estadísticas, conclusiones, dar seguimiento a los planes de acción, tomar decisiones, etc. Este proceso requiere mucho tiempo y esfuerzo por parte del personal de la Oficina de Riesgo y Control Interno.

Con la implementación de una nueva herramienta con un grado mayor de complejidad, en este caso un Sistema de Información, se pretende incrementar la productividad de aplicación del modelo de evaluación del control interno para el Área de Tecnología de Información, así como, la eficiencia, eficacia y agilización de procedimientos por parte de la oficina encargada (Riesgo y Control Interno).

Así mismo, el proceso de evaluación incluye los procedimientos de envío y recibo de los cuestionarios dentro del modelo de evaluación para las distintas oficinas, lo que conlleva, su posterior tabulación manual. Con este nuevo Sistema de Información, se pretende eliminar estos procesos mediante un sitio web interno, en donde los cuestionarios sean respondidos en línea y automáticamente se tabulen los datos almacenados en la base de datos.

Esta herramienta le permitirá al Banco de Costa Rica, obtener mejores resultados, mayor exactitud e integridad de la información, menores tiempos de respuesta, mayor aprovechamiento de los recursos, tanto técnicos como humanos, información oportuna, mayor confiabilidad, etc.

Por otra parte, la Institución está considerando invertir en una herramienta con estas características, por lo que al poder ser desarrollada internamente, disminuye los costos, el tiempo de integración de las normativas y leyes involucradas en el marco teórico del modelo y además, reduce considerablemente el tiempo de implementación. Esto debido a que no se debe realizar el debido proceso de licitación y contratación administrativa (por una Entidad Pública), el cual toma alrededor de varios meses.

PLANTEAMIENTO DEL PROBLEMA

Situación actual:

El Banco de Costa Rica cuenta con una herramienta matricial desarrollada con la herramienta Microsoft Excel con el propósito de realizar la Auto evaluación de la Gestión del área de Tecnología de Información (Calificación Cualitativa) requerida por la Superintendencia General de Entidades Financieras. Esta herramienta, que permite evaluar el sistema de administración de riesgos que la Junta Directiva y la Plana Gerencial han implementado, consta de 26 matrices para los nueve factores por evaluar de conformidad con la normativa SUGEF (Administración de TI, Seguridad lógica y acceso a los datos, Seguridad física, Sistemas de Información, Software y bases de datos, Hardware, redes y comunicaciones, Continuidad de las operaciones, Servicios financieros por Internet y Descentralización de procesamiento en el exterior) y contempla aproximadamente un total de 300 preguntas puntuales a todos y cada uno de los aspectos ponderables para establecer la calificación para cada área sustantiva del área de TI (División de Tecnología de Información, Gerencia de División de Proyectos, Gerencia de División de Producción, Proyectos de Tecnología, Soporte Administrativo, Control y Seguimiento de Proyectos, Ingeniería de Sistemas, Investigación y Estrategias Tecnológicas, Seguridad en Tecnología, Telecomunicaciones y Servicios Técnicos, Procesamiento de Datos y Banca Electrónica).

Lo anterior, hace de esa herramienta un Sistema de Información muy importante, sin embargo, presenta problemas de oportunidad ya que el proceso de calificación es muy laborioso y lento y por su operatividad se requiere un mayor control interno para que los resultados sean precisos y confiables.

El tiempo de análisis de los cuestionarios y su respectiva comunicación de resultados, que le toma a la Oficina de Riesgo y Control Interno, sobrepasa los límites esperados. Esta situación se presenta debido a que se deben tabular todos los datos de las distintas oficinas evaluadas y promediar su resultado manualmente. Así como realizar las

respectivas estadísticas de análisis para la toma de decisiones de la alta Gerencia, aspectos que con un Sistema de Información se realizarían en segundos, prácticamente.

Además, los cuestionarios deben enviarse por correo electrónico a todas las oficinas por evaluar y, posteriormente, se reciben por este mismo medio, por lo que el manejo de los archivos se vuelve prácticamente incontrolable. Actualmente, no existe un método o medio automatizado que reemplace estos procedimientos del proceso de evaluación., como por ejemplo, un sitio web en la red interna del Banco, en donde los encargados de oficina llenen sus respectivos cuestionarios y el sistema automáticamente almacene la información en una base de datos para su posterior análisis.

La carencia de un Sistema de Información en la Oficina de Riesgo y Control Interno provoca lentitud y falta de eficiencia a la hora de evaluar la Gestión del Área de Tecnología de Información. Además, debido a la naturaleza de esta investigación, se pueden llegar a implementar en un futuro, los módulos de evaluación para las evaluaciones correspondientes a la Contraloría General de la República y la evaluación propia específica de la Oficina de Riesgo y Control Interno con la metodología aplicada, cuando éstas así lo requieran.

Además, el Banco de Costa Rica puede llegar a sacarle un mayor provecho a este sistema, ya que actualmente, ninguna de las entidades fiscalizadas por la SUGEF cuenta con un sistema automatizado de aplicación de este modelo de evaluación. Por lo que, adicional a su funcionalidad como herramienta de trabajo, en un futuro cercano, el Banco podría tomar en consideración el llegar a posicionarlo en las demás instituciones.

Otro gran problema que se presenta con la metodología empleada actualmente, es que el proceso de generación de reportes es sumamente lento y tedioso, lo que provoca atrasos considerables en la presentación de resultados.

FORMULACIÓN DE PROBLEMA

Problema:

¿Cómo puede un sistema automatizado incrementar la productividad en la aplicación del modelo de Evaluación del Sistema de Control Interno para el Área de Tecnología de Información del Banco de Costa Rica?

MATRIZ DE OBJETIVOS

Tema	Problema	Objetivos	
		General	Específico
Sistema automatizado de evaluación del Sistema de Control Interno para el Área de Tecnología de Información del Banco de Costa Rica.	¿Cómo se puede incrementar la productividad de la aplicación del modelo de Evaluación del Sistema de Control Interno para el Área de Tecnología de Información en el Banco de Costa Rica?	Investigar la metodología de aplicación de la evaluación del Sistema de Control Interno para el Área de Tecnología de Información del Banco de Costa Rica.	1- Analizar el marco teórico - legal bajo el cuál se sustenta la evaluación. 2- Examinar la metodología empleada actualmente por el modelo de evaluación. 3- Determinar el grado de satisfacción actual del usuario.
		Diseñar un sistema automatizado de evaluación del Sistema de Control Interno para el Área de Tecnología de Información del Banco de Costa Rica.	1- Definir los requerimientos del sistema. 2- Esquematizar el funcionamiento del sistema mediante la herramienta de modelado UML. 3- Materializar el diseño del sistema (Demo).

Fuente: Elaboración propia

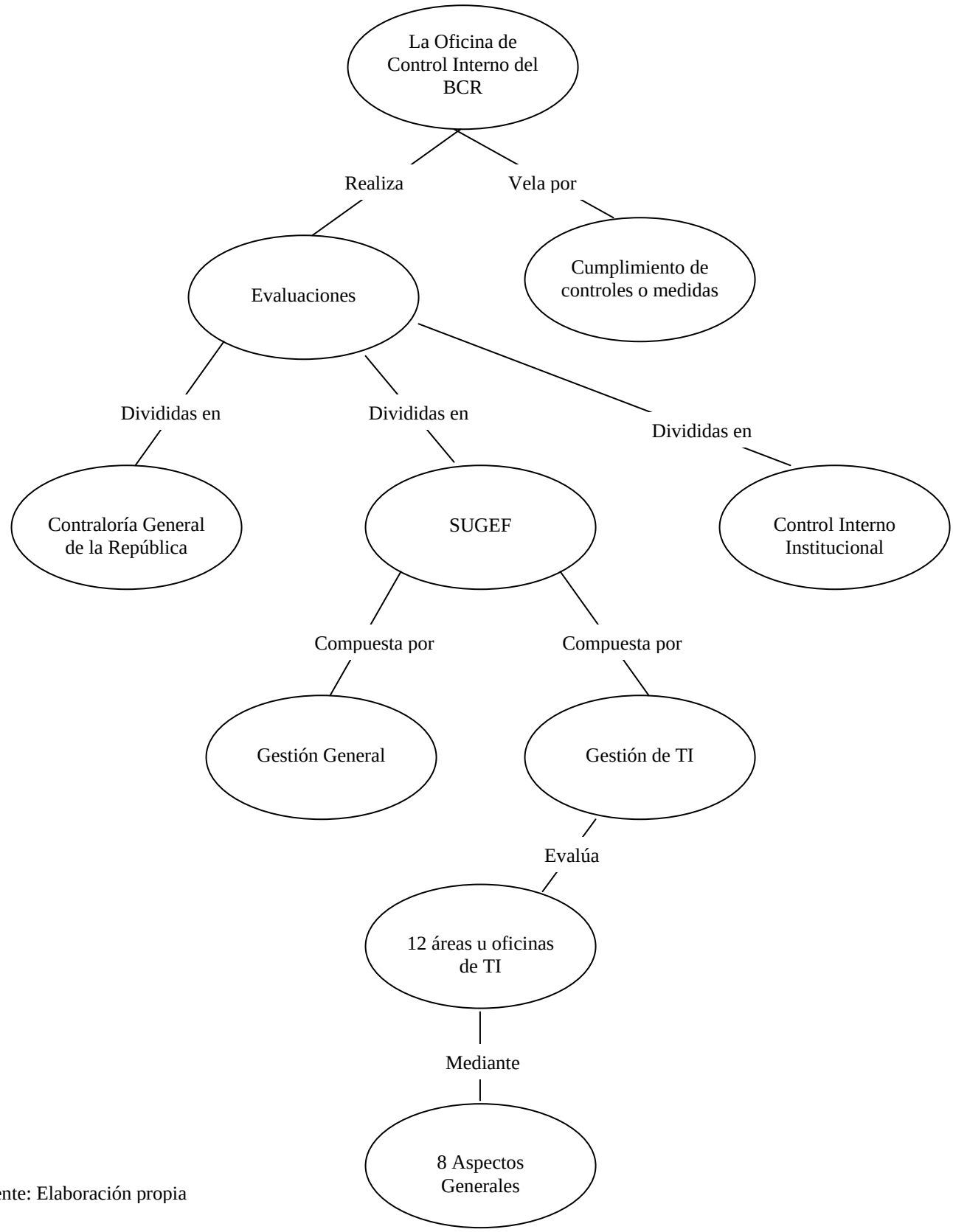
MATRIZ DE VARIABLES

Variable	Definición Conceptual	Definición Operacional	Indicadores	Instrumentos de Recolección de Datos
Tiempo total del proceso de evaluación	Duración total del proceso de evaluación por parte de la oficina de Control Interno.	Medir el tiempo total que le toma a la oficina de Control Interno evaluar las distintas áreas de TI.	Tiempo de envío Tiempo de llenado Tiempo de recibo Tiempo de consolidación Tiempo mínimo Tiempo promedio Tiempo máximo	Observación participante
Cantidad de tareas	Cantidad de tareas o procedimientos que se llevan a cabo	Contar la cantidad de tareas que se realizan durante el proceso de evaluación	Número de tareas manuales y automatizadas Duración de tareas	Observación participante
Grado de conocimiento del modelo de evaluación	Conocimiento del modelo de evaluación por parte de los funcionarios de la Oficina de Riesgo y Control Interno	Medir el grado de conocimiento del modelo de evaluación por parte de los funcionarios de la Oficina de Riesgo y Control Interno	Áreas y enfoque de evaluación Metodología de calificación Áreas a evaluar Metodología de envío/llenado/ recibo Metodología de consolidación	Encuesta Observación

Variable	Definición Conceptual	Definición Operacional	Indicadores	Instrumentos de Recolección
Eficiencia y eficacia del proceso	Mejor aprovechamiento del tiempo, los recursos y la consecución de los objetivos	Medir el tiempo promedio de evaluación y valorar el alcance de los objetivos	Tiempo de envío/recibo Tiempo de consolidación Tiempo de clasificación de resultados Tareas que se pueden automatizar Cantidad de recursos utilizados	Observación participante
Eficiencia y eficacia en la generación de reportes	Eficiencia y eficacia del proceso de generación de reportes	Medir el tiempo de generación de reportes y valorar la calidad del contenido de los mismos	Tiempo de generación Facilidad de generación Calidad del contenido	Observación participante Encuesta
Satisfacción del usuario	Grado de satisfacción del usuario respecto del método actual de evaluación del control interno	Medir el grado de satisfacción del usuario respecto del método actual de evaluación del control interno del área de TI del BCR	Grado de satisfacción general del usuario Facilidad del manejo de respuestas Facilidad de tabulación de respuestas Facilidad de corrección de respuestas	Encuesta

Fuente: Elaboración propia

MAPA CONCEPTUAL



Fuente: Elaboración propia

MARCO TEÓRICO

Aplicación:

La Oficina de Riesgo y Control Interno del Banco de Costa Rica cumple una función contralora dentro de la Institución. Sus funciones son muy parecidas a las de la Auditoría Interna, pero con un énfasis un poco más preventivo que "policial". Entre sus principales funciones se mencionan las siguientes:

- ✓ Evaluar periódicamente las distintas áreas u oficinas de la entidad
- ✓ Incorporar nuevas medidas de control que fomenten la disminución del Riesgo Operativo
- ✓ Velar por el cumplimiento de dichas medidas de control
- ✓ Evaluar los sistemas de información
- ✓ Seguimiento de pendientes de la Auditoría, Comité de Operaciones, Gerencia General o Junta Directiva
- ✓ Entre otros

Con respecto a las evaluaciones periódicas que debe realizar esta oficina, se dividen en 3 grupos:

1. Correspondiente a la Contraloría General de la República
2. Correspondiente al Control Interno Institucional
3. Correspondiente a SUGEF

El primer grupo evalúa todas las áreas de la Institución en una forma general, orientado más que todo al Riesgo Operativo en área financiera. El segundo grupo evalúa áreas específicas, tales como Recursos Humanos, Bolsa de Valores, Comercio Exterior, Banca Comercial, Tecnología de Información, Fondos de Inversión, etc. El tercer y último grupo divide su evaluación en dos grandes áreas:

1. Evaluación de la Gestión General: Evalúa la operación de las distintas áreas de la Institución en una forma general. Esta se divide en Planificación, Políticas y Procedimientos, Administración de Personal, Sistemas de Control y Sistema de Información Gerencial.

2. Evaluación de la Gestión de TI: Evalúa el sistema de control interno respecto de la operación específica del área de Tecnología de Información de las entidades fiscalizadas por la Superintendencia General de Entidades Financieras. Esta se divide en: Planeación y Organización, Seguridad Lógica y Acceso a Datos, Seguridad Física, Sistemas de Información, Software y Bases de Datos, Hardware, Redes y Comunicaciones, Continuidad de las Operaciones, Servicios Financieros por Internet; y Descentralización de Procesamiento en el Exterior (Por el tipo de clasificación de la Institución según la SUGEF, no se evalúa esta área).

Esta evaluación se aplica en las once distintas áreas de la División de Tecnología de Información, las cuales se mencionan a continuación:

1. División de TI
2. Seguridad en TI
3. Servicios Técnicos
4. Ingeniería de Procesos
5. Mantenimiento de Sistemas
6. Desarrollo de Proyectos Informáticos
7. Procesamiento de Datos
8. Investigación Tecnológica
9. Control de Calidad
10. Banca Electrónica
11. Telecomunicaciones

Cada una de estas áreas debe responder el cuestionario de evaluación y remitirlo a la Oficina de Riesgo y Control Interno para su respectivo análisis y comunicación de resultados a las áreas gerenciales.

Matriz de Evaluación:

Según la *Normativa de Tecnología de Información Para las Entidades Fiscalizadas por la SUGEF*, la evaluación debe estar compuesta por las siguientes áreas generales de evaluación:

1. Administración de TI: Se deben evaluar aspectos como:

    a. Realizar un proceso de planificación de TI de acuerdo con la planeación estratégica institucional, que facilite la consecución de sus logros futuros.

    b. Identificar, organizar, capacitar y desarrollar a los usuarios finales en el uso efectivo de la tecnología, seguridad, riesgos y responsabilidades relacionadas con el desarrollo normal de sus funciones. Asimismo, mantener un programa de capacitación de acuerdo con las prioridades de la administración.

    c. Procurar que a través de métodos y esquemas de trabajo, se facilite la consecución de los objetivos planteados, mediante una ubicación independiente de TI dentro de la estructura organizacional, actualización constante del manual de puestos para el personal de TI, definición de procedimientos que permitan la contratación y adquisición de recursos de TI, así como, la correcta administración de los *outsourcing*s.

    d. Procurar a través de diferentes mecanismos, que los miembros de la organización actúen de modo que contribuyan al logro de los objetivos. Para esto la entidad debe establecer y comunicar los objetivos de la

administración y las políticas de TI, a los niveles pertinentes. Además, debe contar con personal técnicamente capacitado o en su ausencia contratarlo externamente.

e. La entidad debe implantar los mecanismos de control necesarios para la supervisión de las tareas. Para esto debe verificar el cumplimiento de los controles y objetivos establecidos para los procesos de TI; contar con un contrato vigente de prestación de servicios para el caso en que sus servicios de TI no sean propios; y Velar por el cumplimiento de sus obligaciones legales, regulatorias y contractuales, en los plazos y formas establecidas, así como las que terceros han establecido con la entidad.

- Seguridad lógica y acceso a datos:

a. La entidad debe administrar adecuadamente la seguridad lógica de los recursos de TI. Para esto la entidad debe:

   - Establecer políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos.

   - Establecer políticas y procedimientos que permitan dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos.

b. La entidad debe mantener una adecuada seguridad en todos aquellos puntos con acceso a redes públicas de datos. Para esto la entidad debe:

   - Definir controles que permitan restringir el tráfico hacia dentro y fuera de la red institucional (Pared de fuego).

- Establecer políticas y procedimientos de prevención, detección y corrección de virus.

- Establecer políticas y procedimientos que regulen la utilización del correo electrónico.

- Seguridad Física: La entidad debe:

  a. Establecer políticas y procedimientos relacionados con la ubicación, construcción, acceso físico al (a los) centro(s) de cómputo y comunicaciones.

  b. Contar con procedimientos de control que regulen las condiciones ambientales del (los) centro(s) de cómputo y comunicaciones.

- Sistemas de Información: La entidad debe:

  a. Procurar a través de procedimientos de trabajo, el diseño e implementación de sistemas de información eficaces, seguros y que impidan la modificación no autorizada, asimismo se ajuste al cumplimento de las leyes, reglamentos y normativa vigente que les sean aplicables. Para esto la entidad debe:

     - Implementar una metodología para el ciclo de vida del desarrollo de sistemas, que asegure la calidad de los sistemas de información y satisfaga los requerimientos del usuario.

     - Definir una adecuada separación de los ambientes de desarrollo y producción, de forma que el personal de desarrollo no tenga acceso al ambiente en producción.

  b. Velar por la adecuada disponibilidad, capacidad y el desempeño de los sistemas de información.

c. Contar con políticas y procedimientos relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, que asegure que los mismos permanezcan completos, precisos y válidos.

- Software y Bases de Datos: La entidad debe:

a. Administrar adecuadamente sus bases de datos. Para esto debe:

- Definir la arquitectura de información para organizar y aprovechar de la mejor forma los sistemas de información.

- Establecer políticas y procedimientos actualizados relacionados con la instalación, administración, migración, mantenimiento y seguridad de las bases de datos.

- Definir mecanismos para controlar la integridad, disponibilidad, capacidad y el desempeño de las bases de datos.

- Definir períodos de almacenamiento y eliminación de información, acordes con los requerimientos legales.

b. Definir políticas y procedimientos para la adecuada instalación, mantenimiento y administración de *Software* debidamente autorizado.

- Hardware, Redes y Comunicaciones: La entidad debe:

a. Administrar adecuadamente el *Hardware*, las redes y las líneas de comunicación. Para esto debe:

- Realizar estudios de capacidad y desempeño del *Hardware* y las líneas de comunicación.

- Establecer mecanismos para procurar que todas las redes instaladas, ya sean eléctricas, de voz o de datos, cumplan con los requerimientos mínimos vigentes de cableado estructurado.

- Establecer políticas y procedimientos para la instalación y mantenimiento del *Hardware* y su configuración base.

b. Administrar adecuadamente su red de Cajeros Automáticos. Para esto:

- Establecer políticas y procedimientos para la ubicación, protección y mantenimiento de los cajeros automáticos.

- Mantener en línea los cajeros automáticos con los sistemas de información de la entidad.

- Establecer políticas y procedimientos para la comunicación al cliente sobre el uso adecuado de los cajeros automáticos.

- Mantener activas las bitácoras.

- <u>Continuidad de las Operaciones</u>: La entidad debe:

a. Establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información.

b. Establecer un plan de continuidad, donde se detallen acciones, procedimientos y recursos que considere los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios de TI.

c. Contar con una infraestructura adecuada, que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red pública.

d. Contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones.

- Servicios Financieros por Internet: La entidad debe:

a. Establecer y comunicar a sus clientes las condiciones legales y operativas bajo las cuales se brindará el servicio financiero por Internet.

b. Administrar adecuadamente la seguridad lógica de los servicios financieros por Internet. Para esto debe:

   - Establecer políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso al servicio financiero por Internet.

   - Implementar mecanismos de seguridad que protejan la integridad y privacidad de la información sensible cuando el canal de transmisión sea Internet.

   - Implementar y dar mantenimiento a los mecanismos de seguridad.

   - Mantener activas las bitácoras.

c. Considerar dentro del plan de continuidad, un apartado donde se detallen acciones, procedimientos y recursos que consideren los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios financieros por Internet.

d. Velar por la adecuada disponibilidad, capacidad y el desempeño de los servicios financieros por Internet.

e. Comunicar a los clientes que utilicen los servicios financieros por Internet, cuando se abandona el sitio *web* de la entidad y se accede el de un tercero.

- Descentralización de Procesamiento en el Exterior: La entidad debe:

    a. Ajustarse a la normativa vigente en TI de la Superintendencia General de Entidades Financieras.

    b. Considerar dentro del plan de continuidad, la interrupción del procesamiento en el sitio remoto.

Metodología de Evaluación:

A continuación se presenta la metodología de evaluación que utiliza SUGEF para evaluar sus entidades fiscalizadas. La Oficina de Riesgo y Control Interno del Banco de Costa Rica debe utilizar la misma metodología pero de forma interna.

La Oficina de Riesgo y Control Interno comunicará a las oficinas bajo su supervisión una calificación cuantitativa sobre el área de Tecnología de Información; en adelante TI, producto de una autoevaluación, de conformidad con la Matriz de Calificación. Como resultado de la evaluación, cada área obtendrá un porcentaje entre 0 y 100%, y será ubicada en rangos según los cuales se asume menor o mayor riesgo, sea en nivel normal, irregularidad 1, irregularidad 2 o irregularidad 3 de acuerdo con la siguiente tabla.

Metodología de Evaluación

Área	*Normal*	*Irregularidad 1*	*Irregularidad 2*	*Irregularidad 3*
Administración del área de TI	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Seguridad lógica y acceso a los datos	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Seguridad física	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Sistemas de información	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Software y bases de datos	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Hardware, redes y comunicaciones	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Continuidad de las operaciones	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Servicios financieros por Internet	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Descentralización de procesamiento en el exterior	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%

Fuente: SUGEF

La Oficina de Riesgo y Control Interno deberá desarrollar sus propios procedimientos de evaluación para que las oficinas evaluadas puedan autoevaluarse en cada una de las áreas, de acuerdo con esta normativa.

La calificación general (CG) dependerá del tipo de entidad en que se haya clasificado el Banco. El tipo de entidad está relacionado con la tenencia de las dos últimas áreas de evaluación (Servicios financieros por Internet y Descentralización de procesamiento en el exterior) y el valor de riesgo asignado a cada una de las áreas, se distribuirá de acuerdo con la siguiente tabla:

Clasificación de la Entidad

Área	*Tipo de Entidad 1*	*Tipo de Entidad 2*	*Tipo de Entidad 3*	*Tipo de Entidad 4*
Administración del área de TI	14%	14%	14%	14%
Seguridad lógica y acceso a los datos	14%	14%	14%	14%
Seguridad física	12%	12%	12%	12%
Sistemas de información	12%	12%	12%	12%
Software y bases de datos	12%	12%	12%	12%
Hardware, redes y comunicaciones	11%	11%	11%	11%
Continuidad de las operaciones	11%	11%	11%	11%
Servicios financieros por Internet	7%	7%	0%	0%
Descentralización de procesamiento en el exterior	7%	0%	7%	0%
	100%	93%	93%	86%

Fuente: SUGEF

El Banco se clasifica como una entidad tipo 4. La calificación general se obtendrá a partir de la sumatoria del valor de riesgo obtenido en cada una de las áreas de evaluación (VROA) y considerando la siguiente tabla:

Tipo de Entidad

Tipo de entidad	*Fórmula*
1	CG = Σ(VROA)
2	CG = (Σ(VROA)*100)/93
3	CG = (Σ(VROA)*100)/93
4	CG = (Σ(VROA)*100)/86

Fuente: SUGEF

Una vez obtenida la calificación general, la entidad se ubicará en alguno de los estados, según la siguiente tabla; y remitirá su resultado a la SUGEF:

Calificación General

ESTADO	*CALIFICACIÓN GENERAL*
Normal	Mayor o igual que 85%
Irregularidad 1	Mayor o igual que 70% y menor que 85%
Irregularidad 2	Mayor o igual que 55% y menor que 70%
Irregularidad 3	Menor que 55%

Fuente: SUGEF

Sustento legal**:**

Ley General de Control Interno:

La Oficina de Riesgo y Control Interno se rige por la Ley General de Control Interno No. 8292, la cual establece los criterios mínimos que deberán observar la Contraloría General de la República y los entes u órganos sujetos a su fiscalización, en el establecimiento, mantenimiento, perfeccionamiento y evaluación de sus sistemas de control interno. (Asamblea Legislativa, 2002)

Esta ley abarca objetivos, definiciones, estructura del sistema de control interno. Así como, aspectos básicos sobre el sistema específico de valoración del riesgo institucional, funciones de la auditoría interna y sus componentes; y responsabilidades y sanciones para con los jerarcas, los titulares subordinados y demás funcionarios públicos.

Debido a que la aplicación por diseñar debe permitir la evaluación del Sistema de Control Interno del Área de Tecnología de Información del Banco de Costa Rica, ésta debe estar a derecho con respecto a las leyes y disposiciones referentes al control interno.

Normativa de Tecnología de Información Para las Entidades Fiscalizadas por la SUGEF:

Esta normativa contiene los lineamientos generales que la Superintendencia General de Entidades Financieras utiliza para evaluar la administración, los sistemas, los equipos, la seguridad, la utilización y los controles aplicados al Área de Tecnología de Información de las entidades bajo su fiscalización, con el fin de velar por la estabilidad y la eficiencia del sistema financiero. (SUGEF, 2003)

Lenguaje Unificado de Modelado – UML:

UML (Unified Modeling Language) nació en 1994 y es el resultado de la unificación de los tres principales métodos de programación orientada a objetos (Booch, Ingeniería del Software Orientada a Objetos de Jacobson y Técnica de Modelado de Objetos de Rumbaugh). Reúne aspectos fundamentales tanto para el diseño como para la construcción de aplicaciones; desde el concepto hasta los artefactos ejecutables. Booch y Rumbaugh unieron esfuerzos y en 1995 publicaron el borrador de la primer versión (UML 0.8). Por esa época, Jacobson se unió al proyecto y en 1996 publicaron su segunda versión, la versión 0.9. Su consolidación se dio en el año de 1997, cuando distintas empresas apoyaron y patrocinaron el proyecto de estos 3 expertos, con el fin de lograr su final estandarización en el mercado internacional, ofreciendo un lenguaje de modelado bien definido, expresivo, potente y aplicable a una gran cantidad de problemas; la versión 1.0. (Booch, Jacobson y Raumbaugh, 2000)

Según Booch, Jacobson y Rumbaugh (1999), UML es un lenguaje gráfico para visualizar, especificar, construir y documentar los artefactos de un sistema con gran cantidad de software. UML proporciona una forma estándar de escribir planos de un sistema, cubriendo tanto las cosas conceptuales, tales como procesos de negocio y funciones del sistema, como las cosas concretas, tales como las clases escritas en un lenguaje de programación específico, esquemas de bases de datos y componentes de software reutilizables.

Este lenguaje permite una presentación clara y concisa del diseño de un sistema de información, desde su visualización más general hasta sus más complejas especificaciones. Mediante distintos tipos de diagramas, se determina el funcionamiento tanto general como específico del sistema, así como la secuencia de sus distintos procesos y procedimientos, diseño de la base de datos, usuarios o actores que participarán, clases por utilizar, etc.

El Lenguaje Unificado de Modelado es una de las herramientas más utilizadas en la actualidad, debido a que permite especificar no sólo la estructura, comportamiento y

arquitectura de una aplicación, sino que también permite determinar el proceso de negocio y la estructura de los datos. (Object Management Group, 2005).

Es un lenguaje estándar para escribir planos de software. Puede utilizarse para visualizar, especificar, construir y documentar los artefactos de un sistema que involucra una gran cantidad de software. Es un lenguaje muy apropiado para modelar desde sistemas de información en empresas hasta aplicaciones distribuidas basadas en Internet. (Booch et. al., 1999).

MARCO METODOLÓGICO

Tipo de Investigación:

La investigación que se pretende desarrollar se clasifica dentro del tipo *descriptivo*. Esto debido a que se pretenden especificar propiedades y características más importantes del modelo de Evaluación del Sistema de Control Interno para el Área de Tecnología de Información, así como describir la situación en la cual se desarrolla y la metodología empleada. Además, se pretende evaluar y recolectar datos sobre diversos aspectos y componentes del modelo, lo que convierte esta investigación en un estudio descriptivo.

Principalmente, este tipo de investigación busca especificar propiedades, características y rasgos importantes de la situación o fenómeno en estudio, en este caso, el modelo de evaluación. Su fin es recolectar datos *medibles* del proceso de aplicación del modelo de evaluación. (Hernández, Fernández y Baptista, 2003)

Además, este tipo de investigaciones pueden ofrecer la posibilidad de predicciones o relaciones aunque sean poco elaboradas. Es decir, con esta investigación se puede llegar a "predecir" si la productividad o eficiencia del proceso de aplicación del modelo de evaluación se puede aumentar mediante un sistema de información automatizado.

Lo que se pretende es describir de forma minuciosa el modelo de evaluación del Sistema de Control Interno para el Área de Tecnología de Información. Su metodología, cómo se aplica, quién lo aplica, qué es lo que se aplica, etc.

Sujetos y Fuentes de Información:

Esta investigación está enfocada en los problemas de oportunidad de información que se presentan en la Oficina de Riesgo y Control Interno del Banco de Costa Rica, respecto de la aplicación de la Evaluación de Control Interno para el área de Tecnología de Información establecida por SUGEF.

Esta oficina está conformada por un total de 10 personas, de las cuales, cuatro realizan labores de Riesgo Operativo, otras 5 realizan labores de Control Interno y el Jefe de la oficina, que vela por el cumplimiento de ambas partes. Esta investigación se enfocará en la población correspondiente al área de Control Interno y al Jefe de oficina, debido a que estas son las personas que están relacionadas directamente con el problema de investigación.

Debido a que la población es de únicamente seis personas, se utilizará el 100% de la misma.

Población - Muestra

Tema	Población	Muestra	Herramientas
Sistema automatizado de evaluación del sistema de Control Interno para el área de Tecnología de Información del Banco de Costa Rica.	6 personas	6 personas	Encuesta Participación Observación

Fuente: Elaboración propia

Cabe mencionar, que existe otro tipo de usuario que se denomina pasivo. Este se refiere al gerente o encargado de las distintas oficinas que conforman la División de Tecnología del Banco de Costa Rica. Se califica como un usuario pasivo, debido a que su participación durante la evaluación es muy limitada y en realidad, su forma de participación, prácticamente no se verá afectada por dicha automatización, a pesar de brindar parte del insumo requerido (respuestas) durante la misma. Esto debido a que el formato de presentación del cuestionario de evaluación debe ser el mismo, ya sea, al utilizar una herramienta como Microsoft Excel o alguna otra en particular empleada por dicha oficina. Para este usuario, debe ser transparente la metodología empleada por la oficina para el manejo de la información, ya que éste se debe limitar a responder el cuestionario y enviar las respuestas.

Instrumentos de Recolección de Datos:

Una de las herramientas de recolección de datos empleada durante la investigación, fue la observación participante, ya que le permite al investigador formar parte del problema y obtener una visión más amplia de las necesidades y de los requerimientos del usuario. Se realizó una simulación del proceso total de evaluación y además, se obtuvo la bitácora de la última evaluación que realizó la oficina en setiembre de 2004, de la cual se pudieron obtener tanto los tiempos de ejecución como la metodología empleada. En ambas evaluaciones se analizaron los siguientes procesos:

1. Envío de cuestionarios
2. Llenado de cuestionarios
3. Recibo de cuestionarios
4. Consolidación y revisión de respuestas
5. Calificación y generación de resultados
6. Generación de reportes

Además, se utilizó la *Encuesta* como instrumento de recolección de datos. Con el fin de determinar el grado de conocimiento de los usuarios respecto del modelo de evaluación del Control Interno del Área de Tecnología de Información del Banco de Costa Rica, se aplicó la encuesta #1 (véase sección de Anexos) que utiliza como herramienta de medición la escala Likert, en la cual se analizaron aspectos tales como las áreas por evaluar, enfoques de la evaluación, metodología de calificación, entre otros.

Se utilizó la siguiente escala: 5 corresponde a Muy bueno, 4 corresponde a Bueno, 3 corresponde a Regular, 2 corresponde a Malo y 1 corresponde a Muy malo.

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Mediante la aplicación del instrumento de recolección de datos O*bservación Participante* durante el proceso de evaluación, se determinaron los siguientes resultados:

Actualmente, las 6 tareas o procesos que componen la evaluación, se ejecutan manualmente, exceptuando el envío y recibo de cuestionarios, debido a que ambas tareas se realizan por medio de correo electrónico, por lo que el tiempo que toma efectuar estas tareas depende directamente de la calidad y velocidad de la red interna del Banco. La Institución cuenta con su red debidamente certificada bajo los lineamientos o estándares establecidos internacionalmente, por lo que se pudo comprobar que las tareas de envío y recibo se realizan en unos pocos segundos, lo cual, prácticamente no influye en los tiempos totales de evaluación. Sin embargo, el proceso de generación del correo sí se realiza manualmente.

Respecto del tiempo de llenado del cuestionario, por parte de los gerentes o encargados de las distintas oficinas que conforman la División de Tecnología, este es muy variable, ya que depende de la prioridad que le den estas personas. Sin embargo, la Oficina de Riesgo y Control Interno establece un plazo máximo de entrega de respuestas de aproximadamente 12 días hábiles. El promedio del tiempo de llenado es de alrededor de 10,5 días. El tiempo mínimo que se registró fue de 7 días hábiles y el máximo fue de 15 días hábiles, inclusive superando el plazo establecido por la oficina. Cabe recalcar, que por este motivo, la oficina asigna 2 días más de gracia (15), con el propósito de que todos los funcionarios evaluados puedan remitir sus repuestas a tiempo y la oficina pueda cumplir con los tiempos establecidos por la Administración.

También se determinó que, el proceso que más tiempo le toma a esta oficina es el correspondiente a la tabulación o consolidación de datos y su respectiva verificación, ya que debe consolidar un promedio de 250 respuestas por cada oficina evaluada, las cuales, suman un total de 12 oficinas. Esta consolidación se realiza en un promedio de 15 a 20 días hábiles.

El proceso de calificación no se torna tan tedioso como el anterior, debido a que una vez obtenido los resultados preliminares de la tabulación, se aplican ciertas fórmulas matemáticas que determinan el grado de cumplimiento del Control Interno del Área de Tecnología de Información. Una vez aplicadas estas fórmulas, se genera un detalle de los resultados obtenidos. Este proceso se realiza en un tiempo de 1 día.

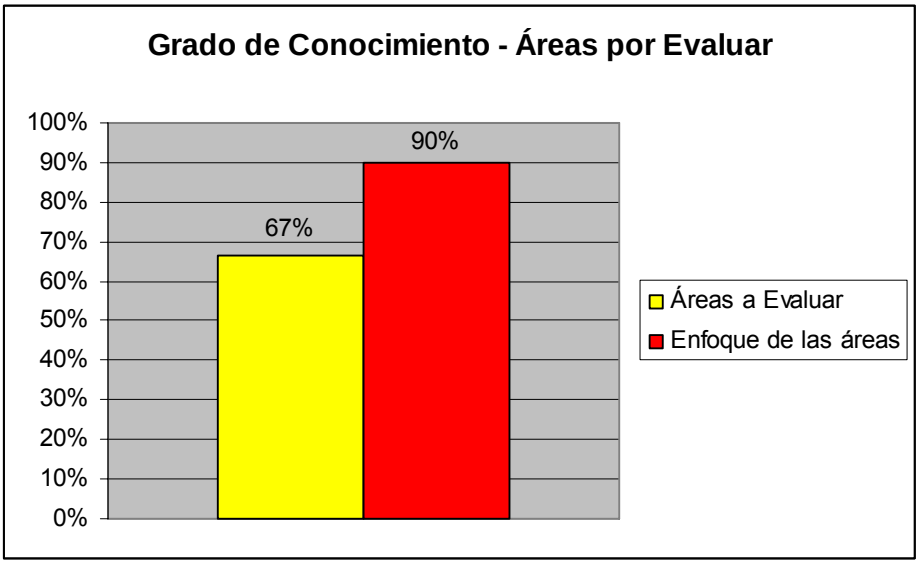
Por último, se evaluó el proceso de generación de reportes, el cual es un poco más complicado, ya que se deben generar reportes específicos por áreas evaluadas, por oficina, reportes generales, etc. Esta es una de las tareas en las que más tiempo consume el usuario, un promedio de 7 días hábiles, ya que al no generarse los reportes automáticamente, debe elaborarlos y rediseñarlos manualmente, según la necesidad.

Se debe tomar en cuenta que los usuarios participantes en el proceso de evaluación deben cumplir con otras tareas asignadas por la Jefatura, por lo que no pueden dedicarse a tiempo completo a cumplir con el desarrollo de la evaluación. Es decir, los funcionarios realizan esta evaluación en paralelo con el resto de sus tareas asignadas.

Como resultado de la aplicación de la *Encuesta #1* (véase sección de Anexos) como instrumento de recolección de datos y utilizando su misma escala, se determinaron los siguientes resultados:

Como se muestra en la Figura #1, el personal de la oficina de Riesgo y Control Interno, en general, tiene un conocimiento *Regular (67%)* respecto de las áreas por evaluar. Sin embargo, posee un grado de conocimiento *Muy Bueno (90%)* en lo que se refiere al enfoque de cada una de éstas. Esto debido a que no conocen "de memoria" las áreas por evaluar, pero una vez identificadas, pueden determinar su enfoque.

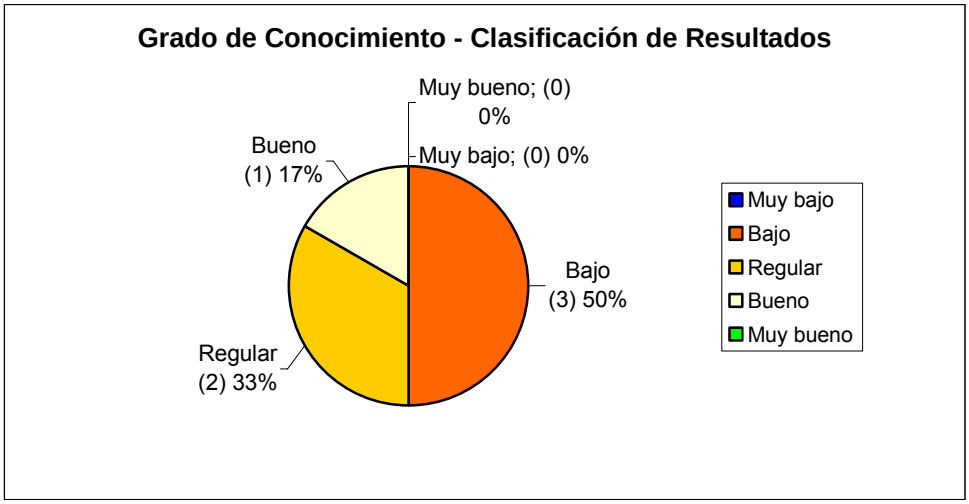
Figura #1



Fuente: Encuesta #1 - Anexos

En la Figura #2 se puede apreciar el grado de conocimiento del usuario respecto de la metodología de clasificación de resultados, donde un 50% de la población, que representa un total de 3 personas, considera que posee un conocimiento *Bajo*, un 33%, 2 personas, lo considera *Regular* y un 17%, es decir una persona, lo considera *Bueno*:

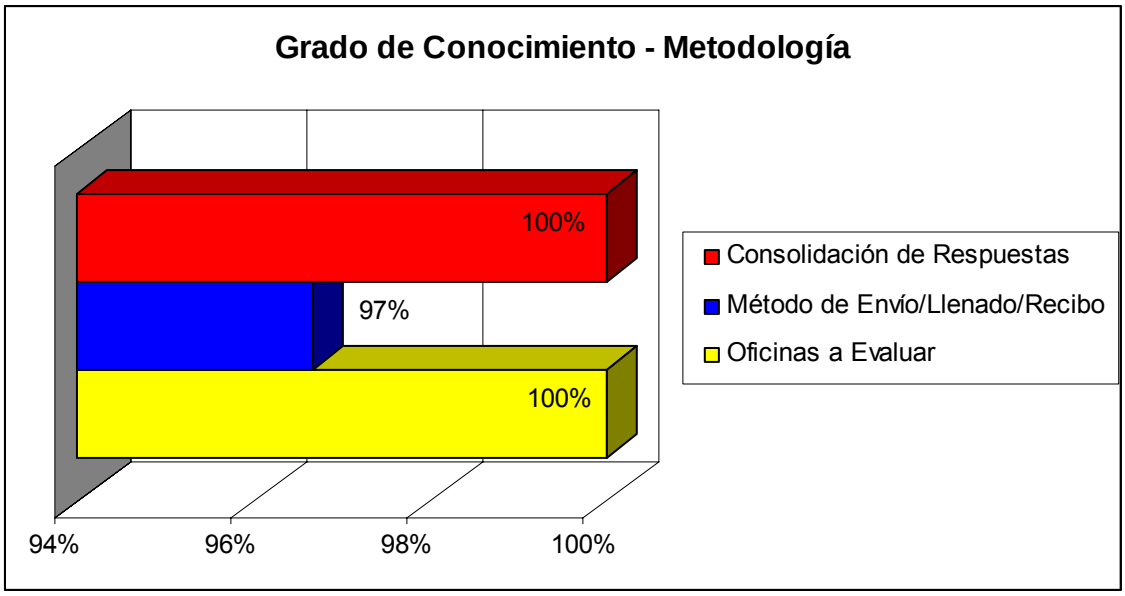
Figura #2



Fuente: Encuesta #1 - Anexos

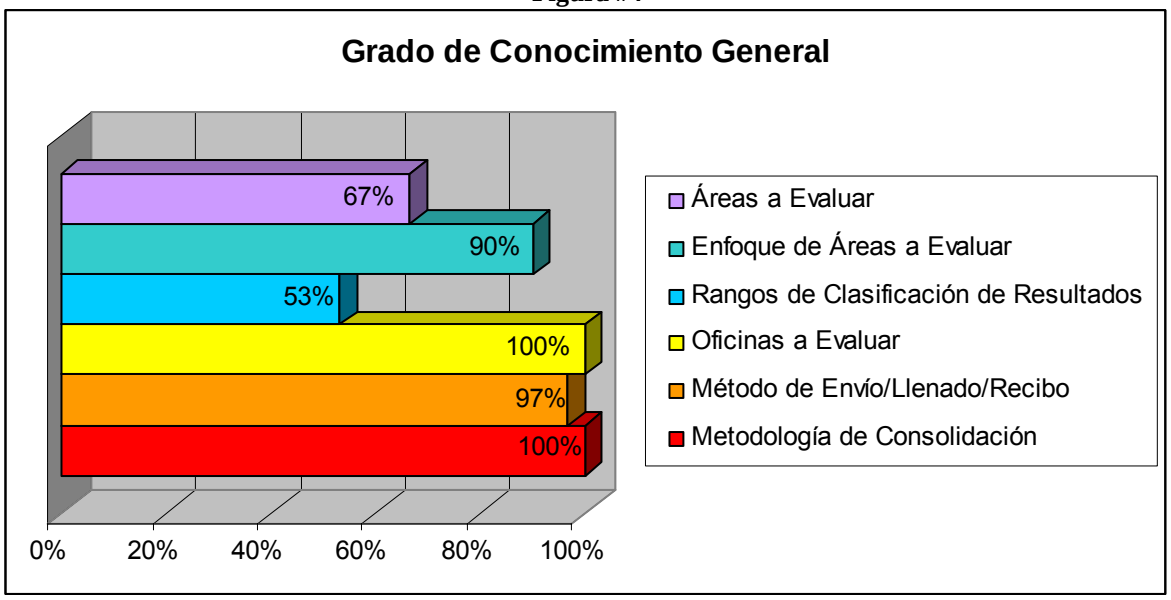
De la Figura #3 se infiere que el grado de conocimiento concerniente a las oficinas a evaluar, metodología de envío/llenado/recibo y consolidación de las distintas respuestas, es un nivel muy alto y satisfactorio, lo que demuestra un amplio dominio del tema por parte del usuario. Esto debido a que esta metodología se utiliza en otras evaluaciones que lleva a cabo esta oficina.

Figura #3



Como se aprecia en la Figura #4, en general, los funcionarios del área de Control Interno de la Oficina de Riesgo y Control Interno, poseen un grado de conocimiento relativamente bueno respecto de la metodología que utiliza el modelo de evaluación del control interno.

Figura #4

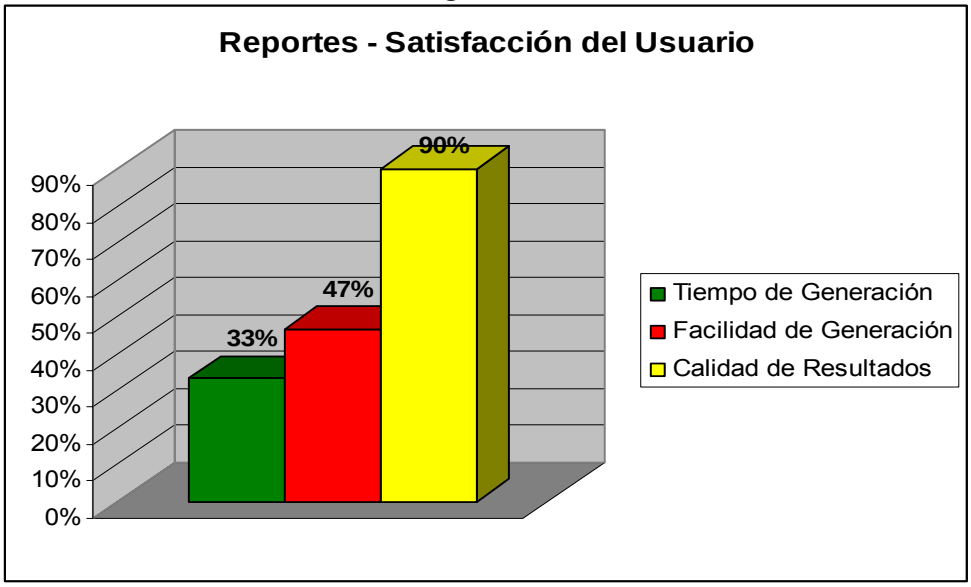


Fuente: Encuesta #1 - Anexos

Sin embargo, a pesar de este buen nivel de conocimiento, se evidenció que su grado de satisfacción respecto de la metodología actualmente empleada es muy deficiente. Esto, mediante la evaluación de aspectos importantes que conforman una gran parte del modelo de evaluación, donde los usuarios concentran una mayor cantidad de esfuerzo y tiempo, tales como la generación de reportes, la tabulación de respuestas, etc.

Como se puede determinar de la Figura #5, el usuario demuestra poca satisfacción (47%) respecto del procedimiento actual o pasos por seguir durante el proceso de generación de reportes, una vez finalizada la consolidación de datos o respuestas. Sin embargo, considera que los resultados o calidad de estos (90%), sí cumple con sus expectativas:

Figura #5

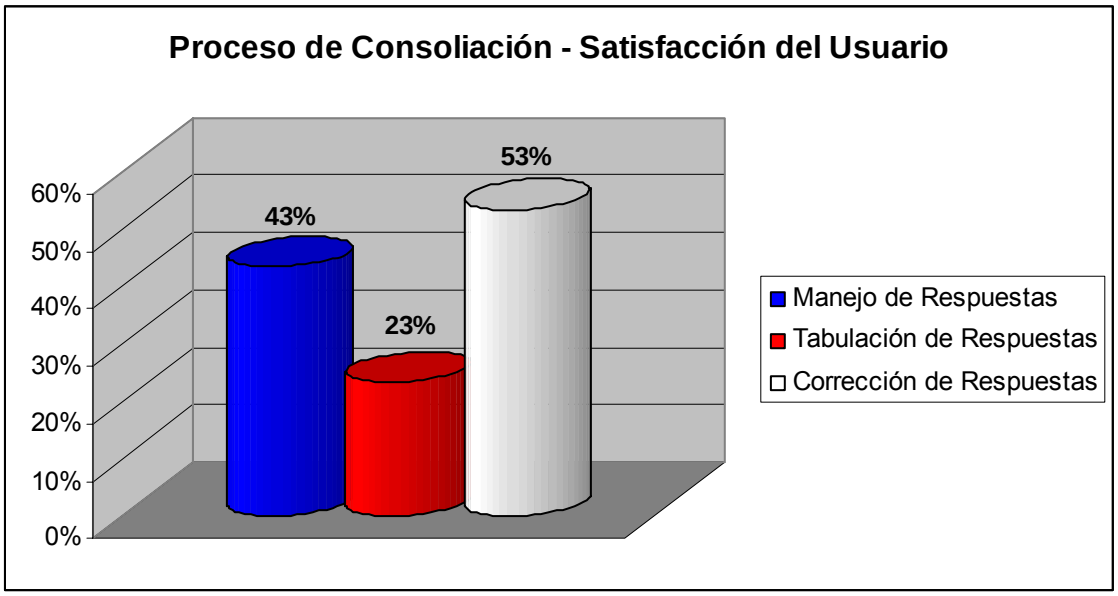


Fuente: Encuesta #1 - Anexos

Además, se puede concluir de la Figura #5 que a pesar de que el tiempo de generación y la facilidad de generación de los reportes (33%) no son muy satisfactorios, la calidad de los resultados sí (90%). Es decir, la calidad de los reportes no se ve afectada por la metodología de aplicación.

Como se mencionó anteriormente, el proceso de consolidación o tabulación de respuestas es el más tedioso debido al alto consumo de tiempo que requiere. Como se muestra en la Figura #6, el usuario se siente muy poco satisfecho con la ejecución manual de esta tarea y califica sus distintas funciones como *Bajo* y *Muy Bajo*.

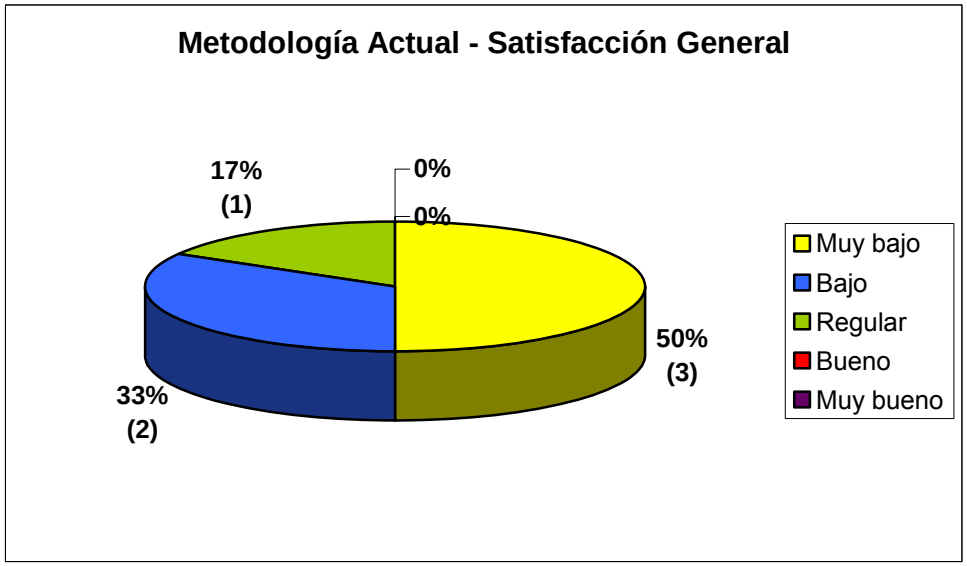
Figura #6



Fuente: Encuesta #1 - Anexos

En general, los usuarios demuestran un nivel muy bajo de aceptación o de satisfacción respecto de le metodología empleada actualmente. Así se demuestra en la Figura #7, donde un 17% de la población, correspondiente a 1 persona, opina que su grado de satisfacción respecto de la metodología empleada actualmente es *Regular*, un 33%, que corresponde a un total de 2 personas, opina que es *Bajo* y un 50%, correspondiente a 3 personas, opina que es *Muy Bajo*.

Figura #7



Fuente: Encuesta #1 - Anexos

CONCLUSIONES

Una vez concluida la investigación, se determinaron las siguientes situaciones:

1) Para completar el proceso de evaluación eficazmente se ejecutan 6 tareas distintas (1-Envío de cuestionarios, 2-Llenado de cuestionarios, 3-Recibo de cuestionarios, 4-Consolidación y revisión de respuestas, 5-Calificación y generación de resultados y 6-Generación de reportes), las cuales actualmente se realizan de forma manual. 5 de las 6 tareas pueden llegar a automatizarse, exceptuando el Llenado de cuestionarios, debido a que depende directamente de la interacción con un tercero (usuario pasivo).

2) La satisfacción del usuario respecto de la metodología manual de evaluación empleada actualmente es sumamente baja. Se demuestra gran disconformidad, debido a que tanto el manejo como el proceso de la información, consumen gran cantidad de recursos innecesarios.

3) Los funcionarios de la Oficina de Riesgo y Control Interno que emplean esta metodología poseen un grado de conocimiento aceptable, respecto de la metodología de evaluación, debido a que deben conocer exactamente como funciona el proceso con el fin de poder aplicarlo como es requerido. Sin embargo, estos pueden llegar a cometer errores que alteren la exactitud y confiabilidad de los resultados obtenidos. Con la implementación de un sistema automatizado, prácticamente se elimina este riesgo, ya que el usuario no debe aplicar directamente la metodología.

4) Al automatizar el proceso total de evaluación, no va a ser necesario un conocimiento tan amplio y particular de las distintas tareas o procesos utilizados por la metodología actual, ya que un sistema automatizado de información la emplearía

internamente y el usuario no debe conocerla en un 100%. El usuario se puede concentrar en el avance de otras tareas y no en la metodología empleada.

5) El proceso de generación de reportes es sumamente lento y complicado, ya que requiere mucho tiempo de preparación y se deben generar manualmente. Esta situación provoca que los usuarios reflejen un bajo grado de satisfacción respecto de dicho proceso de generación; estimulando una gran necesidad de automatización que mejore su eficiencia.

6) El proceso de generación de reportes es muy lento y tedioso, no obstante, éste no afecta la calidad de la información presentada en los reportes.

7) El proceso más importante y que más consume recursos es el de consolidación de respuestas. Lamentablemente, en la actualidad se debe realizar manualmente y es el proceso que provoca mayores contratiempos, debido a su gran complejidad. De este proceso nace la mayor necesidad de automatización.

8) A pesar de que el tiempo de calificación es relativamente corto, éste se puede llegar a automatizar y simplificarlo a prácticamente centésimas de segundo, situación que minimizaría notoriamente el tiempo total de evaluación.

PROPUESTA

Con el fin de subsanar las deficiencias determinadas anteriormente, se recomienda implementar un Sistema Automatizado de evaluación del sistema de control interno para el área de tecnología de información del Banco de Costa Rica. Dicho sistema debe cumplir con los requerimientos que se presentan a continuación:

Requerimientos:

Los requerimientos funcionales para el sistema se listaron una vez finalizada la investigación y analizada la metodología que utiliza el modelo de evaluación. A continuación se presenta la lista general de dichos requerimientos:

El Sistema debe ser capaz de:

1. Agregar, modificar y eliminar distintas instancias del cuestionario.

2. El software deberá utilizar todos los niveles de la estructura organizacional del Banco, para que se pueda llegar a clasificar resultados por gerencia, área o división.

3. Tabulación de datos. Durante la evaluación, el sistema debe permitir la creación de "n" instancias del mismo cuestionario, de tal forma, que permita recolectar, agrupar y tabular los distintos datos de una misma evaluación.

4. El sistema deberá contar para cada medida de control evaluada, con un campo de tipo C*aracter* para indicar un plan de acción.

5. Para cada medida, el sistema debe contar con dos campos de tipo *Fecha*, donde el usuario indique la fecha de inicio y la fecha de vencimiento del plan de acción.

6. Para cada medida, el sistema debe contar con un campo *Responsable*, donde el usuario indique cual (es) persona(s) es (son) responsable(s) de llevar a cabo el plan de acción.

7. Para cada medida, el sistema debe contar con un campo *Referencia*, donde se indique a cual documento y artículo de la *Normativa Institucional* hace referencia la medida.

8. El sistema deberá trabajar con el los siguientes parámetros de calificación:
    - Cumple (C)
    - Cumplimiento Parcial Alto (CPA)
    - Cumplimiento Parcial Bajo (CPB)
    - No Cumple (NC)
    - No Aplica (N/A)

9. Cada uno de las parámetros de calificación anteriores, debe representar un ponderador o un peso parametrizable para efectos de calificación. Por ejemplo, Cumplimiento Parcial Alto debe tener un valor de 70 ó 75% y Cumplimiento Parcial Bajo un valor de 35 ó 40%.

10. Para cada una de las medidas a evaluar en los diferentes cuestionarios, el sistema debe permitir asignar, mediante la selección de una lista de riesgos, el tipo de riesgo al cual pertenece cada medida evaluada.

11. Para cada uno de los controles a evaluar en los diferentes cuestionarios que se indican, el sistema debe permitir asignar, mediante la selección de una lista de procesos, el tipo de proceso al cual pertenece cada medida evaluada.

12. Medidas activas e inactivas. Para cada nueva instancia del cuestionario, el sistema debe permitir seleccionar o activar las medidas que se desean aplicar.

13. El rango de clasificación de resultados debe ser parametrizable.

14. La estructura del cuestionario debe ser la siguiente:

    - Cuestionario
      - Factor
        - Objetivo
          - Medida

15. Cada factor o sub-división debe estar compuesto por “n” cantidad de objetivos.

16. Cada objetivo debe estar compuesto por “n” cantidad de medidas.

17. El sistema debe permitir 1-Agregar, 2-Eliminar y 3-Modificar, tanto los factores como los objetivos y las medidas.

18. El sistema debe aplicar la metodología de calificación indicada en el Artículo 5, de la sección II de la *Normativa de Tecnología de Información Para las Entidades Fiscalizadas por la SUGEF*.

19. Cada Medida, así como cada Objetivo y cada Factor deben de representar un ponderador o un peso parametrizable. Es decir, a cada Medida, a cada Objetivo y a cada Factor se le debe asignar un peso que permita establecer una mayor objetividad de evaluación.

20. El sistema a diseñar debe ser una aplicación web que pueda ser accedida desde la Intranet del Banco.

21. Debe ser totalmente parametrizable, de forma que los usuarios puedan administrar sus datos sin tener que recurrir a labores de programación.

22. El sistema debe ser amigable al usuario, de tal forma que la navegación a través de sus diferentes pantallas sea fácil y sencilla, estandarizando para ello las teclas de función.

23. El sistema debe cumplir con las *Disposiciones para la Administración y Desarrollo de Proyectos Informáticos del Banco de Costa Rica*. En este documento se especifican requerimientos de seguridad, bases de datos, conexiones, arquitectura, programación, etc., con los cuales debe cumplir todo sistema de información que se desee implementar en dicha Institución.

24. El sistema debe almacenar el historial de cada evaluación, de forma tal, que se puedan generar reportes históricos por oficina y por jefe.

25. Cuando la respuesta a una medida sea *Cumple,* el usuario debe llenar como requisito el campo *Evidencia*.

26. Cuando la respuesta a una medida sea *Parcial Alto, Parcial Bajo* o *No Cumple,* el usuario debe llenar como requisito el campo *Plan de Acción*.

Reportes

El sistema debe estar en capacidad de cumplir al menos con los siguientes requerimientos concernientes a los reportes generados por el sistema:

1. Todos los reportes generados por el sistema deben de contar con los siguientes campos:
    - Encabezado (1-BCR (imagen), 2-Oficina de Riesgo y Control Interno, 3-Cuestionario aplicado y 4-Nombre de Reporte).
    - Fecha de generación
    - Identificación del usuario que genera el reporte
    - Fecha de evaluación
    - Número de página de total de páginas (“Página 1 de 10”).

2. Todos los reportes deben contar con la opción de ser presentados tanto en pantalla como enviados a impresora. Además, deben contar con la opción de ser exportados a Microsoft Excel.

3. El sistema debe estar en capacidad de emitir al menos los siguientes reportes:

   3.1. Resultado General
      3.1.1. Medidas evaluadas, medidas incumplidas y calificación obtenida, con espacio para que tanto el jefe de oficina como un funcionario de la Oficina de Riesgo y Control Interno firmen el documento.

   3.2. Resultado por Factor
      3.2.1. Detalle de resultado de evaluación de cada Factor evaluado.

   3.3. Resultado por Objetivo
      3.3.1. Detalle de resultado de evaluación de cada Objetivo evaluado, agrupado por Factor.

   3.4. Resultado por Medida
      3.4.1. Detalle de resultado de evaluación de cada Medida evaluada, agrupado por Objetivos y este a su vez por Factor. (Cuestionario completo)

   3.5. Debilidades identificadas
      3.5.1. Detalle de Medidas incumplidas, agrupadas por Objetivo y a su vez por Factor.

   3.6. Plan de Acción
      3.6.1. Detalle del Plan de Acción, Responsable y Fecha para cada Medida incumplida, agrupado por Objetivo y a su vez por Factor.

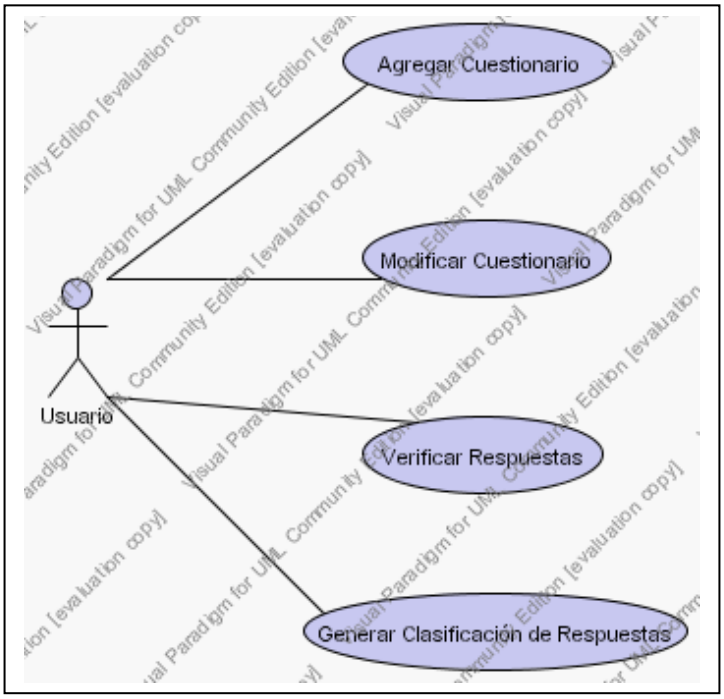
   3.7. Histórico por Oficina:
      3.7.1. Detalle de las calificaciones obtenidas, medidas evaluadas y medidas incumplidas de una oficina determinada.

   3.8. Histórico por Jefe:
      3.8.1. Detalle de las calificaciones obtenidas, medidas evaluadas y medidas incumplidas de las oficinas que han estado bajo responsabilidad de un determinado jefe.

Diagramas (Visión General):

Diagrama de Casos de Uso

El diagrama de casos de uso describe las principales actividades o procesos a realizar y su respectiva relación con los actores o participantes de éstos. A continuación se presenta el diagrama de casos de uso en un nivel general:

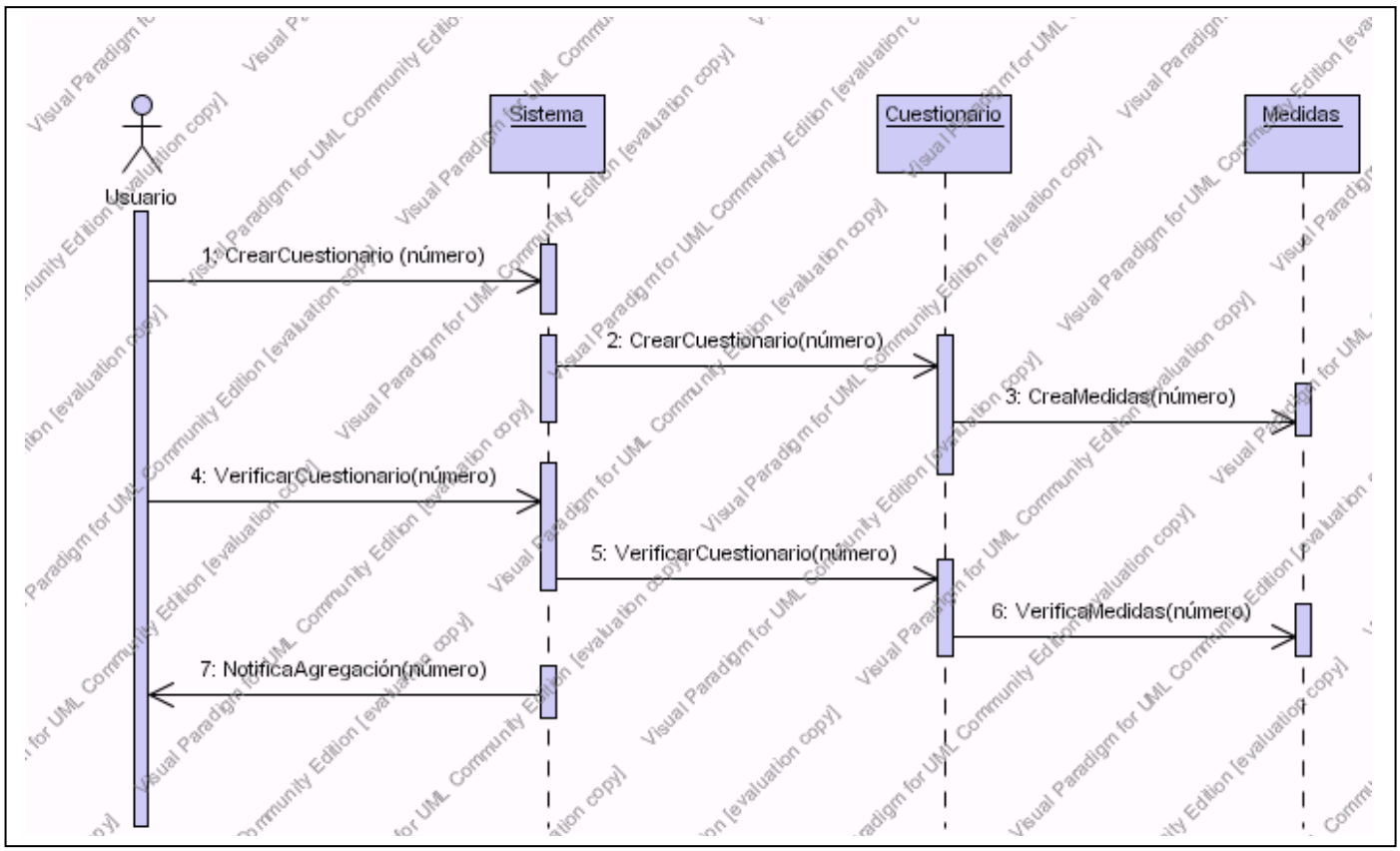


Fuente: Elaboración propia

Casos de Uso Expandidos:

1.1 Agregar o Publicar Cuestionario

1.1.1 Diagrama de Secuencia:

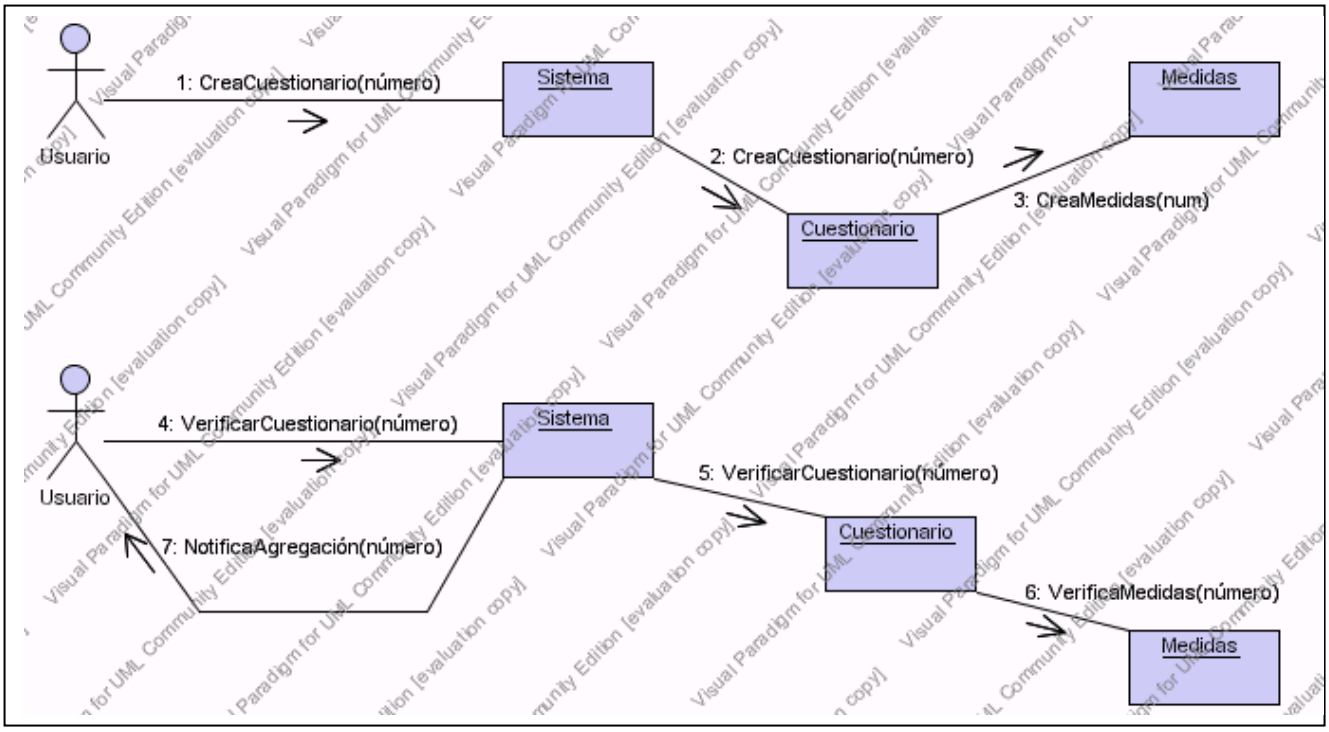


Fuente: Elaboración propia

En el diagrama anterior se muestra la secuencia de acciones o tareas que se deben realizar durante la *Publicación del Cuestionario.*

1.1 Agregar o Publicar Cuestionario

1.1.2 Diagramas de Colaboración:

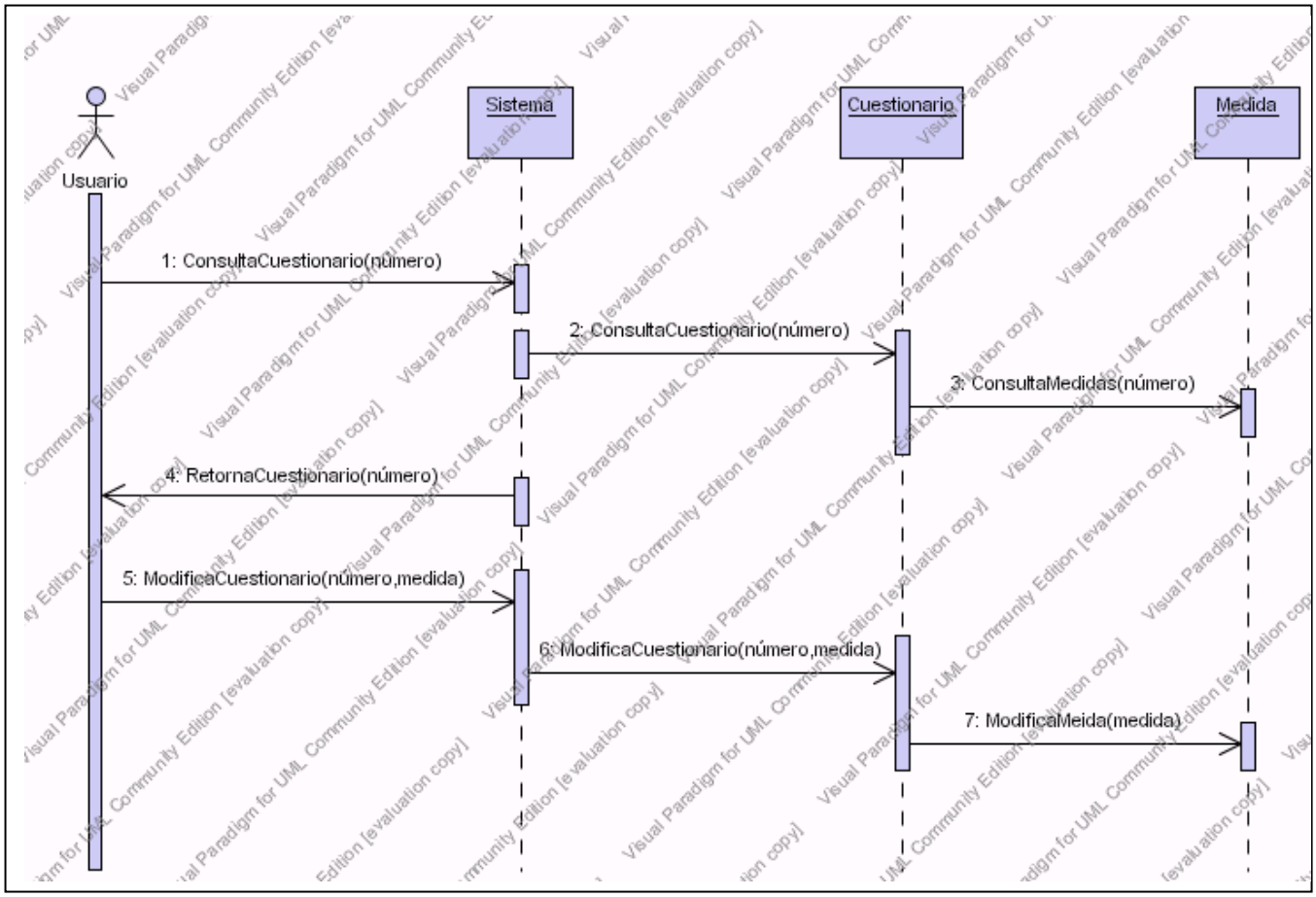


Fuente: Elaboración propia

En el diagrama anterior se presenta la colaboración existente entre los objetos que participan en el proceso de *Publicación del Cuestionario.*

1.2 Modificar Cuestionario

1.2.1 Diagrama de Secuencia:

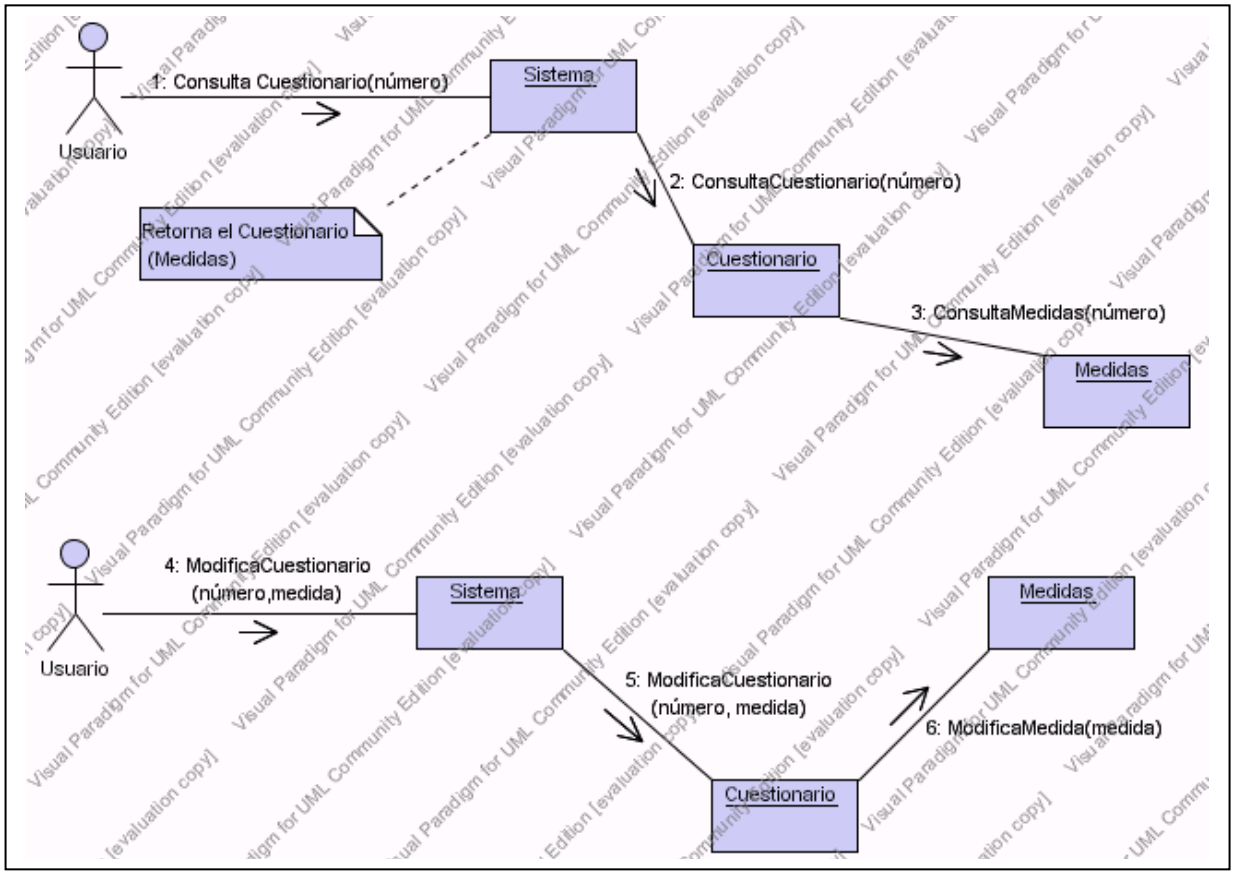


Fuente: Elaboración propia

En el diagrama anterior se muestra la secuencia de acciones o tareas que se deben realizar durante el proceso de *Modificación del Cuestionario.*

1.2 Modificar Cuestionario

1.2.2 Diagrama de Colaboración:

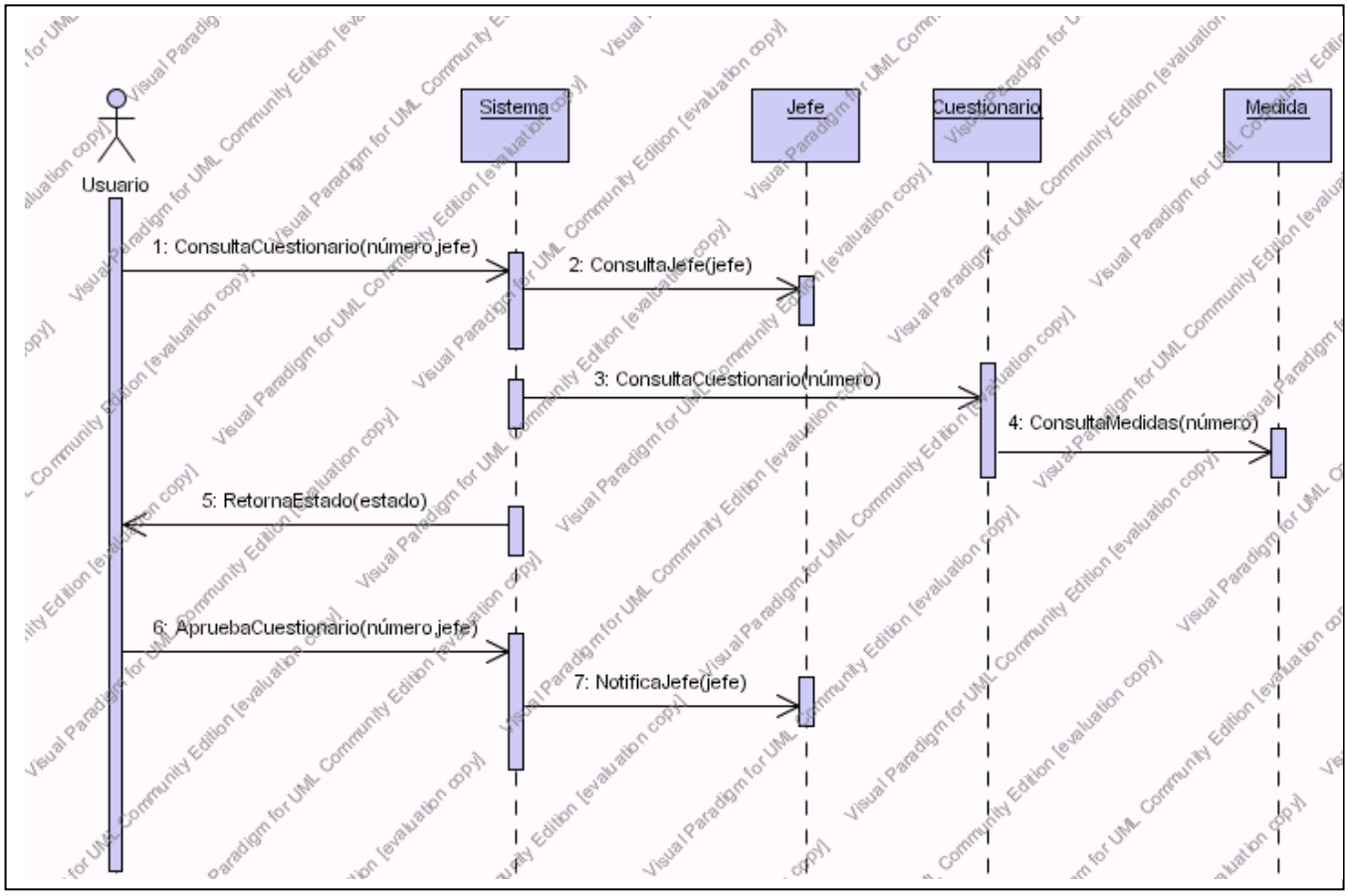


Fuente: Elaboración propia

En el diagrama anterior se aprecia la colaboración existente entre los objetos que participan en el proceso de *Modificación del Cuestionario*.

1.3 Verificar Respuestas

1.3.1 Diagrama de Secuencia:

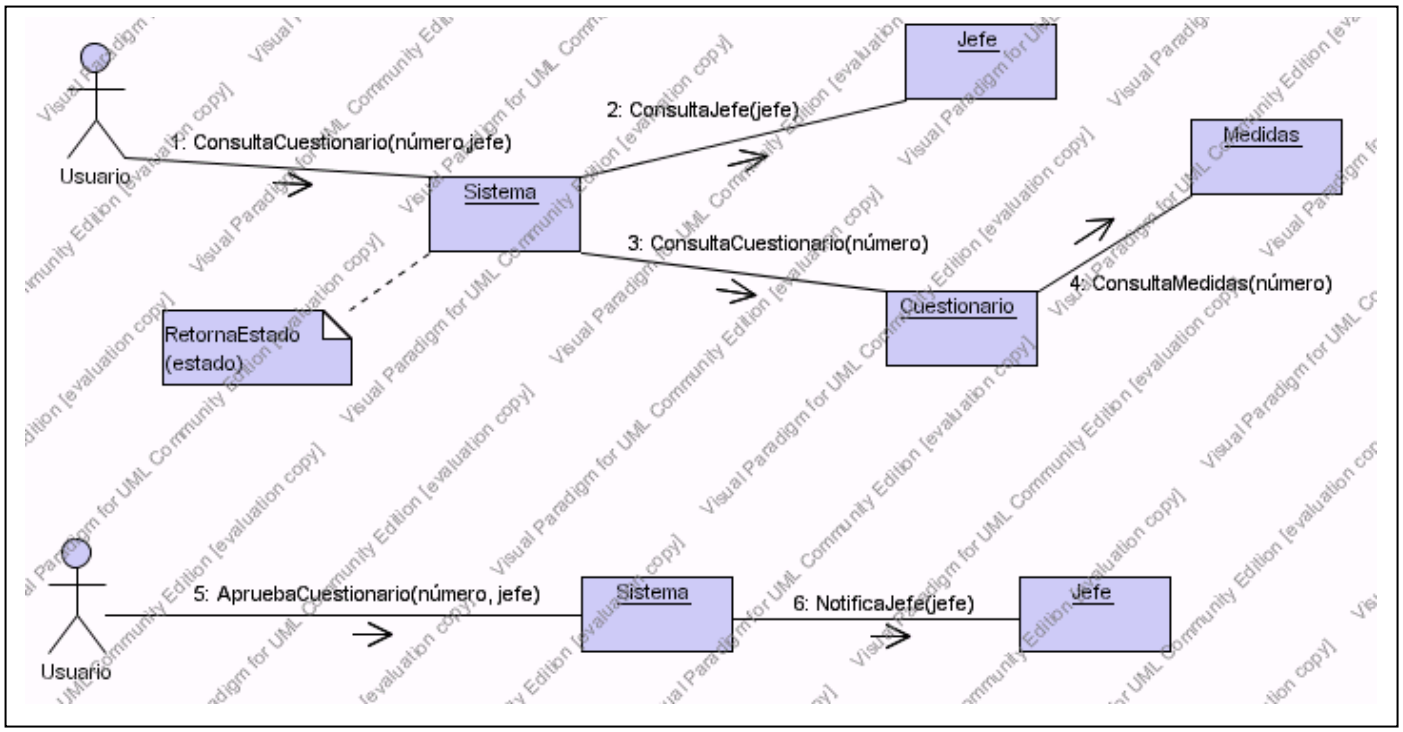


Fuente: Elaboración propia

En el diagrama anterior se muestra la secuencia de acciones o tareas que se deben realizar durante la *Verificación de Respuestas*.

1.3 Verificar Respuestas

1.3.2 Diagrama de Colaboración

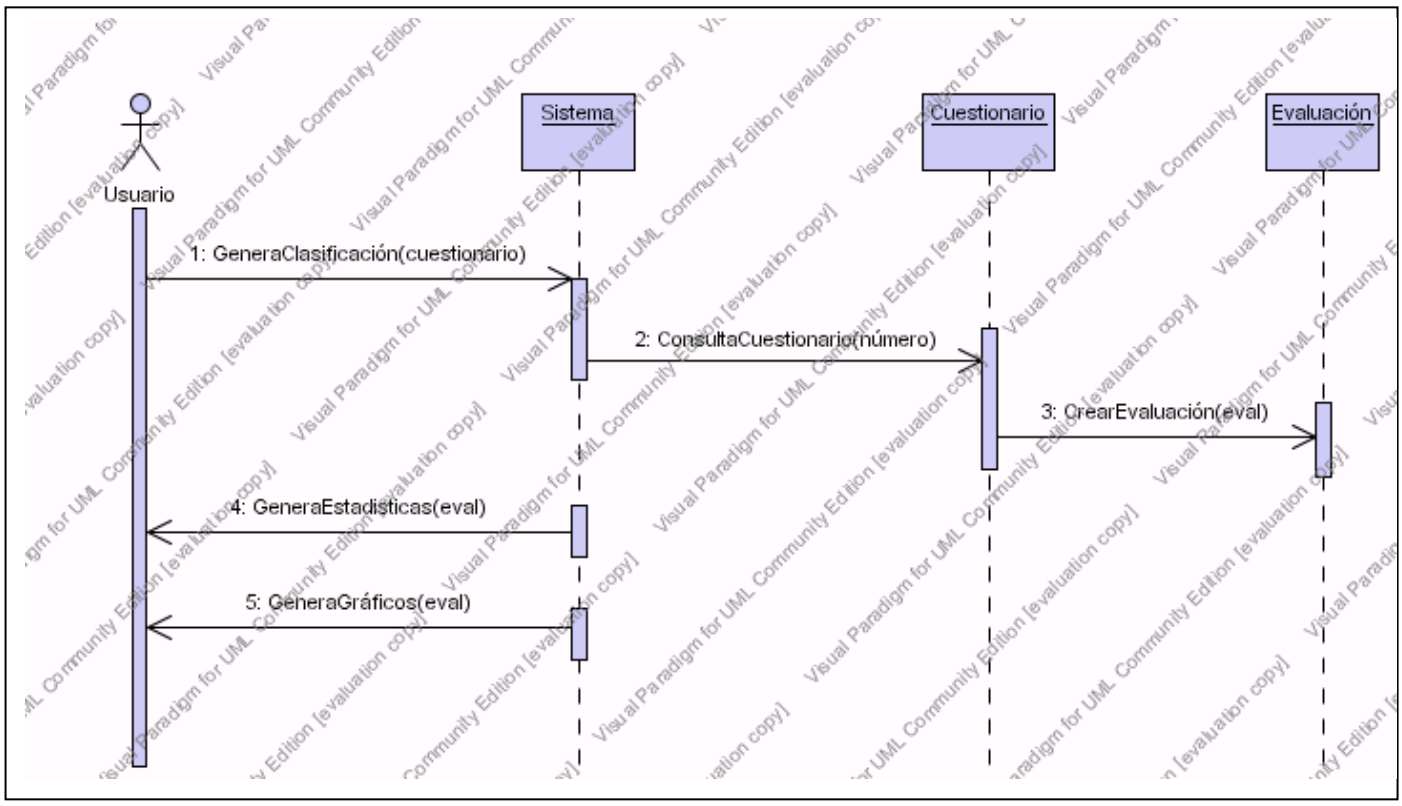


Fuente: Elaboración propia

En el diagrama anterior se aprecia la colaboración existente entre los objetos que participan en el proceso de *Verificación de Respuestas*.

1.4 Generar Clasificación de Respuestas

1.4.1 Diagrama de Secuencia

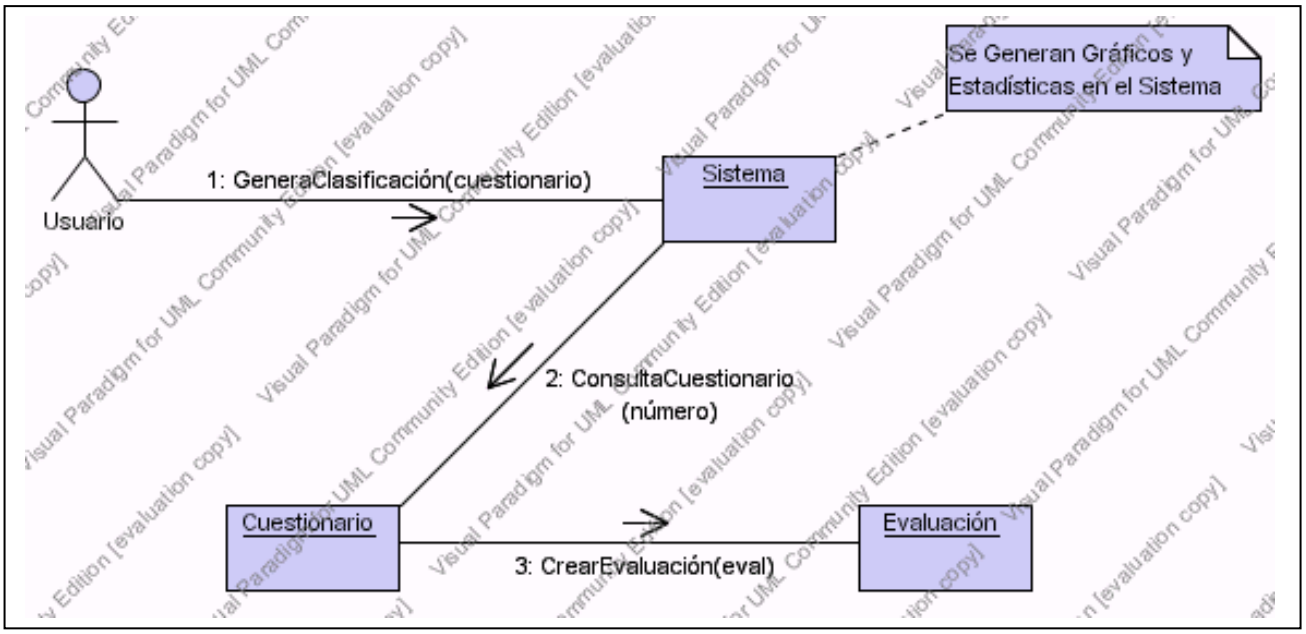


Fuente: Elaboración propia

En el diagrama anterior se muestra la secuencia de acciones o tareas que se deben realizar durante la *Generación de Clasificación de Respuestas.*

1.4 Generar Clasificación de Respuestas

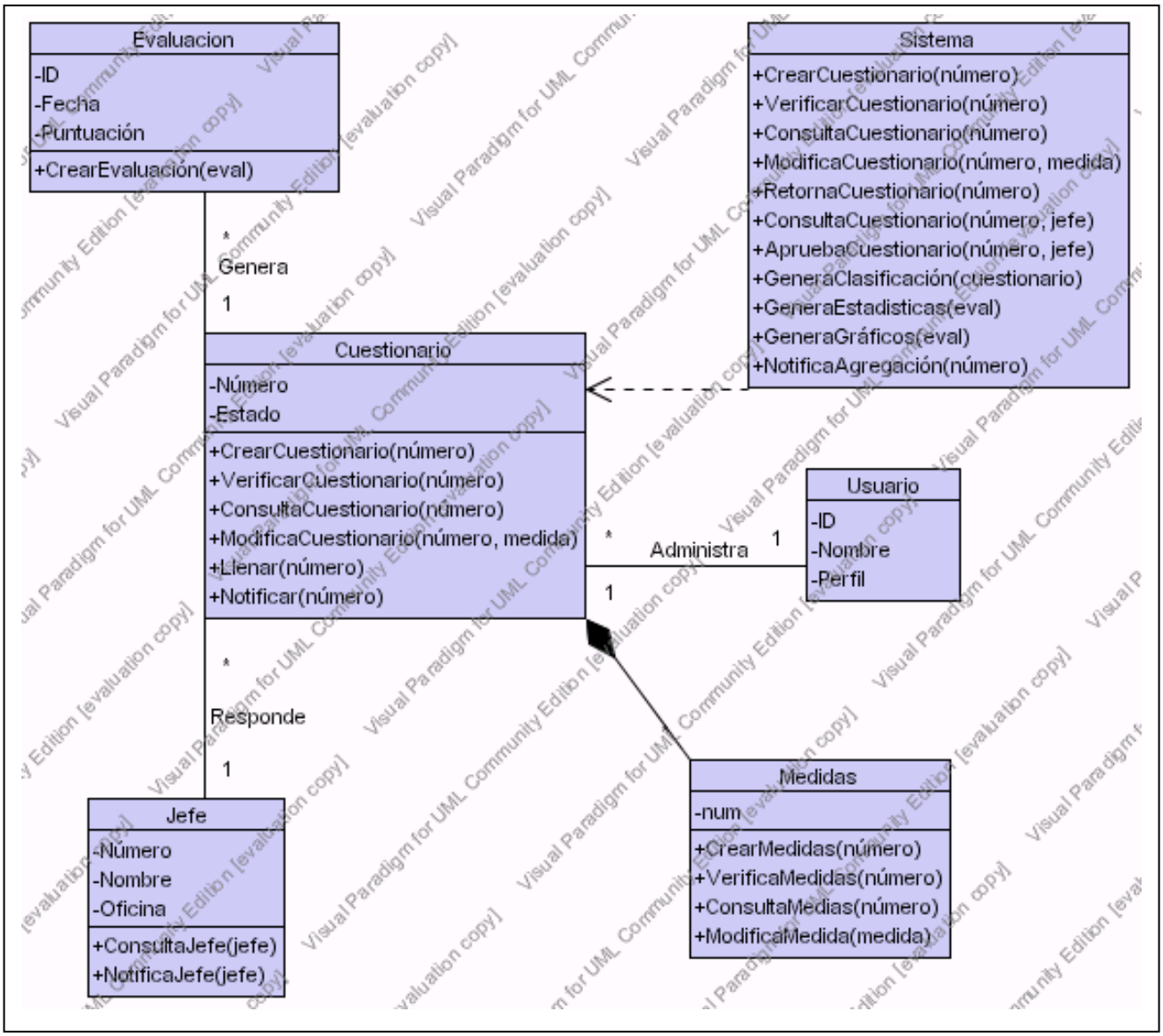
1.4.2 Diagrama de Colaboración



Fuente: Elaboración propia

En el diagrama anterior se aprecia la colaboración existente entre los objetos que participan en el proceso de *Generación de Clasificación de Respuestas.*

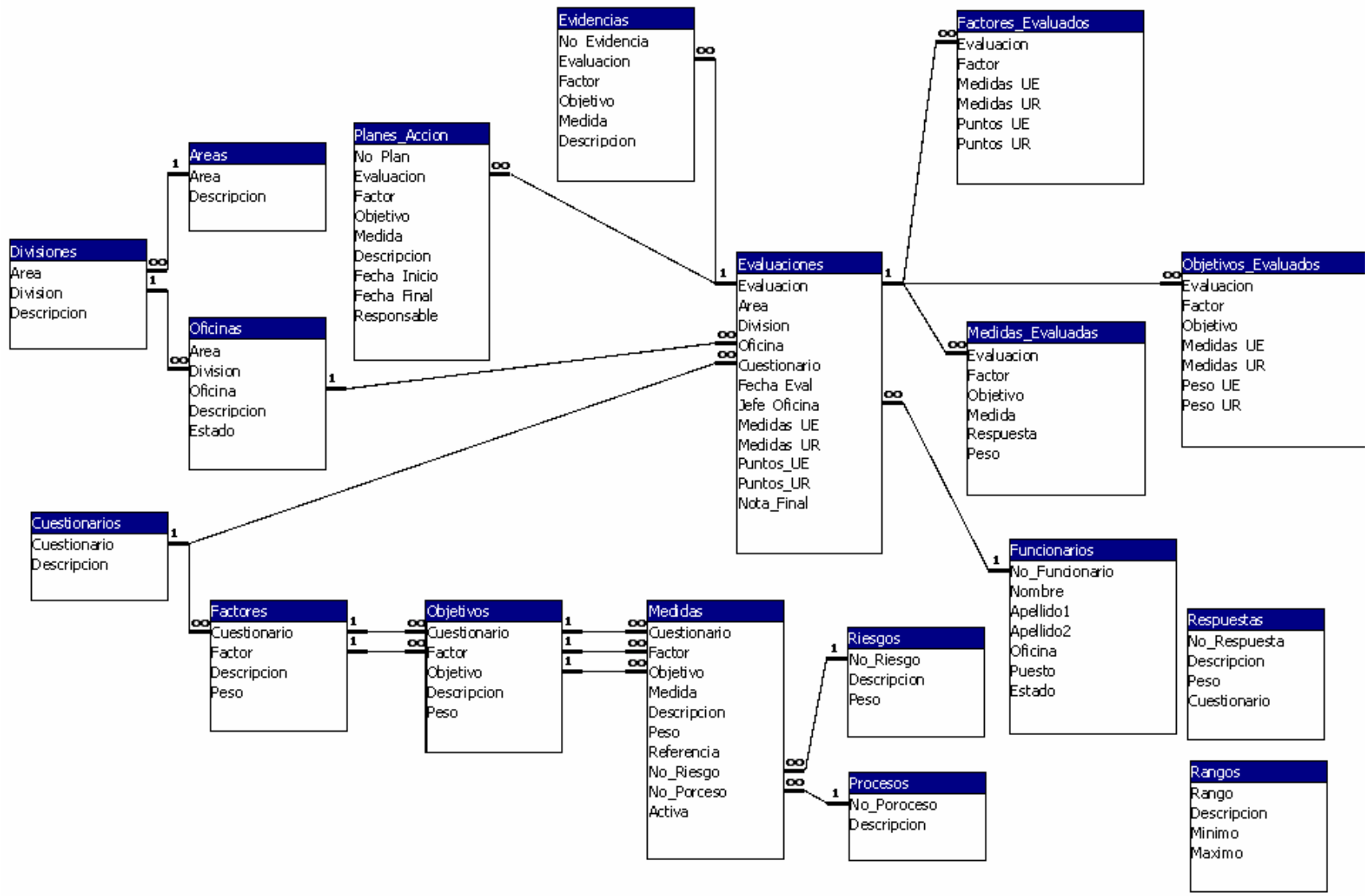
Diagrama de Clases



Fuente: Elaboración propia

El diagrama de clases muestra las relaciones entre las clases que involucra el sistema, según la estructura propuesta para su diseño.

DIAGRAMA ENTIDAD – RELACIÓN

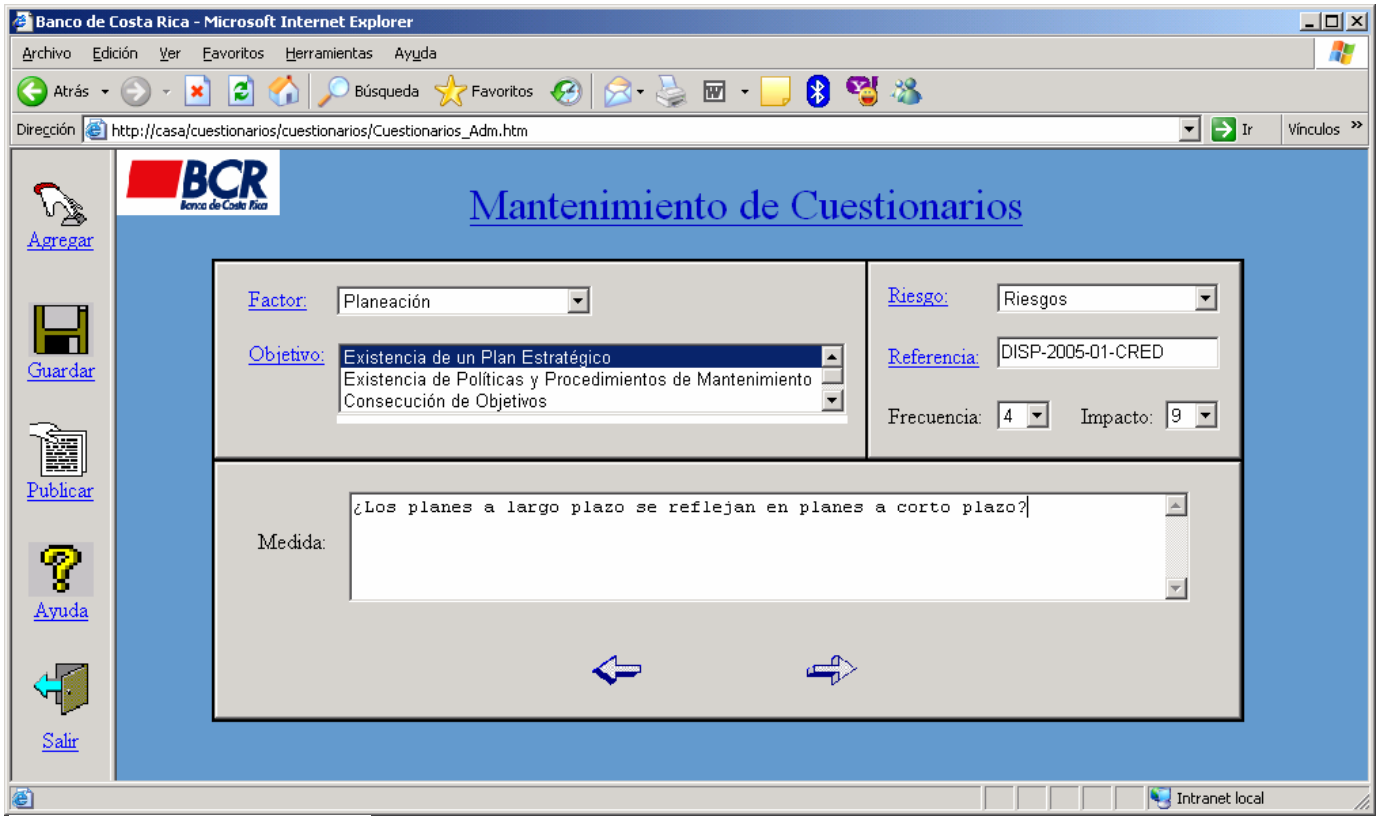


DEMO:

Uno de los objetivos de esta investigación es el desarrollar un pequeño *Demo* (aplicación de prueba) del sistema propuesto, que muestre una posible aplicación de la metodología investigada. Este *Demo* fue desarrollado con la herramienta Visual Basic .Net de Microsoft, debido a que es una de las herramientas de programación más poderosas y utilizadas del mercado actual, y que además permite desarrollar aplicaciones tanto para clientes Windows como servicios web avanzados, tales como páginas web, aplicaciones de interacción, aplicaciones XML, etc. A continuación se presenta la descripción gráfica de algunas pantallas principales de la aplicación:

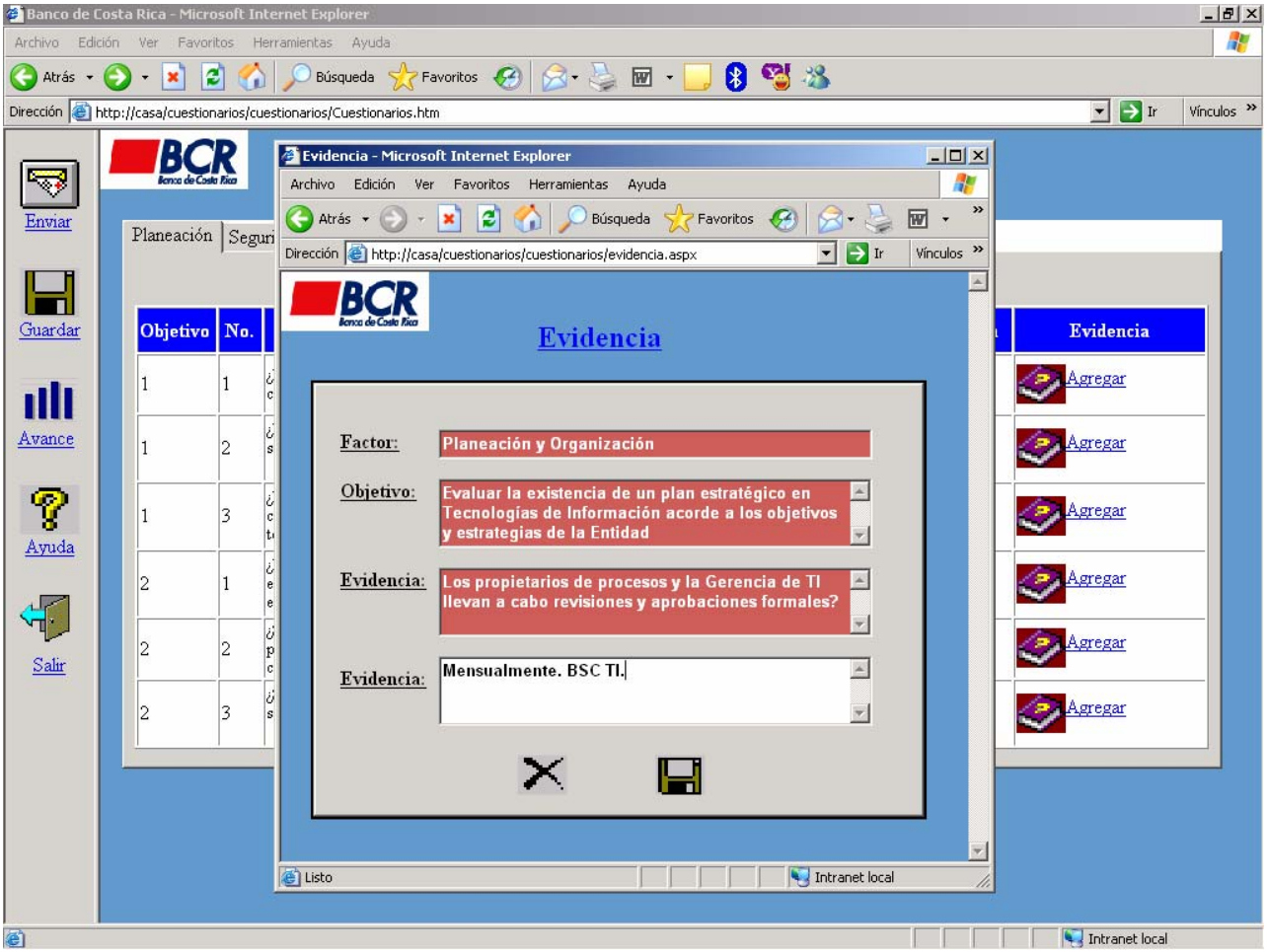
Fuente: Elaboración propia

La figura anterior corresponde a la pantalla principal de llenado o inclusión de respuestas del cuestionario, donde los encargados de las distintas oficinas por evaluar se autocalifican.



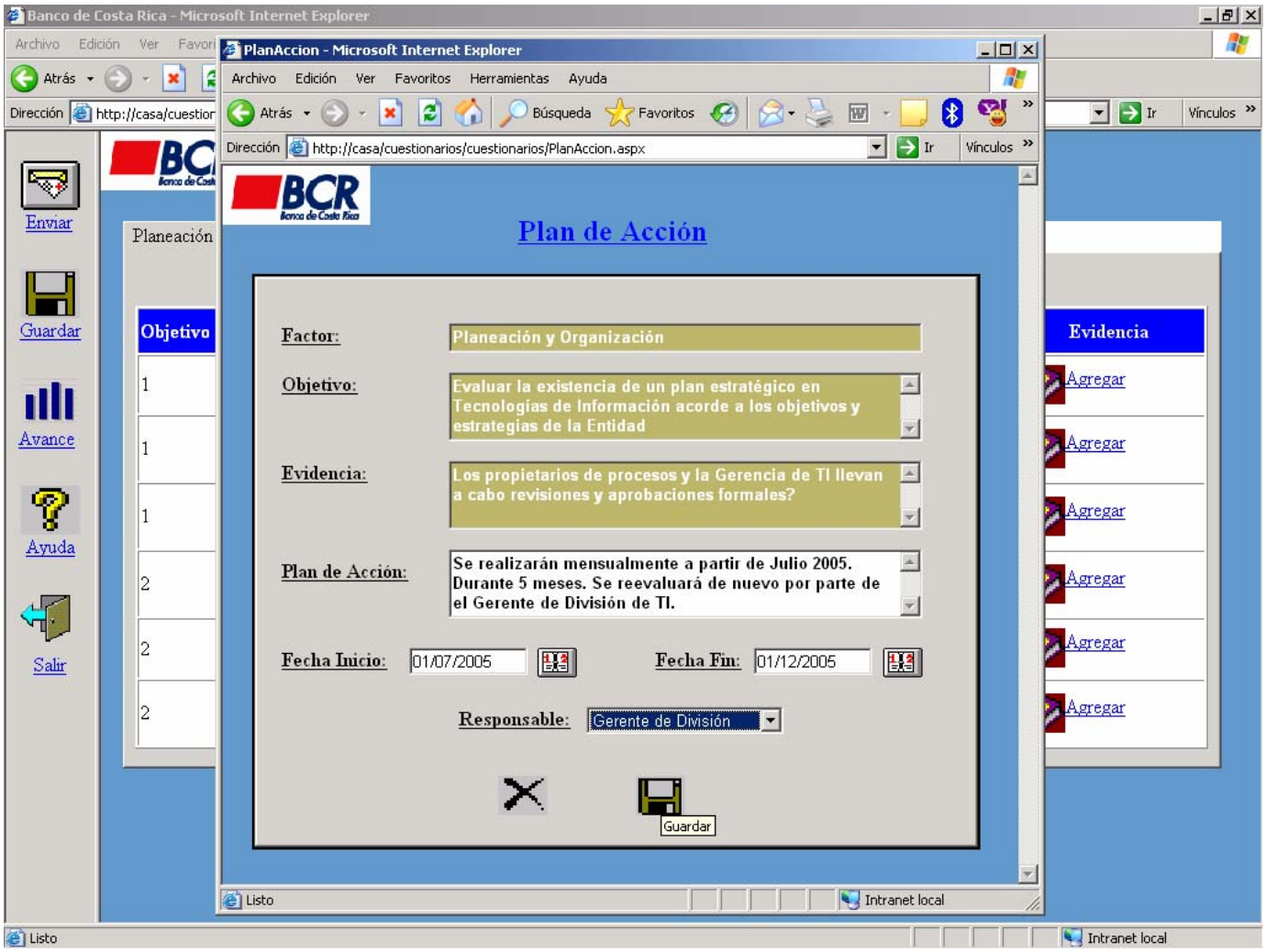
Fuente: Elaboración propia

La imagen anterior corresponde al mantenimiento de las medidas que deben de realizar los funcionarios de la Oficina de Riesgo y Control Interno del Banco de Costa Rica.



Fuente: Elaboración propia

La imagen anterior corresponde al campo *Evidencia* que se debe de almacenar para todas las medidas que así lo requieran.



Fuente: Elaboración propia

La imagen anterior corresponde al campo *Plan de Acción* que se debe de almacenar para al menos todas las medidas que su respuesta sea *Cumple Alto*, *Cumple Bajo* y *No Cumple*. Es opcional para la respuesta de tipo *Cumple.*

REFERENCIA BIBLIOGRÁFICA

Asamblea Legislativa de la República de Costa Rica (2002). *Ley General de Control Interno No. 8292*. San José: Autor.

Booch, G., Rumbaugh, J. y Jacobson, I. (1999). *El Lenguaje Unificado de Modelado*. Madrid: Addison Wesley Iberoamericana.

Booch, G., Rumbaugh, J. y Jacobson, I. (2000). *El Proceso Unificado de Desarrollo de Software*. Madrid: Pearson Educación, S.A.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2003). *Metodología de la Investigación*. México: Mc Graw Hill.

Microsoft Corporation. (2005). *Visual Basic Language Specification.* Recuperado el 28 de abril de 2005, de http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vbls7/html/vblrfvbspec1.asp

Object Management Group. (2005). *Unified Modeling Language*. Recuperado el 15 de abril de 2005, de http://www.uml.org/.

Riordan, R. M. (2002). *Aprenda Ya Microsoft ADO.NET*. España: Mc Graw Hill/Interamericana de España, S.A.

Soler, B. y Spotts, J. (2002). *Edición Especial Visual Basic.Net*. Madrid: Pearson Educación, S.A.

Superintendencia General de Entidades Financieras (2003). *Normativa de Tecnología de Información Para las Entidades Fiscalizadas por la SUGEF*. San José: Autor.

ANEXOS

Encuesta #1

1- Indique su grado de conocimiento respecto de los siguientes enunciados, donde 1- Muy bajo, 2- Bajo, 3- Regular, 4- Bueno y 5- Muy bueno:

a) Áreas que comprende la evaluación

1	2	3	4	5

b) Enfoque de cada una de las áreas de evaluación

1	2	3	4	5

c) Rangos de clasificación de resultados

1	2	3	4	5

d) Oficinas o gerencias a las que se aplica la evaluación

1	2	3	4	5

e) Método de envío/llenado/recibo de la evaluación

1	2	3	4	5

f) Método de consolidación de los resultados de la evaluación

1	2	3	4	5

2- Indique su grado de satisfacción respecto de los siguientes enunciados, donde 1- Muy bajo, 2- Bajo, 3- Regular, 4- Bueno y 5- Muy bueno:

a) Tiempo que toma generar reportes con base en los resultados obtenidos

1	2	3	4	5

b) Facilidad de generación de reportes

1	2	3	4	5

c) Calidad de los resultados obtenidos en los reportes

1	2	3	4	5

d) Manejo de las distintas respuestas enviadas por los gerentes de oficina

1	2	3	4	5

e) Proceso de tabulación de respuestas

1	2	3	4	5

f) Facilidad de corrección de respuestas y su re-tabulación

1	2	3	4	5

g) Grado de satisfacción general con la metodología empleada actualmente

1	2	3	4	5