UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NTP ISO 27001 Y 27002 Y COBIT

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE

INGENIERO DE COMPUTACIÓN Y SISTEMAS

ÁREA DE INVESTIGACIÓN: AUDITORÍA DE SISTEMAS DE INFORMACIÓN / E-GOVERNMENT

AUTORES: Br. ENCALA MALCA REINALDO ALBERTO

Br. QUISPE CHILCÓN JOSÉ HERNÁN

ASESOR: Ing. DÍAZ SANCHEZ JAIME EDUARDO

TRUJILLO - PERÚ, 2015

SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NTP ISO 27001 Y 27002 Y COBIT

Por: Br. Encalada Malca Reinaldo Alberto

Br. Quispe Chilcón José Hernán

Aprobado:

Dr. Lazo Aguirre Walter Aurelio _____

Presidente

Nº CIP: 36034

Ing. Abanto Cabrera Heber Gerson _____

Secretario

Nº CIP: 106421

Ms. Carranza Medina Percy Lucio _____

Vocal

Nº CIP: 149877

Asesor:

Ing. Díaz Sánchez Jaime Eduardo

Nº CIP: 73304

PRESENTACIÓN

Señores Miembros del Jurado

Cumpliendo con los requerimientos estipulados en el reglamento de Grados y Títulos de la "Universidad Privada Antenor Orrego" para optar el grado de Ingeniero de Computación y Sistemas, ponemos a vuestra disposición la presente tesis titulada: **SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NTP ISO 27001 Y 27002 Y COBIT.**

Gracias

Trujillo, 11 de mayo de 2015

Br. Encalada Malca, Reinaldo Alberto	Br. Quispe Chilcón, José Hernán

DEDICATORIA

Este proyecto de tesis está dedicado íntegramente a Dios y a mi familia, por el apoyo incondicional y la motivación que debiera tener todo ser exitoso.

Reinaldo A. Encalada Malca

A mi madre, Elizabeth, quien siempre es promotora del estudio y la superación, y a todos los que me apoyaron a elaborar y concluir esta tesis.

José H. Quispe Chilcón

AGRADECIMIENTO

A Dios por la oportunidad de llegar aquí siendo un profesional íntegro del cual estoy complacido y orgulloso, a mi familia por todo su apoyo durante estos años de esfuerzo y sacrificio por lo que ruego a Dios me dé la vida suficiente para disfrutarla a lado de las personas que más quiero, a mi amigo y compañero de tesis por confiar en mí para el desarrollo de este trabajo y porque a pesar de poseer diferentes criterios para algunas situaciones de trabajo, conciliamos y terminamos este proyecto exitosamente, finalmente agradezco a todo aquel que considere haber contribuido positivamente a cumplir esta meta.

Reinaldo A. Encalada Malca

Agradezco inmensamente a Dios, por darme la salud que tengo, sin la cual no hubiese podido concluir este camino. Agradezco de manera especial y sincera a todos los miembros de mi familia, quienes siempre me apoyaron, tomando algunas de mis responsabilidades como suyas. A Anays, por su apoyo incondicional y por su forma de animarme a continuar con este trabajo. Finalmente como olvidarme de agradecer a un nuevo amigo y próximo socio de negocios Reinaldo, con el cual aprendimos a hacer buena dupla, combinando nuestras fortalezas.

José H. Quispe Chilcón

ÍNDICE GENERAL

I. INTRODUCCIÓN……1

II. MARCO TEÓRICO…… 4

2.1 Inteligencia Artificial y Sistemas Expertos.....4

2.1.1. Características de los Sistemas Experto.....5

2.1.2. Tipos de Sistemas Expertos 7

2.1.3. Algoritmos 10

2.1.4. Herramientas 10

2.1.5. Ventajas y limitaciones 14

2.2 Sistemas de Soporte de Decisiones 15

2.3 Sistemas de Soporte para Ejecutivos.....16

2.3.1 Comparación Entre DSS, Sistemas Expertos y ESS.....16

2.4 Técnicas de Auditoría Asistidas por Computador.....17

2.5 Auditoría.....18

2.6 Consultoría 18

2.7 Control Interno Informático 18

2.8 Auditoría Informática 19

2.8.1 Auditoría Interna y Auditoría Externa 19

2.9 Norma Técnica Peruana 27001 20

2.10 Activo 20

2.11 Seguridad de la información.....21

2.12 Disponibilidad 21

2.13 Confidencialidad 21

2.14 Integridad.....21

2.15 Sistema de Gestión de Seguridad de la información (SGSI).....21

2.16 Control 21
2.17 Política 22
2.18 Amenaza 22
2.19 Vulnerabilidad 22
2.20 Norma Técnica Peruana 27002 22
2.21 COBIT 5 23
III. MATERIALES Y METODOS 27
3.1 Materiales 27
3.1.1 Personal 27
3.1.2 Bienes 27
3.1.3 Servicios 28
3.2 Método 28
3.2.1 Objeto de Estudio 28
3.2.2 Tipo de Estudio 28
3.2.3 Procedimiento Experimental 31
3.4 Diseño de Contrastación 33
3.4.1 Población 33
3.4.2 Muestra 33
3.4.3 Diseño de Pruebas 33
3.5 Proceso general de Contrastación 33
IV. RESULTADOS 36
4.1 Inicio 36
4.1.1 Lista de metodologías de desarrollo de Sistemas Expertos 36
4.1.2 Estudio de viabilidad de desarrollo del SE 44
4.1.3 Descripción del proyecto propuesto 52
4.1.4 Adaptar una metodología para el desarrollo del SE 53

4.2 Análisis de Requisitos 58
4.2.1 Lista de fuentes de alimentación de conocimiento del Sistema Experto…….....58
4.2.2 Diagrama de Casos de Uso 59
4.2.3 Modelo de Dominio 65
4.3 Diseño.....66
4.3.1 Descripción de Casos de Uso.....66
4.3.2 Diagramas de Secuencia 106
4.3.3 Diagrama de clases.....184
4.3.4 Prototipos 185
4.4 Implementación.....226
4.4.1 Interfaces del Sistema 226
4.4.2 Diagrama de componentes 291
4.4.2.1 Diagrama de componentes (View).....292
4.4.2.2 Diagrama de componentes (db) 293
4.4.2.3 Diagrama de componentes (controller).....294
4.4.2.4 Diagrama de componentes (beans) 295
4.4.3 Diagrama de despliegue 296
4.4.4 Diagrama físico 297
4.5 Pruebas 298
V. DISCUSIÓN……299
5.1. Contrastación de la Hipótesis 299
5.1.1. Identificación de Variables e Indicadores 299
5.1.2. Método de Análisis para los Indicadores Cualitativos.....299
5.1.3. Método de Análisis para los Indicadores Cuantitativos.....301
5.2. Prueba de Hipótesis para el Indicadores Cualitativos 303

5.2.1. Indicador “Disponibilidad del Informe de Auditoría” 303
5.2.2. Indicador “Integridad del Informe de Auditoría”.....306
5.2.3. Indicador “Confidencialidad del Informe de Auditoría” 310
5.2.4. Indicador “Facilidad de Uso de la Aplicación”.....314
5.3. Prueba de Hipótesis para el Indicadores Cuantitativos 317
5.3.1. Indicador “Cantidad de vulnerabilidades identificadas”.....317
5.3.2. Indicador “Cantidad de amenazas identificadas”.....319
5.4. Discusión de Resultados.....321
VI. CONCLUSIONES……323
VII. RECOMENDACIONES……...325
VIII. REFERENCIAS……326
IX. ANEXOS……..328

ÍNDICE DE FIGURAS

Figura II-1: Estructura de un Sistema Experto 7
Figura II-2: Familia de productos COBIT 5.0 24
Figura II-3: APO13 - Gestionar Seguridad 25
Figura II-4: DSS05 Gestionar los Servicios de Seguridad 26
Figura III-1: Región de aceptación 1 34
Figura III-2: Región de aceptación 2 35
Figura III-3: Estructura del conocimiento del Sistema Experto en Seguridad de la Información Propuesto 46

ÍNDICE DE TABLAS

Tabla II.1: Comparación entre DSS, Sistemas Expertos y ESS 17
Tabla III.1: Indicadores de Evaluación 30
Tabla III.2: Método de trabajo 32
Tabla III.3: Instrumentos empleados en el Proyecto 32
Tabla IV.1: Cronograma del proyecto 46
Tabla IV.2: Gastos generales de la auditoría 1 49
Tabla IV.3: Costo de materiales empleados 1 49
Tabla IV.4: Resumen de costos 1 50
Tabla IV.5: Gastos generales de la auditoría 2 50
Tabla IV.6: Costos de materiales empleados 2 51
Tabla IV.7: Resumen de costos 2 51
Tabla IV.8: Comparación de costos 1 y 2 52
Tabla IV.9: Descripción del lineamiento L1 54
Tabla IV.10: Descripción del lineamiento L2 54
Tabla IV.11: Descripción del lineamiento L3 54
Tabla IV.12: Descripción del lineamiento L4 55
Tabla IV.13: Matriz de evaluación de metodologías 55

SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NTP ISO 27001 Y 27002 Y COBIT.

RESUMEN

Por: Br. Encalada Malca, Reinaldo Alberto
Br. Quispe Chilcón, José Hernán

La información es uno de los activos con mayor importancia e impacto de toda organización, representa el elemento clave capaz de garantizar la continuidad de cualquier negocio e influye directamente en el desempeño de las operaciones. Con el paso de los años aparecieron buenas prácticas y estándares relacionados a Sistemas de Gestión de Seguridad de la Información (SGSI), buscando garantizar un adecuado tratamiento y protección de la información; sin embargo, se está todavía lejos de obtener un sistema totalmente seguro, por la naturaleza inherente de las vulnerabilidades de los activos de información, sus amenazas y riesgos.

Se propone el desarrollo de un Sistema Experto en Seguridad de la Información (denominado XSIS) que facilite la identificación de vulnerabilidades y amenazas de los activos de información, desarrollado bajo los Criterios de Auditoría NTP ISO 27001:2013 e ISO 27002:2013, combinado con las buenas prácticas de COBIT 5, y el conocimiento propio añadido de expertos en auditoría informática.

Los resultados de la aplicación de XSIS demuestran que es posible realizar una Auditoría de Seguridad de Información con personal experto y no experto en la materia, además su base de conocimiento permite la identificación de vulnerabilidades y amenazas de los activos de información asociados a través de formatos de evaluación diseñados específicamente para situaciones particulares.

Palabras clave: Auditoría, Sistema Experto, Seguridad de la Información, Integridad, Disponibilidad, Confidencialidad, Vulnerabilidad, Amenaza, Norma Técnica Peruana, ISO y COBIT 5.

EXPERT SYSTEM AUDIT INFORMATION SECURITY BASED NTP ISO 27001 and 27002 and COBIT

ABSTRACT

By: Br. Encalada Malca, Reinaldo Alberto
Br. Quispe Chilcón, José Hernán

Information is one of the most important assets and impact of any organization, represents the key element capable of ensuring continuity of any business and directly influences the performance of operations. Over the years they were good practices and standards related to Management Systems Information Security (ISMS), seeking to ensure proper treatment and protection of information; however, it is still far from obtaining a totally secure system, the inherent nature of the vulnerabilities of information assets, threats and risks.

The development of an Expert System for Information Security is proposed, to facilitate the identification of vulnerabilities and threats of information assets developed under the Audit standard NTP ISO 27001: 2013 and "ISO 27002: 2013" combined with the best practices of COBIT 5, and self-knowledge added Computer audit experts.

The results of the application of XSIS show that it is possible to perform an Audit of Information Security expert staff and non-skilled, besides their knowledge base allows the identification of vulnerabilities and threats associated information assets across formats assessment designed specifically for particular situations.

Keywords: COBIT 5, Audit, Expert System, Information Security, Integrity, Availability, Confidentiality, Vulnerability, Threat, International Standard, and ISO.

I. INTRODUCCIÓN

La información es uno de los activos con mayor importancia e impacto de toda organización, representa el elemento clave capaz de garantizar la continuidad de cualquier negocio e influye directamente en el desempeño de las operaciones. Con el paso de los años aparecieron los Sistemas de Gestión de Seguridad de la Información (SGSI) que buscan garantizar su adecuado tratamiento y protección, sin embargo se está todavía lejos de obtener un sistema totalmente seguro: por la constante aparición de riesgos, la naturaleza inherente de las vulnerabilidades los activos de información y sus amenazas.

Es necesario comprender que cada activo de información debe ser correctamente gestionado de forma que se asegure su total contribución hacia el alcance de los objetivos organizacionales; sin embargo al conocer la naturaleza inherente de las vulnerabilidades de cada activo se está expuesto a un conjunto de amenazas que impedirían dicha contribución si los mecanismos encargados de su gestión (SGSI) no cumplen con los procedimientos establecidos por las políticas y buenas prácticas.

Los SGSI están compuestos por un conjunto de políticas que buscan garantizar la seguridad de la información, sin embargo, siempre se formulará la siguiente pregunta ¿cómo evaluar la implantación y madurez del SGSI? Muchas respuestas pueden surgir, pero los especialistas recomiendan se realice a través de auditorías de Seguridad de la Información.

Es en este sentido, que se plantea la necesidad de revisar de forma continua el SGSI de forma que se cumpla con los estándares y buenas prácticas establecidas por políticas empresariales: de aquellas plasmadas en normas técnicas[1,2] marcos de gobierno[3] y las que son resultado del trabajo y experiencia

[1] *Comisión de Reglamentos Técnicos y Comerciales - INDECOPI. (2013). "Norma Técnica Peruana NTP-ISO/IEC 27002 2013". Lima.*

de personal cualificado en la materia y que por su naturaleza no se encuentran descritas formalmente y radican en el interior de cada autor o grupo de trabajo como conocimiento propio.

Este trabajo de investigación tiene como hipótesis: "La aplicación de un Sistema Experto en Seguridad de la Información durante una auditoría mejora la identificación de vulnerabilidades y amenazas de los activos de información", objetivo general: "Implementar un Sistema Experto en Seguridad de la información que soporte la realización de auditorías facilitando la identificación de vulnerabilidades y amenazas de los activos de información" y objetivos específicos: (1) "Identificar las diferentes metodologías de desarrollo de Sistemas Expertos", (2) "Identificar fuentes de conocimiento de alimentación del Sistema Experto", (3) "Determinar la viabilidad del desarrollo de un Sistema Experto en Auditoría de Seguridad de la Información", (4) "Adaptar una metodología de Sistemas Expertos en la construcción de un Sistema Experto en Auditoría de Seguridad de la Información, basado en las NTP ISO 27001 y 27002, COBIT 5 y conocimiento de un experto" y (5) "Evaluar la aplicación del Sistema Experto en una Auditoría de Seguridad de la Información".

Se justica la investigación por los siguientes aportes: (1) Aporte Económico: Reducción de los costos asociados a la auditoría por el tiempo de ejecución y materiales que se utilicen, (2) Aporte Tecnológico: El desarrollo de un Sistema Experto en Seguridad de la Información basado en normas técnicas peruanas y COBIT 5, (3) Aporte Legal: Difusión de las NTP 27001 y 27002, (4) Aporte Operacional: Dar soporte al proceso de auditoría y mejorar la identificación de vulnerabilidades y amenazas de los activos de información y (5) Aporte Social: La mejora de las condiciones del trabajo, al brindar soporte a un proceso largo y riguroso de verificación, permitiendo la flexibilidad e independencia geográfica.

[2] *Comisión de Normalización y de Fiscalización de Barreras Comerciales Noarancelarios - INDECOPI. (2013). "Norma Técnica Peruana NTP-ISO/IEC 27001 2013". Lima.*
[3] *ISACA (Information Systems Audit and Control Asociation) e ITGI (Information Technology Governance Institute). (2012). COBIT 5 Objetivos de Control para la Información y las Tecnologías Relacionadas.*

Para una mejor lectura el informe se ha estructurado en:

Capítulo II: Marco Teórico, en este capítulo se describe los conceptos más significativos de la investigación.

Capítulo III: Materiales y Métodos, se encuentran descritos los materiales y el método empleado para el desarrollo del proyecto.

Capítulo IV: Resultados, se describe los resultados de cada etapa del método empleado.

Capítulo V: Discusión, se definen los indicadores que permitirán contrastar la hipótesis del trabajo.

Finalmente se presentan las conclusiones, recomendaciones, referencias bibliográficas, anexos y referencias biográficas.

II. MARCO TEÓRICO

2.1 Inteligencia Artificial y Sistemas Expertos

(Kendall & Kendall, 2011) La inteligencia artificial (AI) puede ser considerada como el campo dominante de los sistemas expertos. La idea general de la AI ha sido desarrollar equipos que se comporten de manera inteligente. Dos ramas de investigación de la AI son: 1) la comprensión del lenguaje natural y 2) el análisis de la habilidad para razonar un problema y llegar a una conclusión lógica. Los sistemas expertos utilizan las metodologías de razonamiento de la AI para resolver los problemas que los usuarios de negocios (y otro tipo de usuarios) les presentan.

Un sistema experto (también conocido como sistema basado en el conocimiento) captura y utiliza en forma efectiva el conocimiento de uno o varios expertos humanos para resolver un problema específico al que una organización se enfrenta. Cabe mencionar que a diferencia de los Sistemas de Soporte a las Decisiones (DSS), que en última instancia dejan la decisión a la persona encargada de la toma de decisiones, un sistema experto selecciona la mejor solución para un problema o una clase específica de problemas.

Los componentes básicos de un sistema experto son la base de conocimiento, un motor de inferencia que conecta al usuario con el sistema mediante el proceso de consultas en lenguajes - como el lenguaje de consulta estructurado (SQL), y la interfaz de usuario. Las personas conocidas como ingenieros del conocimiento capturan la experiencia de los expertos, crean un sistema computacional que incluye este conocimiento y después lo implementan.

2.1.1. Características de los Sistemas Expertos

(Badaró, Javier Ibañez, & Agüero, 2013)

Estructura

Los SE están compuestos por dos partes principales: el ambiente de desarrollo y el ambiente de consulta. El ambiente de desarrollo es utilizado por el constructor para crear los componentes e introducir conocimiento en la base de conocimiento.

El ambiente de consulta es utilizado por los no expertos para obtener conocimiento experto y consejos.

Los siguientes son los componentes básicos de un SE:

Subsistema de adquisición de conocimiento

Es la acumulación, transferencia y transformación de la experiencia para resolver problemas de una fuente de conocimiento a un programa de computadora para construir o expandir la base de conocimiento. El estado del arte actual requiere un ingeniero en conocimiento que interactúe con uno o más expertos humanos para construir la base de conocimiento.

Base de conocimiento

Contiene el conocimiento necesario para comprender, formular y resolver problemas. Incluye dos elementos básicos: heurística especial y reglas que dirigen el uso del conocimiento para resolver problemas específicos en un dominio particular.

Base de hechos

Es una memoria de trabajo que contiene los hechos sobre un problema, alberga los datos propios correspondientes a los problemas que se desean tratar.

Motor de inferencia

Es el cerebro del SE, también conocido como estructura de control o interpretador de reglas. Este componente es esencialmente un programa de computadora que provee metodologías para razonamiento de información en la base de conocimiento.

Este componente provee direcciones sobre cómo usar el conocimiento del sistema para armar la agenda que organiza y controla los pasos para resolver el problema cuando se realiza una consulta. Tiene tres elementos principales:

1) Intérprete, ejecuta la agenda seleccionada; 2) programador, mantiene el control sobre la agenda; 3) control de consistencia, intenta mantener una representación consistente de las soluciones encontradas.

Subsistema de justificación

Se encarga de explicar el comportamiento del SE al encontrar una solución.

Permite al usuario hacer preguntas al sistema para poder entender las líneas de razonamiento que este siguió. Resulta especialmente beneficioso para usuarios no expertos que buscan aprender a realizar algún tipo de tarea.

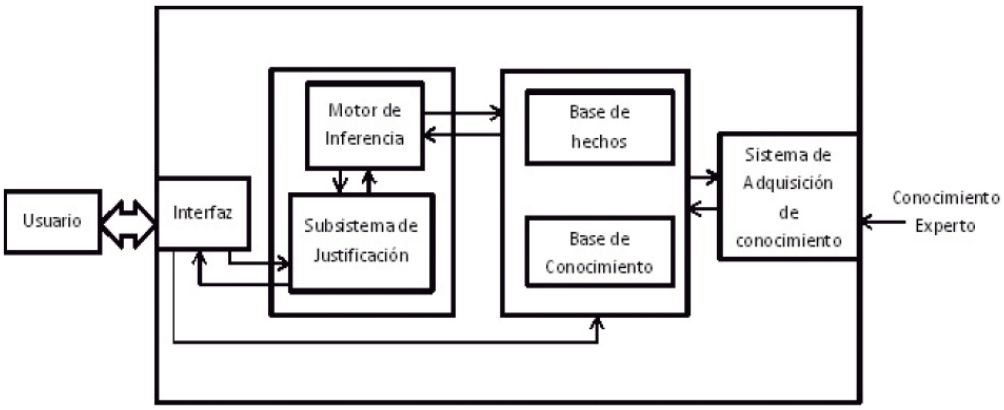


Figura II-1: *Estructura de un Sistema Experto*

2.1.2. Tipos de Sistemas Expertos

(Badaró, Javier Ibañez, & Agüero, 2013)

2.1.2.1. Basados en reglas previamente establecidas

Los sistemas basados en reglas trabajan mediante la aplicación de reglas, comparación de resultados y aplicación de las nuevas reglas basadas en situación modificada. También pueden trabajar por inferencia lógica dirigida, bien empezando con una evidencia inicial en una determinada situación y dirigiéndose hacia la obtención de una solución, o bien con hipótesis sobre las posibles soluciones y volviendo hacia atrás para encontrar una evidencia existente (o una deducción de una evidencia existente) que apoya una hipótesis en particular.

Representación del conocimiento

Hay numerosas formas de representar el conocimiento en IA, sin embargo, los Sistemas Expertos suelen ser llamados sistemas basados en reglas.

Reglas "Si...entonces..."

Las reglas "Si... Entonces…" son el principal tipo de conocimiento usado en Sistemas Expertos, donde dichas normas se utilizan para capturar razonamiento de expertos que emplean a menudo. Sin embargo, con el tiempo los investigadores comenzaron a desarrollar e integrar otras formas de representación del conocimiento, tales como el razonamiento basado en casos.

Los sistemas que incluyen múltiples tipos de conocimiento a veces se conocen como sistemas híbridos, o etiquetados después de un determinado tipo de representación del conocimiento, por ejemplo, basado en casos (O'Leary, 2008).

2.1.2.2. Basados en casos

El razonamiento basado en casos es el proceso de solucionar nuevos problemas basándose en las soluciones de problemas anteriores. Un mecánico de automóviles que repara un motor porque recordó que otro auto presentaba los mismos síntomas está usando razonamiento basado en casos. Un abogado que apela a precedentes legales para defender alguna causa está usando razonamiento basado en casos.

También un ingeniero cuando copia elementos de la naturaleza, está tratando a esta como una "base de datos de soluciones". El Razonamiento basado en casos es una manera de razonar haciendo analogías. Se ha argumentado

que el razonamiento basado en casos no sólo es un método poderoso para el razonamiento de computadoras, sino que es usado por las personas para solucionar problemas cotidianos. Más radicalmente se ha sostenido que todo razonamiento es basado en casos porque está basado en la experiencia previa.

2.1.2.3. Basados en redes bayesianas

Una red bayesiana, red de Bayes, red de creencia, modelo bayesiano o modelo probabilístico en un gráfico acíclico dirigido es un modelo gráfico probabilístico (un tipo de modelo estático) que representa un conjunto de variables aleatorias y sus dependencias condicionales a través de un gráfico acíclico dirigido (DAG por sus siglas en inglés).

Por ejemplo, una red bayesiana puede representar las relaciones probabilísticas entre enfermedades y síntomas. Dados los síntomas, la red puede ser usada para computar las probabilidades de la presencia de varias enfermedades.

2.1.2.4. Sistemas Expertos difusos

Los Sistemas Expertos difusos se desarrollan usando el método de lógica difusa, la cual trabaja con incertidumbre. Esta técnica emplea el modelo matemático de conjuntos difusos, simula el proceso del razonamiento normal humano permitiendo a la computadora comportarse menos precisa y más lógicamente que las computadoras convencionales. Este enfoque es utilizado porque la toma de decisiones no

es siempre una cuestión de blanco y negro, verdadero o falso; a veces involucra áreas grises y el término "quizás".

2.1.3. Algoritmos

(Badaró, Javier Ibañez, & Agüero, 2013)
A pesar de sus características particulares, todos los algoritmos realizan comparaciones incrementales, es decir, utilizan soporte de estado para reducir la cantidad de coincidencias en ciclos sucesivos.

El algoritmo más popular es el Rete y en menor frecuencia también se emplean los siguientes algoritmos: Eager, Evaluantion y Lazy Evaluation.

Rete

El algoritmo de emparejamiento es un método eficiente para comparar una larga colección de patrones con una larga colección de objetos. Encuentra todos los objetos que coinciden con cada patrón.

El algoritmo fue desarrollado para el uso en intérpretes de sistemas de producción y se ha empleado por sistemas que contienen desde algunos cientos hasta miles de patrones y objetos. Este algoritmo es particularmente eficiente porque no itera sobre sobre los sets de patrones sino que contiene una red de ordenamiento con estructura de árbol o índice para los patrones. Los patrones son compilados en un programa que realiza el proceso de emparejamiento.

2.1.4. Herramientas

En esta sección se enumeran y describen brevemente distintos frameworks y tecnologías disponibles para la construcción de un Sistema Experto:

2.1.4.1. PROLOG

(Escrig, Pacheco, & Toledo, 2001)

PROLOG es un lenguaje de programación declarativo. Los lenguajes declarativos se diferencian de los lenguajes imperativos o procedurales en que están basados en formalismos abstractos (PROLOG está basado en la lógica de predicados de primer orden y LISP, otro lenguaje de programación declarativa, en lambda cálculo), y por tanto su semántica no depende de la máquina en la que se ejecutan. Las sentencias en estos lenguajes se entienden sin necesidad de hacer referencia al nivel máquina para explicar los efectos colaterales. Por tanto, un programa escrito en un lenguaje declarativo puede usarse como una especificación o una descripción formal de un problema. Otra ventaja de los programas escritos en lenguajes declarativos es que se pueden desarrollar y comprobar poco a poco, y pueden ser sintetizados o transformados sistemáticamente.

PROLOG es un lenguaje de programación muy útil para resolver problemas que implican objetos y relaciones entre objetos. Está basado en los siguientes mecanismos básicos:

- Unificación
- Estructuras de datos basadas en árboles.
- Back tracking automático.

La sintaxis del lenguaje consiste en lo siguiente:

- Declarar hechos sobre objetos y sus relaciones.
- Hacer preguntas sobre objetos y sus relaciones.

- Definir reglas sobre objetos y sus relaciones.

2.1.4.2. CLIPS

(Badaró, Javier Ibañez, & Agüero, 2013)

A mediados de los años ochenta, la NASA requería el apoyo de Sistemas Expertos para el desarrollo de proyectos. Por lo tanto, una serie de prototipos surgen pero sus resultados no fueron lo suficientemente buenos para cumplir con los requerimientos internos. En consecuencia, se desarrolló un prototipo de un Sistema Experto, denominado CLIPS (C Language Integrated Production System) cuya principal característica era su capacidad para funcionar con otros sistemas existentes. Posteriores mejoras y ampliaciones han convertido CLIPS en un punto de referencia para el desarrollo de otros Sistemas Expertos.

2.1.4.3. JESS

(Badaró, Javier Ibañez, & Agüero, 2013)

El motor de reglas JESS es un proyecto que tuvo su origen en CLIPS pero que fue escrito enteramente en Java. Se desarrolló durante la década de los noventa en los Sandia National Laboratories y comparte con CLIPS varios conceptos de diseño y similitudes con respecto a la sintaxis. Asimismo implementa la especificación de referencia JSR94.

2.1.4.4. DROOLS

(Badaró, Javier Ibañez, & Agüero, 2013)

Al igual que en el caso de los CLIPS y JESS, Drools es la implementación y ampliación del algoritmo Rete diseñado por el Dr. Charles L. Forgy en la Universidad Carnegie Mellon. Básicamente, su algoritmo consiste en una red de nodos interconectados con diferentes características que evalúan las entradas mediante la propagación de los resultados del siguiente nodo cuando hay coincidencias. DROOLS ofrece herramientas de integración con Java, la capacidad de escalabilidad y una división clara entre los datos y la lógica de dominio.

2.1.4.5. JENA

(Badaró, Javier Ibañez, & Agüero, 2013)
Jena es un framework desarrollado en tecnología Java que incluye un motor de inferencia basado en normas, una API ontológica y un motor de búsqueda (Jena, 2013).

2.1.4.6. JEOps

(Badaró, Javier Ibañez, & Agüero, 2013)
JEOPS añade encadenamiento hacia adelante, las normas de producción de primer orden con el fin de facilitar el desarrollo de Sistemas Expertos mediante programación declarativa.

2.1.4.7. OPENCYC

(Badaró, Javier Ibañez, & Agüero, 2013)
OpenCyc es la versión de código abierto de la tecnología CyC más completa base de conocimientos generales del mundo y motor de razonamiento de sentido común.

2.1.5. Ventajas y limitaciones

(Badaró, Javier Ibañez, & Agüero, 2013)

Ventajas

Mientras que un experto humano tiene limitaciones y percances propias de su condición humana, es decir: se enferma, envejece, migra a otras empresas, el Sistema Experto, respecto a sus pares humanos, no sufre de estas cuestiones y se convierte en una herramienta estable para su entorno y fiable porque sus actividades son completamente replicables (siempre contesta de la misma manera a menos que se le cambie el diseño). A esto se le suma la velocidad de procesamiento que es mayor al de un ser humano. Debido a la escasez de expertos humanos en determinadas áreas, los SE pueden almacenar su conocimiento para cuando sea necesario poder aplicarlo. Así mismo los SE pueden ser utilizados por personas no especializadas para resolver problemas. Además si una persona utiliza con frecuencia un SE aprenderá de él.

Finalmente, si se evalúa el costo total del empleo de esta tecnología, la replicabilidad y estabilidad, asociado a la seguridad que provee, resulta una ecuación favorable, aun considerando que las inversiones iniciales pueden ser relativamente elevadas.

Limitaciones

Es evidente que para actualizar se necesita de reprogramación de estos (tal vez este sea una de sus limitaciones más acentuadas) otra de sus limitaciones puede ser el elevado costo en dinero y tiempo,

además que estos programas son poco flexibles a cambios y de difícil acceso a información no estructurada.

Los Sistemas Expertos carecen de sentido común, para un SE no hay nada obvio Además no podemos mantener una conversación informal con estos sistemas. Para un sistema experto es muy complicado de aprender de sus errores y de errores ajenos. No son capaces de distinguir cuales son las cuestiones relevantes de un problema y separarlas de cuestiones secundarias.

Por otra parte, la inteligencia artificial no ha podido desarrollar sistemas que sean capaces de resolver problemas de manera general o de aplicar el sentido común para resolver situaciones complejas ni de controlar situaciones ambiguas.

2.2 Sistemas de Soporte de Decisiones

(Kendall & Kendall, 2011)

Los sistemas de soporte de decisiones (DSS, o sistemas de apoyo a la toma de decisiones) pertenecen a una clase superior de sistemas de información computarizados. Los sistemas DSS son similares al sistema de información administrativa tradicional debido a que ambos dependen de una base de datos como fuente de datos. La diferencia estriba en que el sistema de soporte de decisiones está más enfocado a brindar respaldo a la toma de decisiones en todas sus fases, aunque la decisión misma aun corresponde de manera exclusiva al usuario.

Los sistemas de soporte de decisiones se ajustan más a la persona o el grupo usuario que un sistema de información administrativa tradicional. También se describen a veces como sistemas enfocados en la inteligencia de negocios.

2.3 Sistemas de Soporte para Ejecutivos

(Kendall & Kendall, 2011)
Cuando los ejecutivos fijan su atención en la computadora, a menudo buscan obtener ayuda para tomar decisiones en el nivel estratégico.

Los sistemas de soporte para ejecutivos (ESS, sistemas de apoyo para ejecutivos) ayudan a los ejecutivos a organizar sus interacciones con el entorno externo ofreciendo tecnologías de gráficos y comunicaciones en sitios accesibles como salas de juntas u oficinas corporativas personales.

Aunque los sistemas ESS se basan en la información que generan los sistemas TPS Y MIS, ayudan a sus usuarios a enfrentar los problemas relacionados con decisiones no estructuradas inespecíficas de una aplicación, para lo cual crean un entorno que les ayude a pensar sobre los problemas estratégicos de una manera informada. Los sistemas ESS extienden las capacidades de los ejecutivos y les ofrecen soporte para que puedan entender mejor sus entornos.

2.3.1 Comparación Entre DSS, Sistemas Expertos y ESS

(Kendall & Kendall, 2011)
Las Principales diferencias se resumen en la siguiente tabla:

Sistemas de Soporte a las Decisiones	Sistemas Expertos	Sistema de Soporte Para Ejecutivos
La decisión final corresponde de manera exclusiva al usuario.	Selecciona la mejor solución para un problema o una clase específica de problemas.	Ayudan a sus usuarios a enfrentar los problemas relacionados con decisiones no estructuradas inespecíficas de una aplicación.
Brinda respaldo a la toma de decisiones.	Captura y utiliza en forma efectiva el conocimiento de uno o varios expertos humanos para resolver un problema específico al que una organización se enfrenta.	Ayudan a los Ejecutivos a entender mejor su entorno.
Depende de una base de datos como fuente de datos.	Tiene como componentes básicos una base de conocimiento, un motor de inferencia, y la interfaz de usuario.	Se basan en información que generan los TPS y MIS
Se describen como sistemas enfocados a la inteligencia de negocios	Utilizan metodologías de razonamiento de la AI para resolver problemas que los usuarios de negocios presentan	Ayudan a los ejecutivos a organizar sus interacciones con el entorno externo ofreciendo tecnologias de graficos y comunicaciones en sitios accesibles como salas de juntas u oficinas corporativas personales.

Tabla II.1: Comparación entre DSS, Sistemas Expertos y ESS

2.4 Técnicas de Auditoría Asistidas por Computador

(Salazar Say, 2005)

Las técnicas de auditoría asistidas por computador o CAAT's, por sus siglas en inglés: Computer Assisted Audit Techniques, son programas que están diseñados para examinar los registros de procesamiento computarizado.

Son herramientas y técnicas de auditoría que permiten al auditor aumentar el alcance y la eficiencia de la auditoría con procedimientos automatizados. Pueden generar una gran parte de la evidencia de la auditoría de los sistemas de información.

Existen de distintos tipos, los cuales pueden utilizarse para prueba de los detalles de operaciones y saldos, procedimientos de revisión analíticos, pruebas de cumplimiento de los controles generales de sistemas de información, pruebas de cumplimiento de los controles de aplicación.

Finalmente, el auditor elabora determinadas partes del informe con archivos que son resultados de las pruebas y controles, por lo cual resulta necesario el manejo de software de fácil utilización como procesadores de texto, paquetes de gráficos, hojas de cálculo, etc.

Actualmente, existen muchas CAAT's en el mercado de las cuales se dará una descripción de algunas, entre ellas tenemos: ACLTM, IDEATM, PanAudit, Easytrieve, DYL280 (300), Culprit, FOCUS, FocAudit, etc.

2.5 Auditoría

(Piattini Velthuis, 2001)

Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

2.6 Consultoría

(Piattini Velthuis, 2001)

La consultoría consiste en "dar asesoramiento o consejo sobre lo que se ha de hacer o cómo llevar adecuadamente una determinada actividad para obtener los fines deseados".

2.7 Control Interno Informático

(Piattini Velthuis, 2001)

El Control Interno Informático controla diariamente que todas las actividades de sistema de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección y/o la Dirección de Informática, así como los requerimientos legales.

2.8 Auditoría Informática

(Piattini Velthuis, 2001)

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

2.8.1 Auditoría Interna y Auditoría Externa

(Piattini Velthuis, 2001)

a. Auditoría Interna

La auditoría Interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

b. Auditoría Externa

La auditoría Externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados.

2.9 Norma Técnica Peruana 27001

(INDECOPI C. d., 2013)

Esta Norma Técnica Peruana de Seguridad de la Información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de la Información ISMS, por sus siglas en Inglés (Information Security Management System). La adopción de un ISMS debe ser una decisión estratégica para una organización. El diseño e implementación del ISMS de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como que las situaciones simples requieran soluciones ISMS simples.

Esta Norma Técnica Peruana puede usarse en el ámbito interno y externo de las organizaciones.

Esta Norma Técnica Peruana está diseñada para hacer posible que una organización se alinee o integre su ISMS con los requisitos de los sistemas de gestión relacionados.

2.10 Activo

(INDECOPI C. d., 2013)

Cualquier bien que tiene valor para la organización.

2.11 Seguridad de la información

(INDECOPI C. d., 2013)

La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

2.12 Disponibilidad

(INDECOPI C. d., 2013)

La propiedad de ser accesible y utilizable por una entidad autorizada.

2.13 Confidencialidad

(INDECOPI C. d., 2013)

La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

2.14 Integridad

(INDECOPI C. d., 2013)

La propiedad de salvaguardar la exactitud y completitud de los activos.

2.15 Sistema de Gestión de Seguridad de la información (SGSI)

(INDECOPI C. d., 2013)

La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

2.16 Control

(INDECOPI C. d., 2013)

Medio de gestión del riesgo, que incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización, y que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

2.17 Política

(INDECOPI C. d., 2013)

Intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la organización.

2.18 Amenaza

(INDECOPI C. d., 2013)

Posible causa de un incidente no deseado, el cual puede ocasionar un daño a un sistema o a una organización.

2.19 Vulnerabilidad

(INDECOPI C. d., 2013)

Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

2.20 Norma Técnica Peruana 27002

(INDECOPI C. d., 2013)

Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

La norma puede servir como una guía práctica para desarrollar estándares organizacionales de seguridad y prácticas efectivas de la gestión de seguridad. Igualmente, permite proporcionar confianza en las relaciones entre organizaciones. Las recomendaciones que se establecen en esta norma deberían elegirse y utilizarse de acuerdo con la legislación aplicable en la materia.

2.21 COBIT 5

(ISACA, 2012)

Esta nueva versión de COBIT 5.0 se ajusta a todos los modelos de negocio, ambientes tecnológicos, posiciones y culturas corporativas.

"COBIT 5 es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Este documento contiene los 5 principios de COBIT 5 y define los 7 catalizadores que componen el marco." (COBIT 5.0, 2012)

Con COBIT 5.0 se mantiene la calidad de la información para la toma de decisiones, se tiene una excelencia operativa aplicando la mejor tecnología, reducir los riesgos de TI.

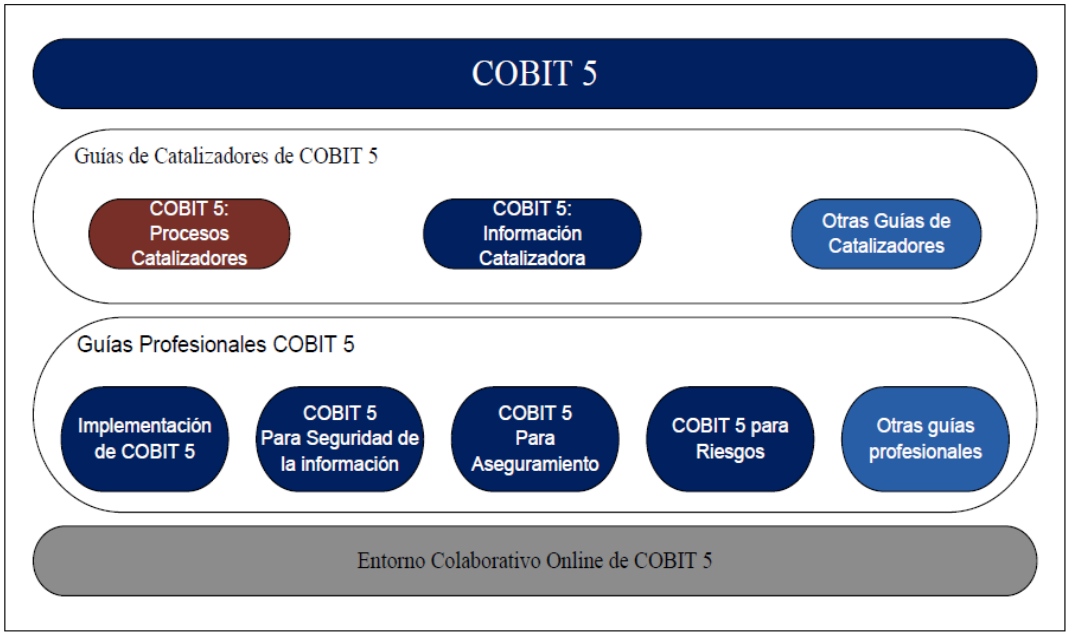


Figura II-2: Familia de productos COBIT 5.0

(ISACA, 2012)

Los procesos a utilizarse para apoyo de la ISO 27001 y la ISO 27002 son:

- APO13 - Gestionar Seguridad.
- DSS05 Gestionar los Servicios de Seguridad.

APO13 Gestionar la Seguridad	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	
El proceso contribuye al logro de un conjunto de objetivos principales relacionados con TI:	
Metas TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de casos de inversión de negocio, que tienen claramente definidos y aprobados los costes y beneficios esperados relacionados con TI • Porcentaje de servicios de TI que tienen claramente definidos y aprobados los costes operacionales y los beneficios esperados • Encuestas de satisfacción dirigidas a los principales accionistas en relación al nivel de transparencia, entendimiento y precisión de la información financiera de TI
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
14 Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión • Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos •Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

Figura II-3: *APO13 - Gestionar Seguridad*

(ISACA, 2012)

DSS05 Gestionar Servicios de Seguridad	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	
Declaración del Propósito del Proceso Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	• Número de vulnerabilidades descubiertas • Número de rupturas (*breaches*) de cortafuegos
2. La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final • Número de incidentes que impliquen dispositivos de usuario final • Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	• Promedio de tiempo entre los cambios y actualizaciones de cuentas • Número de cuentas (con respecto al número de usuarios/empleados autorizados)
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno • Clasificación media para las evaluaciones de seguridad física • Número de incidentes relacionados con seguridad física
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	• Número de incidentes relacionados con accesos no autorizados a la información

Figura II-4: *DSS05 Gestionar los Servicios de Seguridad*

(ISACA, 2012)

III. MATERIALES Y METODOS

3.1 Materiales

3.1.1 Personal

a. Autores

Br. Encalada Malca Reinaldo Alberto.

Br. Quispe Chilcón José Hernán.

b. Asesor

Ing. Díaz Sánchez, Jaime Eduardo.

3.1.2 Bienes

a. Materiales

- Papel Bond A4 de 80 gramos.
- Sobres de Manila A4.
- Útiles de escritorio (lápiz, lapiceros, borrador, corrector de tinta, tajador, regla y otros).
- Dispositivos de almacenamiento USB.
- DVD de 4.2 GB.
- Cartuchos de tinta color para impresora.

b. Equipos

- Computadora con microprocesador Intel® Core™ i7-3770T (caché de 8 MB, hasta 3.70 GHz), 8 GB RAM, Disco duro de 720 GB, Intel® HD Graphics 4000.
- Impresora HP 2400 D.
- Cámara fotográfica digital SONY DSC-TX200V - Cyber-shot™.

c. Software

- Microsoft Windows 7 Ultimate.

- Microsoft Office Professional 2010.
- Microsoft Project Professional 2010.
- IBM Rational Rose 7.0.0.
- NetBeans IDE 8.0.1.
- MySQL Workbench Community Edition 6.2.
- MySQL Server 5.6.
- Balsamiq Mockups 2.1.19.
- Bizagi Process Modeler.

3.1.3 Servicios

- Impresión
- Anillado.
- Empastado.
- Fotocopiado.
- Telefonía.
- Transporte.
- Bibliografía.
- Internet.

3.2 Método

3.2.1 Objeto de Estudio

Una universidad privada de la Ciudad de Trujillo.

3.2.2 Tipo de Estudio

La investigación a realizar es del tipo investigación cuasi-experimental, porque no se manipulan las variables deliberadamente, lo que se hará es observar tal y como suceden en el contexto natural para después analizarlos.

Se utilizara el modelo Post-test, con medición previa y posterior.

Formulación:

$$\ldots \rightarrow E \rightarrow o_2$$

Dónde:

… : No existe un Sistema Experto.

E : Implementación del Sistema Experto.

o₂ : La identificación de vulnerabilidades y amenazas de los activos informáticos después de la implementación del Sistema Experto.

Al final, se establecerán las diferencias entre o_1 y o_2, para determinar si hay un mejoramiento o no en los resultados obtenidos según los indicadores propuestos:

Indicador	U.M	Técnica	Instrumento	Fuente	Informante	Fórmula
Disponibilidad del Plan de Auditoría	%	Encuesta	Hoja de cálculo	Prueba del Sistema	Usuario	$\frac{1}{n}\sum_{1}^{n} x_{1i}$
Integridad del Plan de Auditoría	%.	Encuesta	Hoja de cálculo	Prueba del Sistema	Usuario	$\frac{1}{n}\sum_{1}^{n} x_{2i}$
Confidencialidad del Plan de Auditoría	%	Encuesta	Hoja de cálculo	Prueba del Sistema	Usuario	$\frac{1}{n}\sum_{1}^{n} x_{3i}$
Facilidad de uso del Sistema Experto	%	Encuesta	Hoja de cálculo	Prueba del Sistema	Usuario	$\frac{1}{n}\sum_{1}^{n} x_{4i}$
Cantidad de vulnerabilidades identificadas	-	Prueba del Sistema	Reporte	Sistema Experto	Sistema Experto	$\frac{1}{n}\sum_{1}^{n} x_{5i}$
Cantidad de amenazas identificadas	-	Prueba del Sistema	Reporte	Sistema Experto	Sistema Experto	$\frac{1}{n}\sum_{1}^{n} x_{6i}$

Tabla III.1: Indicadores de Evaluación

3.2.3 Procedimiento Experimental

El procedimiento utilizado es un marco de trabajo basado en la metodología de desarrollo de Jhon Durkin combinado con la metodología ICONIX, descrito en la siguiente tabla:

FASES	FLUJOS TRABAJO	RESULTADOS
1 Inicio	● Identificación de metodologías de desarrollo de Sistemas Expertos ● Estudio del Proceso. ● Determinar el Problema. ● Análisis de Costo/Beneficio.	● Lista de metodologías de desarrollo de Sistemas Expertos ● Estudio de viabilidad de desarrollo del SE. ● Descripción del Proyecto Propuesto. ● Metodología elegida para el desarrollo del SE.
2 Análisis de requisitos	● Determinación de los requisitos del Sistema. ● Adquisición del conocimiento.	● Diagrama de Casos de Uso de Requerimientos. ● Modelo de dominio. ● Lista de fuentes de alimentación de conocimiento del Sistema Experto.
3 Diseño	● Elaborar descripción de los casos de uso de Requerimientos. ● Seleccionar técnica de representación del conocimiento. ● Seleccionar técnica de control. ● Elaborar diagrama de secuencia. ● Elaborar diagrama de clases. ● Selección de software para el desarrollo de Sistema ● Prototipo de Producto.	● Descripción de Casos de Uso de Requerimientos. ● Diagramas de Secuencia. ● Diagrama de Clases. ● Prototipo del Producto.
4 Implementación	● Elaborar diagrama de componentes. ● Elaborar diagrama de despliegue. ● Elaborar diagrama físico de la BD.	● Diagrama de Componentes. ● Diagrama de

FASES	FLUJOS TRABAJO	RESULTADOS
	● Construir interfaces del Sistema. ● Desarrollo del producto.	despliegue. ● Diagrama físico de la BD. ● Producto Implementado.
5 Pruebas	● Realizar pruebas de Sistema Experto en una empresa. ● Documentar el proceso de prueba. ● Analizar resultados de la prueba. ● Comprobar hipótesis.	● Informe de las pruebas realizadas en el Sistema Experto en un ambiente de Producción.
6 Cierre	● Documentar la Tesis. ● Escribir Conclusiones y Recomendaciones.	● Informe de Tesis.

Tabla III.2: Método de trabajo

3.3 Instrumentos

En el presente proyecto las técnicas e instrumentos empleados para el levantamiento de información son:

TECNICA	INSTRUMENTOS
Entrevistas	Preguntas pre-formuladas
Encuestas	Hojas de Encuesta
Pruebas del Sistema Experto	Reporte

Tabla III.3: Instrumentos empleados en el Proyecto

3.4 Diseño de Contrastación

3.4.1 Población

El personal encargado en la universidad, de la seguridad de la información son DOS (02) y el personal experto son TRES (03).

3.4.2 Muestra

Al ser la población muy pequeña, la muestra será la misma.

3.4.3 Diseño de Pruebas

Para las pruebas de los indicadores cualitativos se utilizará la Distribución t de Student.

Para las pruebas de los indicadores cuantitativos se utilizará la prueba estadística z (normal).

3.5 Proceso general de Contrastación

- Establecer la Hipótesis Nula y la Hipótesis Alternativa:

  Hipótesis Nula $\longrightarrow$ $H_o : \mu_\beta - \mu_\alpha = 0$

  La aplicación de un Sistema Experto en Seguridad de la Información durante una auditoría mejora la identificación de vulnerabilidades y amenazas de los activos de información.

  Hipótesis Alternativa $\longrightarrow$ $H_1 : \mu_\beta - \mu_\alpha > 0$

  La aplicación de un Sistema Experto en Seguridad de la Información durante una auditoría no mejora la identificación de vulnerabilidades y amenazas de los activos de información.

- Establecer el Nivel de Significancia:

  Es la posibilidad de aceptar H_0 cuando en realidad es falsa y que generalmente es de 95%.

- Determinar Variables Estadísticas:

  t_0 : Estadístico t : Valor Crítico.

  z_0 : Estadístico z : Valor Crítico.

- Determinar la Región de Aceptación:

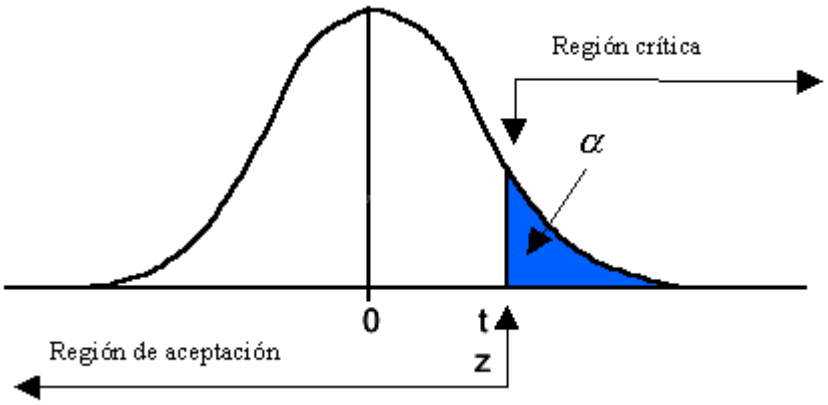


Figura III-1: Región de aceptación 1

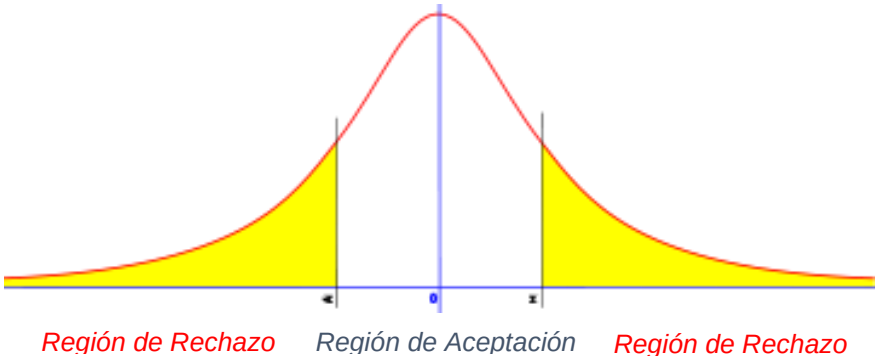


Figura III-2: Región de aceptación 2

- Decisión:

Si $t_0, z_0 \in R.R \rightarrow$ Rechazamos $H_o : \mu_\beta - \mu_\alpha = 0$

Aceptamos $H_1 : \mu_\beta - \mu_\alpha > 0$

Si $t_0, z_0 \notin R.R \rightarrow$ Aceptamos $H_o : \mu_\beta - \mu_\alpha = 0$

Rechazamos $H_1 : \mu_\beta - \mu_\alpha > 0$

IV. RESULTADOS

4.1 Inicio

4.1.1 Lista de metodologías de desarrollo de Sistemas Expertos

4.1.1.1 Blanqué y García Martínez.

(Martínez, 1992) Esta metodología se abrevia como BGM en base a las siglas de los creadores: Javier Blanqué y Ramón García Martínez. La característica más importante es la etapa de "Planteo de causalidades", la cual permite representar (mediante grafos) el conocimiento antes de formalizar las reglas.

La metodología consta de cinco etapas, las cuales se nombran a continuación.

- Adquisición del Conocimiento.
- Enunciación de conceptos.
- Parametrización de conceptos.
- Planteo de causalidades.
- Verificación.

Además existe una modificación de la metodología BGM original, la cual está enfocada en aquellos casos donde se pueden descubrir las reglas fácilmente. Las etapas son las siguientes.

- Adquisición del Conocimiento.
- Búsqueda de reglas causales.
- Búsqueda y Unificación de los conceptos y parámetros.
- Verificación.

4.1.1.2 Brulé.

(Brulé, J. & Bount, A., 1989) Esta metodología fue publicada por James F. Brulé. La característica más importante es la obtención temprana de un prototipo del sistema, es decir el uso de prototipado rápido.

Consta de siete etapas las cuales se nombran a continuación:

- Pre-planteamiento.
- Diseño y Especificación.
- Desarrollo temprano.
- Implementación.
- Evaluación.
- Supervisión.
- Mantenimiento.

4.1.1.3 Buchanan.

(Buchanan, B.G.; , Barstow, R.; , Betchal, R.; , Bennet, J.; , Clancey, W.; , Kulikowski, C., 1983) Esta metodología fue creada por Bruce G. Buchanan. La característica más importante es la constante relación que debe existir entre el

Ingeniero de conocimiento y el Experto Humano, pues la metodología se enfoca en la Adquisición del Conocimiento.

Consta de seis etapas las cuales se nombran a continuación:

- Identificación.
- Conceptualización.
- Formalización.
- Implementación.
- Pruebas.
- Revisión del Prototipo.

4.1.1.4 CommonKADS.

(Schreiber, 1999)
Esta metodología parte siendo un método sólo para la Adquisición del Conocimiento la cual fue denominada KADS, posteriormente se amplió al desarrollo completo de Sistemas Expertos (desde el análisis y diseño del software hasta la gestión del proyecto) la cual se conoce actualmente con el nombre de CommonKADS. Fue una propuesta del Instituto de Tecnología de Massachusetts.

Se puede considerar amplia y compleja, pero cubre todos los aspectos necesarios para el buen desarrollo de un sistema (desde el estudio del problema hasta la implantación y gestión del software).

Está basada en el ciclo de vida en espiral donde al final de cada etapa se entrega la documentación apropiada antes de pasar a la siguiente.
A continuación se nombran las etapas de la metodología:

- Análisis.
- Diseño.
- Implantación.
- Instalación.
- Uso.

Esta metodología posee dos grandes características:

- La gestión de proyecto, pues involucra aspectos administrativos que generalmente no son considerados al momento de desarrollar un sistema informático.
- El planteamiento de desarrollo de modelos que reflejan diferentes vistas del proyecto, estos modelos son de: Diseño, Conocimientos, Comunicación, Organización, Tareas y Agentes.

4.1.1.5 González – Dankel.

(González, 1993)
Esta metodología fue creada por Avelino J. González y Douglas D. Dankel. La característica más importante es que está basada en prototipado rápido, procedimiento que permite reducir los tiempos de desarrollo y obtener prototipos del sistema tempranamente para que puedan ser modificados y perfeccionados lo mejor posible.

Consta de ocho etapas las cuales se nombran a continuación:

- Análisis del problema.
- Especificación de requisitos.
- Diseño preliminar.
- Prototipado inicial y Evaluación.
- Diseño final.
- Implementación.
- Prueba.
- Ajuste de diseño y Mantenimiento.

4.1.1.6 Grover

(Grover, 1983)

Esta metodología fue publicada el año 1983 y se enfoca en el desarrollo del proceso de Adquisición del Conocimiento. La característica más importante es el énfasis en la obtención de documentación, la cual reemplaza parcialmente al experto y además otorga referencia a los diseñadores y usuarios del sistema.

Se compone de tres etapas detalladamente documentadas, éstas son:

- Definición del dominio: conocimientos, referencias, situaciones y procedimientos.

- Formulación del conocimiento fundamental: reglas elementales, creencias y expectativas.
- Consolidación del conocimiento de base: revisión y ciclos de corrección.

4.1.1.7 I.D.E.A.L.

(Pazos, 1996) (Alonso, 1996)

Fue desarrollado en la Facultad de Informática de la Universidad Politécnica de Madrid. I.D.E.A.L. es un acrónimo de las palabras: Identificación, Desarrollo, Ejecución, Acción y Logro.

Las cuales coinciden con las cinco etapas que conforman esta metodología:

- Identificación de la Tarea.
- Desarrollo de Prototipos.
- Ejecución de la Construcción Del Sistema Integrado.
- Actuación para Conseguir el Mantenimiento Perfectivo.
- Lograr una Adecuada Transferencia Tecnológica.

Se caracteriza por estar basada en prototipado rápido, por ende se obtienen prototipos iniciales los cuáles se van mejorando de manera paulatina hasta converger en un sistema óptimo. Otra de sus características es la adaptación a sistemas:

- Reutilizables.
- Integrables.
- Con requisitos abiertos.
- Con diversidad de modelos computacionales.

4.1.1.8 John Durkin.

(Durkin, 1994)

Metodología publicada en 1994 por John Durkin. Consta de seis etapas las cuales se nombran a continuación:

- Evaluación.
- Adquisición del Conocimiento.
- Diseño.
- Pruebas.
- Documentación.
- Mantenimiento.

4.1.1.9 M.I.K.E.

(Angele, 1993)

M.I.K.E. es un acrónimo de: Model-based and Incremental Knowledge Engineering. Define un marco de trabajo que cubre desde la extracción del conocimiento hasta el diseño e implementación del sistema. Consta de un desarrollo cíclico

e incremental donde se propone la integración de: modelo de ciclo de vida, prototipos y técnicas de especificación semi-formal y formal.

Esta metodología se basa más en la integración de prototipos que en la construcción de diferentes vistas del problema y del sistema.

Consta de cuatro etapas las cuales se nombran a continuación:

- Adquisición del Conocimiento.
- Diseño.
- Implementación.
- Evaluación.

4.1.1.10 Weiss y Kulikowski

(Weiss, 1984)

Esta metodología, fue publicada en el año 1984 por Sholom M. Weiss y Casimir A. Kulikowski, integrantes del Departamento de Informática de la Universidad de Rutgers.

Consta de siete etapas las cuales se nombran a continuación:

- Planteamiento del problema.
- Encontrar Expertos Humanos.

- Diseño de un Sistema Experto.
- Elección de la herramienta de desarrollo.
- Desarrollo y Prueba de un prototipo.
- Refinamiento y Generalización.
- Mantenimiento y Puesta al día.

4.1.2 Estudio de viabilidad de desarrollo del SE

La determinación de la viabilidad del desarrollo del Sistema Experto estuvo basada en la evaluación de la disponibilidad, cantidad y calidad de las fuentes de conocimiento, tiempo para el desarrollo del proyecto, beneficios y costos de implementación.

a. Fuentes de conocimiento

La lista de fuentes de alimentación de conocimiento del Sistema Experto se encuentra descrita en el numeral 4.2.1 del capítulo IV.

b. Tiempo para el desarrollo

El tiempo total para el desarrollo del proyecto fue de ocho meses, por lo que se programaron las actividades de la metodología, quedando de la siguiente manera:

Nombre de tarea	Duración	Comienzo	Fin	Pred.
SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NTP ISO 27001 Y 27002 Y COBIT	**240 días**	**mié 16/07/14**	**lun 16/03/15**	
Inicio	**14 días**	**mié 16/07/14**	**mar 29/07/14**	
Identificación de metodologías de desarrollo de Sistemas Expertos	**1 día**	**mié 16/07/14**	**mié 16/07/14**	
Identificar metodologías de desarrollo de Sistemas Expertos	1 día	**mié 16/07/14**	mié 16/07/14	
Estudio del proceso	**5 días**	**mié 16/07/14**	**dom 20/07/14**	
Describir el proceso de auditoría de seguridad de la	2 días	mié 16/07/14	jue 17/07/14	

información				
Elaborar mapa de procesos	1 día	vie 18/07/14	vie 18/07/14	6
Realizar análisis del desarrollo del proceso	2 días	sáb 19/07/14	dom 20/07/14	7
Determinación del problema	**4 días**	**lun 21/07/14**	**jue 24/07/14**	
Determinar motivación para el esfuerzo	2 días	lun 21/07/14	mar 22/07/14	8
Identificar problema o problemas candidatos	2 días	lun 21/07/14	mar 22/07/14	8
Realizar estudio de viabilidad	2 días	mié 23/07/14	jue 24/07/14	11
Análisis de Costo/Beneficio	**5 días**	**vie 25/07/14**	**mar 29/07/14**	**9**
Determinar los costos del proyecto	1 día	vie 25/07/14	vie 25/07/14	12
Determinar los beneficios del proyecto	1 día	sáb 26/07/14	sáb 26/07/14	14
Realizar análisis de costo beneficio	2 días	dom 27/07/14	lun 28/07/14	15
Describir el proyecto propuesto	1 día	mar 29/07/14	mar 29/07/14	16
Análisis de requerimientos	**26 días**	**mié 30/07/14**	**dom 24/08/14**	
Determinación de los requisitos del Sistema	**12 días**	**mié 30/07/14**	**dom 10/08/14**	
Elaborar cuestionarios para recopilación de requisitos	3 días	mié 30/07/14	vie 01/08/14	17
Aplicar cuestionarios de recopilación de requisitos	5 días	sáb 02/08/14	mié 06/08/14	20
Analizar información recopilada y definir requerimientos finales	2 días	jue 07/08/14	vie 08/08/14	21
Elaborar diagrama de casos de uso de requerimientos	1 día	sáb 09/08/14	sáb 09/08/14	22
Elaborar el modelo de dominio	1 día	dom 10/08/14	dom 10/08/14	23
Adquisición del conocimiento	**14 días**	**lun 11/08/14**	**dom 24/08/14**	
Identificar fuentes de conocimiento de alimentación del Sistema Experto	1 día	lun 11/08/14	lun 11/08/14	24
Determinar técnicas de recopilación de información	1 día	lun 11/08/14	lun 11/08/14	24
Elaborar instrumentos para las técnicas de recopilación seleccionadas	3 días	mar 12/08/14	jue 14/08/14	27
Aplicar técnicas de recopilación seleccionadas	5 días	vie 15/08/14	mar 19/08/14	28
Organizar y analizar información recopilada	5 días	mié 20/08/14	dom 24/08/14	29
Diseño	**34 días**	**lun 25/08/14**	**sáb 27/09/14**	
Elaborar descripción de los casos de uso de requerimientos	2 días	lun 25/08/14	mar 26/08/14	30
Seleccionar técnica de representación del conocimiento	2 días	mié 27/08/14	jue 28/08/14	32
Seleccionar técnica de control	2 días	mié 27/08/14	jue 28/08/14	32
Elaborar diagrama de secuencia	2 días	vie 29/08/14	sáb 30/08/14	33,34
Elaborar diagrama de clases	2 días	dom 31/08/14	lun 01/09/14	35
Selección de software para el desarrollo del Sistema	**3 días**	**mar 02/09/14**	**jue 04/09/14**	
Prototipo del producto	**23 días**	**vie 05/09/14**	**sáb 27/09/14**	
Realizar prototipación del producto	14 días	vie 05/09/14	jue 18/09/14	39
Presentar prototipos a experto para corrección para su revisión	2 días	vie 19/09/14	sáb 20/09/14	41
Realizar mejoras	7 días	dom 21/09/14	sáb 27/09/14	42
Implementación	**104 días**	**dom 28/09/14**	**vie 09/01/15**	

Elaborar diagrama de componentes	2 días	dom 28/09/14	lun 29/09/14	43
Elaborar diagrama de despliegue	2 días	mar 30/09/14	mié 01/10/14	45
Elaborar diagrama físico de la BD	5 días	jue 02/10/14	lun 06/10/14	46
Construir interfaces del sistema	25 días	mar 07/10/14	vie 31/10/14	47
Desarrollar el producto	70 días	sáb 01/11/14	vie 09/01/15	48
Pruebas	**35 días**	**sáb 10/01/15**	**vie 13/02/15**	
Realizar pruebas del Sistema Experto en un empresa	18 días	sáb 10/01/15	mar 27/01/15	49
Documentar el proceso de prueba	7 días	mié 28/01/15	mar 03/02/15	51
Analizar resultados de la prueba	7 días	mié 04/02/15	mar 10/02/15	52
Comprobar hipótesis	3 días	mié 11/02/15	vie 13/02/15	53
Cierre	**27 días**	**sáb 14/02/15**	**lun 16/03/15**	
Documentar la Tesis	20 días	sáb 14/02/15	jue 05/03/15	54
Escribir Conclusiones y Recomendaciones	7 días	vie 06/03/15	lun 16/03/15	56

Tabla IV.1: Cronograma del proyecto

c. Lenguaje de programación empleado

La estructura del conocimiento del Sistema Experto ha sido diseñada de una forma sencilla basada en preguntas, vulnerabilidades y amenazas declaradas literalmente.

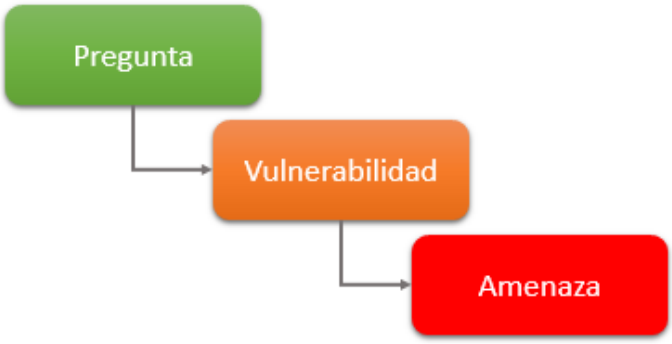


Figura IVI-1: *Estructura del conocimiento del Sistema Experto en Seguridad de la Información Propuesto*

La lógica del sistema radica en lo siguiente: el sistema determina una vulnerabilidad cuando la respuesta a una

pregunta de auditoría es NO y la determinación de vulnerabilidades y amenazas es a través de las relaciones lógicas de la BD.

Se ha consultado con un Experto en Sistemas Expertos sobre cuál sería el mejor lenguaje de programación para el desarrollo de este tipo de Sistemas, dando como resultado la sugerencia de un lenguaje de propósito general si la estructura de la información lo permite. (Anexo Nº 2).

Es por esto y por la simplicidad en su estructura que no ha sido necesario usar un lenguaje de programación lógica sino uno de propósito general como Java, lo cual ha reducido considerablemente los tiempos de desarrollo del Sistema.

d. Beneficios del proyecto

A continuación se listan los beneficios que tendrá el Sistema Experto en Seguridad de la Información:

Productividad mejorada

- **Mejores Decisiones:** En consecuencia de la realización de la auditoría por un Sistema Experto, las decisiones pueden llegar a ser mejores, ya que el Sistema cuenta con reglas establecidas por los expertos auditores en Seguridad de la Información.
- **Decisiones más rápidas:** Optimización en el tiempo de realización de la auditoría y establecimiento de

conclusiones, debido a que la auditoría es soportada por el sistema.

- **Propaga especialización:** El sistema experto de auditoría en seguridad de la información brindará apoyo a personal experto y no experto en la materia.

Costos más bajos

- **Reduce costos de trabajo:** Por concepto de contratación de expertos para ejecutar la auditoría. Debido a que se necesitarán pocas horas de un experto auditor en seguridad de la información.

Calidad mejorada

- **Proporciona entrenamiento:** Los nuevos empleados dedicados a la auditoría de seguridad de la información siempre necesitan una guía, esta será proporcionada por el sistema experto, el cual contará con un fácil manejo, guiado por una metodología para la realización de auditorías.

Imagen mejorada

- **Innovador:** Realización de auditorías basadas en la unificación de normas internacionales para la seguridad de la información (ISO 27001 e ISO 27002) y apoyados en el marco de referencia COBIT 5.

e. Costos de implementación

Para determinar el costo de una auditoría en seguridad de la información tradicional, se consultó con el personal experto, el cual detalló la siguiente tabla:

Concepto	Costo/Unit.	Unidad	Cantidad	Costo (S/.)
Experto en Auditoría de Seguridad de la información	S/. 100,00	Horas	200	20.000,00
Viáticos (ida y vuelta)	S/. 1000	Unid.	1	1.000,00
Alimentación (10 días)	S/. 100	Día	10	1.000,00
Hospedaje (10 días)	S/. 300	Día	10	3.000,00
Total	**-**	**-**	**-**	**S/. 25.000,00**

Tabla IV.2: Gastos generales de la auditoría 1

Concepto	Costo(S/.)/Unidad	Cantidad	Costo (S/.)
Millar de Papel B.	S/. 15,00	1	S/. 15,00
Lapiceros	S/. 1,00	20	S/. 20,00
Impresiones	S/. 0,20	400	S/. 80,00
Sobre Manila	S/. 0,50	30	S/. 15,00
DVD	S/. 1,50	10	S/. 15,00
Total	**-**	**-**	**S/. 145,00**

Tabla IV.3: Costo de materiales empleados 1

Por cuanto, una auditoría tradicional puede significar un costo total de S/.25.145,00 tal como se puede apreciar en el resumen de costos de la Tabla IV.4.

Concepto	Costo (S/.)
Experto en Auditoría de Seguridad de la información	S/. 20.000,00
Viáticos (ida y vuelta)	S/. 1.000,00
Alimentación (20 días)	S/. 2.000,00
Hospedaje	S/. 2.000,00
Materiales	S/. 145,00
Total	**S/. 25.145,00**

Tabla IV.4: Resumen de costos 1

Ahora se describirán los costos en el desarrollo de la auditoría usando el Sistema Experto:

Concepto	Costo/Unit.	Unidad	Cantidad	Costo (S/.)
Experto en Auditoría de Seguridad de la información	S/. 100,00	Horas	80	8.000,00
Viáticos (ida y vuelta)	S/. 1000	Unid.	1	1.000,00
Alimentación	S/. 100	Día	4	400,00
Hospedaje	S/. 300	Día	4	1.200,00
Total	**-**	**-**	**-**	**S/. 10.600,00**

Tabla IV.5: Gastos generales de la auditoría 2

Concepto	Costo(S/.)/Unidad	Cantidad	Costo (S/.)
Millar de Papel Bond	S/. 15,00	0,5	S/. 7,50
Lapiceros	S/. 1,00	2	S/. 2,00
Impresiones	S/. 0,20	500	S/. 100,00
Sobre Manila	S/. 0,50	20	S/. 10,00
DVD	S/. 1,50	10	S/. 15,00
Total	**-**	**-**	**S/. 134,50**

Tabla IV.6: Costos de materiales empleados 2

Por cuanto, una auditoría tradicional desarrollada con el Sistema Experto puede significar un costo total de S/.10.734,50 tal como se puede apreciar en el resumen de costos de la Tabla IV.7.

Concepto	Costo (S/.)
Experto en Auditoría de Seguridad de la información	S/. 8.000,00
Viáticos (ida y vuelta)	S/. 1.000,00
Alimentación (1 días)	S/. 400,00
Hospedaje (1 días)	S/. 1200,00
Materiales	S/. 134,50
Total	**S/. 10.734,50**

Tabla IV.7: Resumen de costos 2

Por lo tanto, una auditoría tradicional puede significar un costo total de S/.25.145,00 (Tabla IV.4), comparado con los costos haciendo uso del Sistema Experto, S/.10,734.50 (Tabla IV.7), se puede apreciar una reducción del costo en S/.14,410.50 (Tabla IV.8).

Concepto	Costos 1	Costos 2
Experto en Auditoría	S/. 20.000,00	S/. 8.000,00
Viáticos (ida y vuelta)	S/. 1.000,00	S/. 1.000,00
Alimentación	S/. 2.000,00	S/. 400,00
Hospedaje	S/. 2.000,00	S/.1200,00
Materiales	S/. 145,00	S/. 134,50
Total	**S/. 25.145,00**	**S/. 10.734,50**
Horas empleados	**200**	**80**
Total reducción	**S/. 14.410,50**	

Tabla IV.8: Comparación de costos 1 y 2

4.1.3 Descripción del proyecto propuesto

Se propone el desarrollo de un Sistema Experto en Seguridad de la Información, desarrollado bajo los Criterios de Auditoría NTP ISO 27001:2008 e ISO 27002:2009, combinado con las buenas prácticas de COBIT 5, y el conocimiento propio de expertos en auditoría informática.

El Sistema Experto denominado "XSIS", por sus siglas en inglés: eXpert System for Information Security, es un sistema desarrollado bajo tecnologías libres web cuyo objetivo es dar soporte al proceso de auditoría, identificar vulnerabilidades y amenazas y crear informes de Auditoría basado en la evaluación de los controles del Sistema de Gestión de Seguridad de la Información.

Si el uso del sistema es interno, el SE permitirá a la organización anticiparse a un proceso posterior de auditoría e identificará vulnerabilidades y amenazas de los activos de información con la finalidad que la organización pueda tomar las medidas correctivas necesarias que mejoren la gestión de la información y generen valor a través de las tecnologías de información.

El SE puede ser usado por personal experto y no experto auditoría informática, es intuitivo y los mecanismos de evaluación han sido diseñados en formatos de verificación; asimismo el SE es un sistema de apoyo al auditor tradicional pues brinda soporte al proceso de evaluación y verificación de la auditoría, siendo esta, mecánica y susceptible de automatización, permitiendo el ahorro de tiempo y recursos al disminuir los días empleados y costos asociados, enfocando el esfuerzo en tareas específicas que el auditor considere pertinentes.

4.1.4 Adaptar una metodología para el desarrollo del SE

Luego de la revisión de algunas metodologías, se establecieron lineamientos según las necesidades del proyecto que permitan escoger la metodología más adecuada para el desarrollo de Sistema Experto, estos se representan con la letra "L" y tienen asociado un puntaje según su nivel de impacto.

a. L1: Información bibliográfica (autor(es), año de publicación, etc.)

Nivel de impacto	Puntaje
No existe información	0
Escasa información	1
Suficiente información	2
Buena información	3

Tabla IV.9: Descripción del lineamiento L1

b. L2: Disponibilidad de información detallada y viable

Nivel de impacto	Puntaje
No existe información	0
Escasa información	1
Suficiente información	2
Buena información	3

Tabla IV.10: Descripción del lineamiento L2

c. L3: Enfocada más en los beneficios que en otros aspectos

Nivel de impacto	Puntaje
Imposible	0
Forzadamente posible	1
Posible	2

Tabla IV.11: Descripción del lineamiento L3

d. L4: Adaptable a los objetivos y tiempos del proyecto

Nivel de impacto	Puntaje
Imposible	0
Forzadamente posible	1
Posible	2

Tabla IV.12: Descripción del lineamiento L4

Es así como se procede con el siguiente cuadro para evaluar las metodologías previamente investigadas y asignarles puntajes, según los criterios fijados. La metodología que obtenga el mayor puntaje será aquella que se considerará como base para ser ajustada al proyecto de Tesis.

Metodología - Criterios	L1	L2	L3	L4	TOTAL
Blanqué y García Martínez	1	1	0	1	**3**
Brulé	1	1	1	2	**5**
Buchanan	1	2	1	1	**5**
CommonKADS	2	3	1	0	**6**
González - Dankel	1	1	1	2	**5**
Grover	1	1	0	1	**3**
I.D.E.A.L.	2	2	2	1	**7**
John Durkin	2	2	2	2	**8**
M.I.K.E.	1	1	1	1	**4**
Weiss y Kulikowski	2	1	2	1	**6**

Tabla IV.13: Matriz de evaluación de metodologías

Por el resultado de la evaluación, se escoge como metodología base de desarrollo la propuesta por **John Durkin,** a la cual le fueron añadidas o modificadas etapas del ciclo de vida y artefactos de ingeniería, quedando estructurada de la siguiente forma:

a. Fase de Inicio

Esta fase está conformada por 3 actividades:

- Estudio del Proceso, extraída de la metodología J. Durkin.
- Determinar el Problema, extraída de la metodología J. Durkin.
- Análisis de Costo/Beneficio, extraída de la metodología J. Durkin.

b. Fase de Análisis de Requisitos

- Determinación de los requisitos del Sistema, extraída de la metodología ICONIX.
- Adquisición del conocimiento, extraída de la metodología J. Durkin.

c. Fase de Diseño:

- Elaborar descripción de los casos de uso de Requerimientos, extraída de la metodología ICONIX.

- Seleccionar técnica de representación del conocimiento, extraída de la metodología J. Durkin.
- Seleccionar técnica de control, extraída de la metodología J. Durkin.
- Elaborar diagrama de secuencia, extraída de la metodología ICONIX.
- Elaborar diagrama de clases, extraída de la metodología ICONIX.
- Selección de software para el desarrollo de Sistema, extraída de la metodología J. Durkin.
- Prototipo de Producto, extraída de la metodología ICONIX.

d. Fase de Implementación:

- Elaborar diagrama de componentes, extraída de la metodología ICONIX.
- Elaborar diagrama de despliegue, extraída de la metodología ICONIX.
- Elaborar diagrama físico de la BD, extraída de la metodología ICONIX.
- Construir interfaces del Sistema, extraída de la metodología ICONIX.
- Desarrollo del producto, extraída de la metodología ICONIX.

e. Fase de Pruebas:

- Realizar pruebas de Sistema Experto en una empresa, extraída de la metodología J. Durkin.

- Documentar el proceso de prueba, extraída de la metodología J. Durkin.
- Analizar resultados de la prueba, extraída de la metodología J. Durkin.
- Comprobar hipótesis.

f. Fase de Cierre:

- Documentar la Tesis.
- Escribir Conclusiones y Recomendaciones.

4.2 Análisis de Requisitos

4.2.1 Lista de fuentes de alimentación de conocimiento del Sistema Experto

La siguiente lista de fuentes de alimentación de conocimiento del Sistema fue producto del asesoramiento del personal Experto en Seguridad de la Información y responden a los siguientes criterios para su selección:

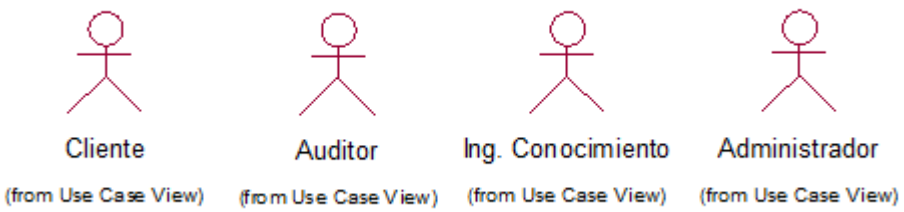
a. Criterios de Auditoría generalmente usados para Auditorías de Seguridad de la Información para entidades públicas.
b. Criterios de Auditoría generalmente usados para Auditorías de Seguridad de la Información para entidades privadas.
c. Lineamientos del ámbito legal peruano para Seguridad de la Información.
d. Experticia en el desarrollo de Auditorías de Seguridad de la Información.

Quedado la lista conformada por las siguientes fuentes de conocimiento:

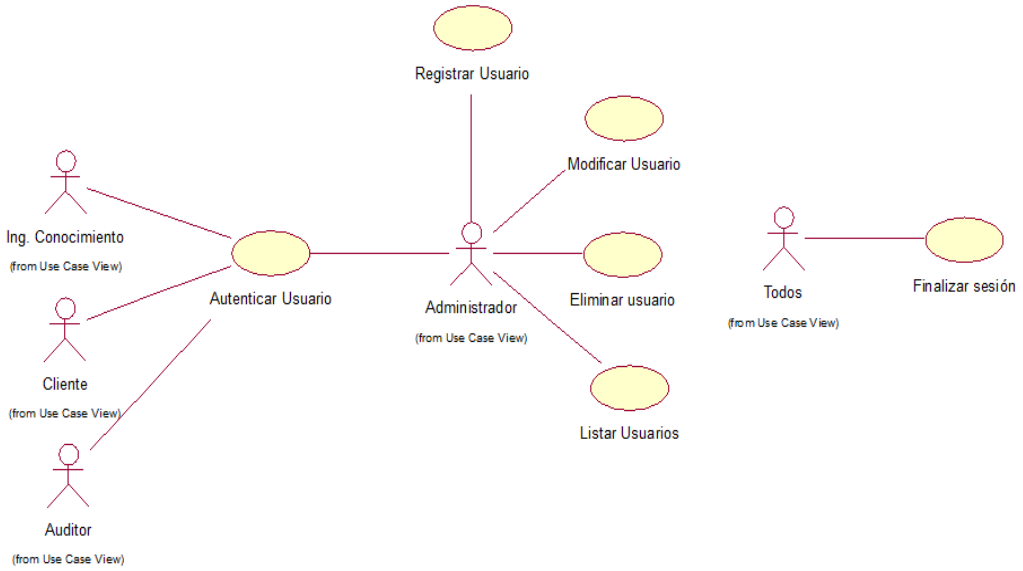
- NTP ISO 27001:2013
- NTP ISO 27002:2013
- COBIT 5
- Conocimiento propio de personal Experto.

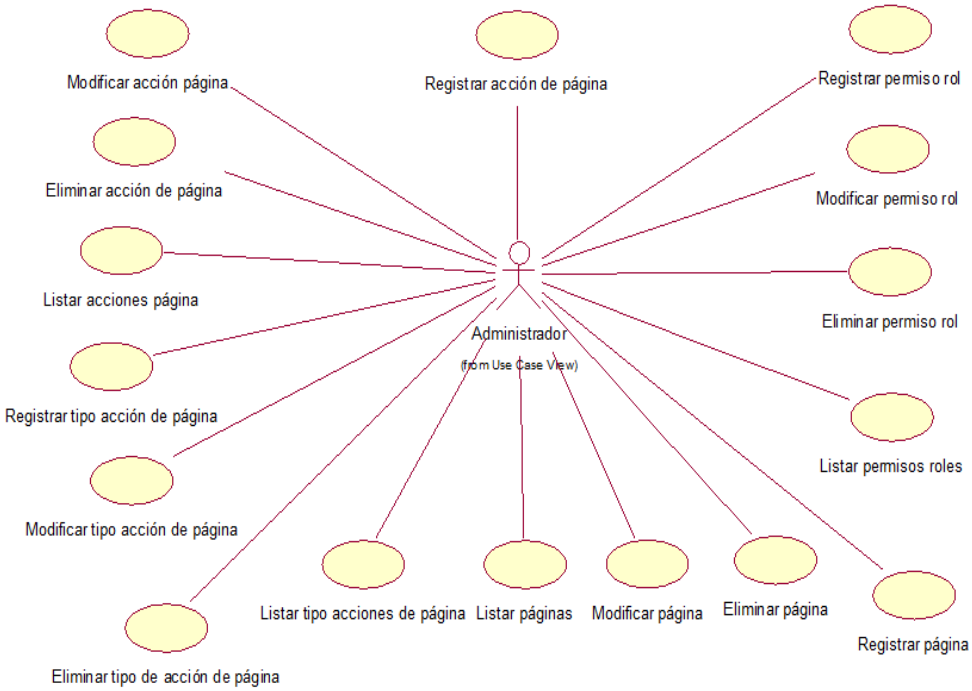
4.2.2 Diagrama de Casos de Uso

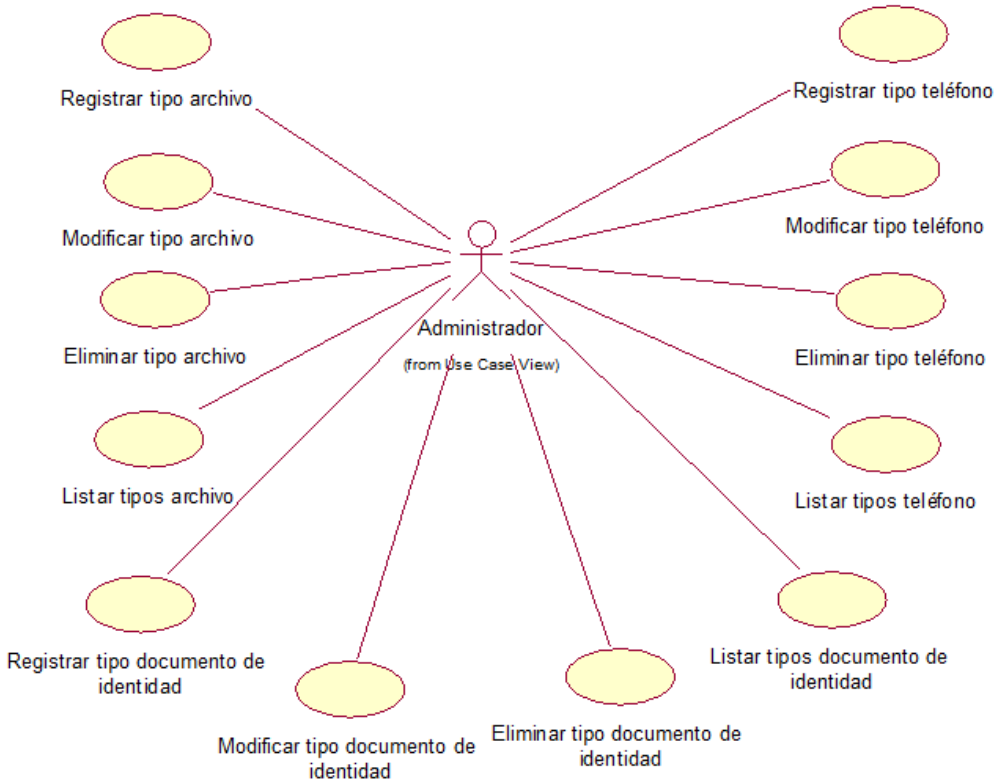
Actores

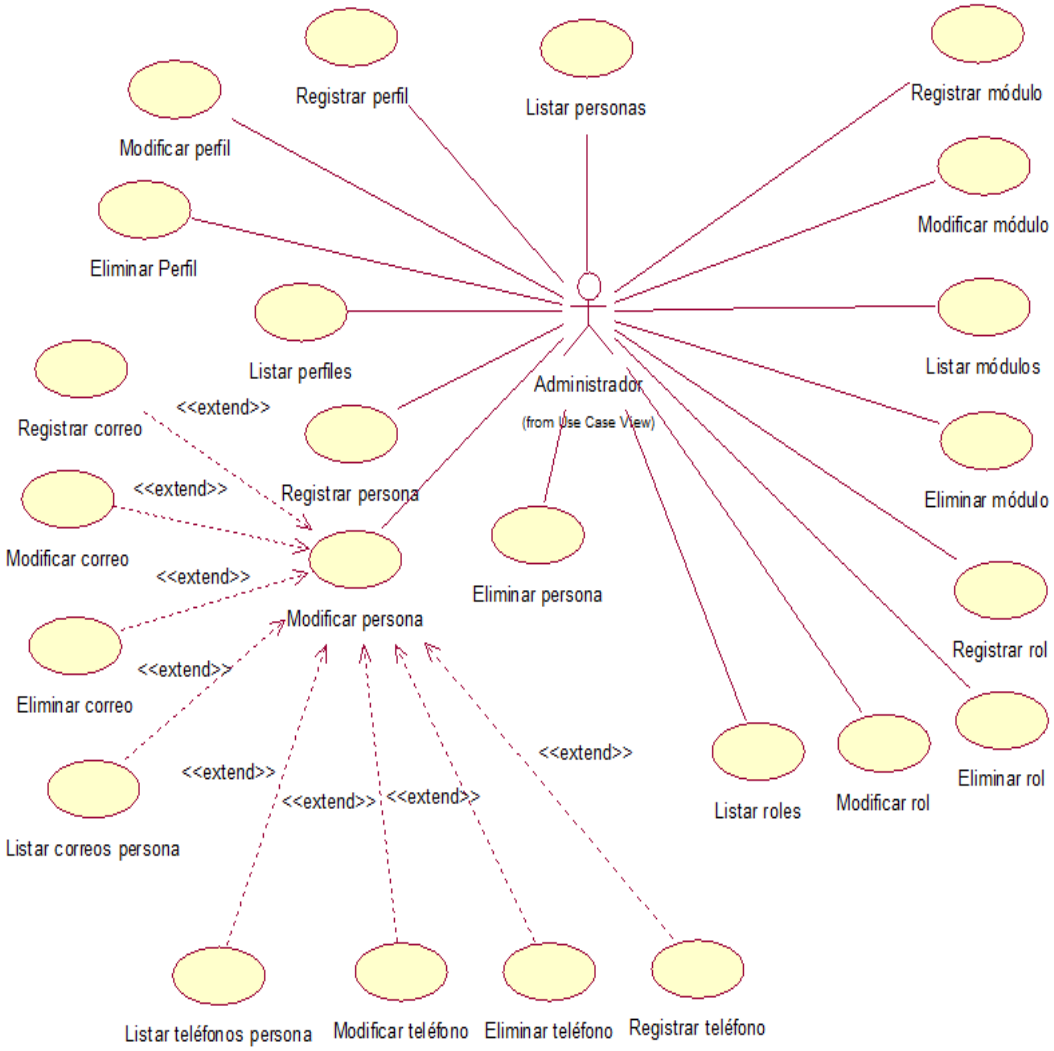


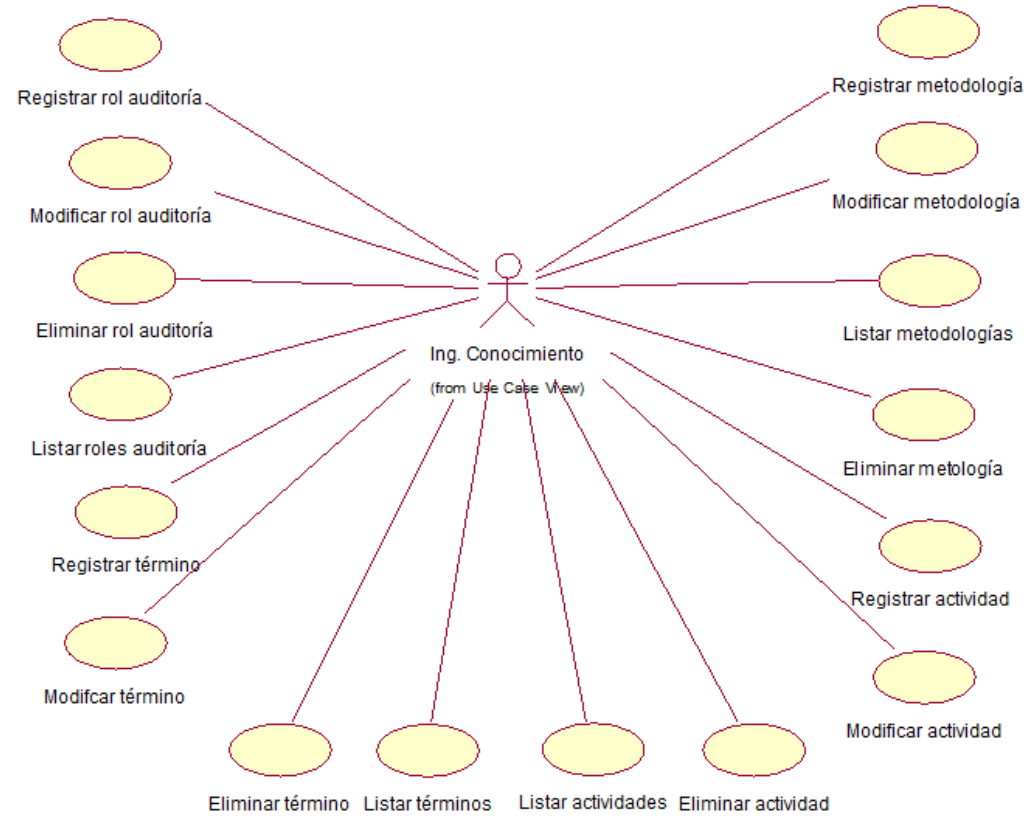
Diagramas

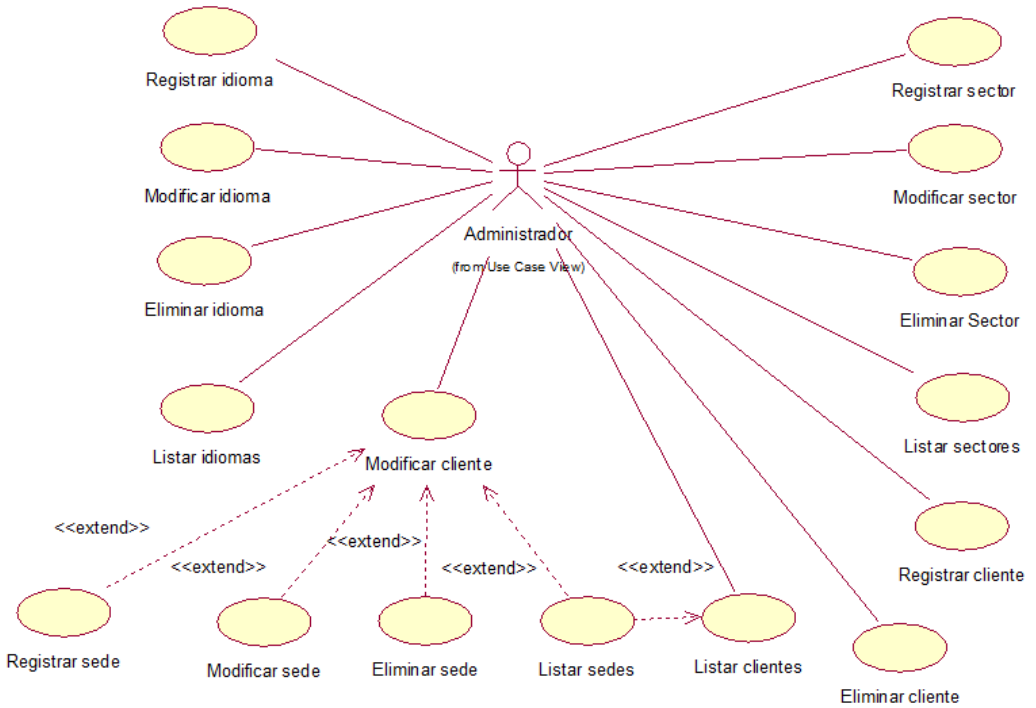


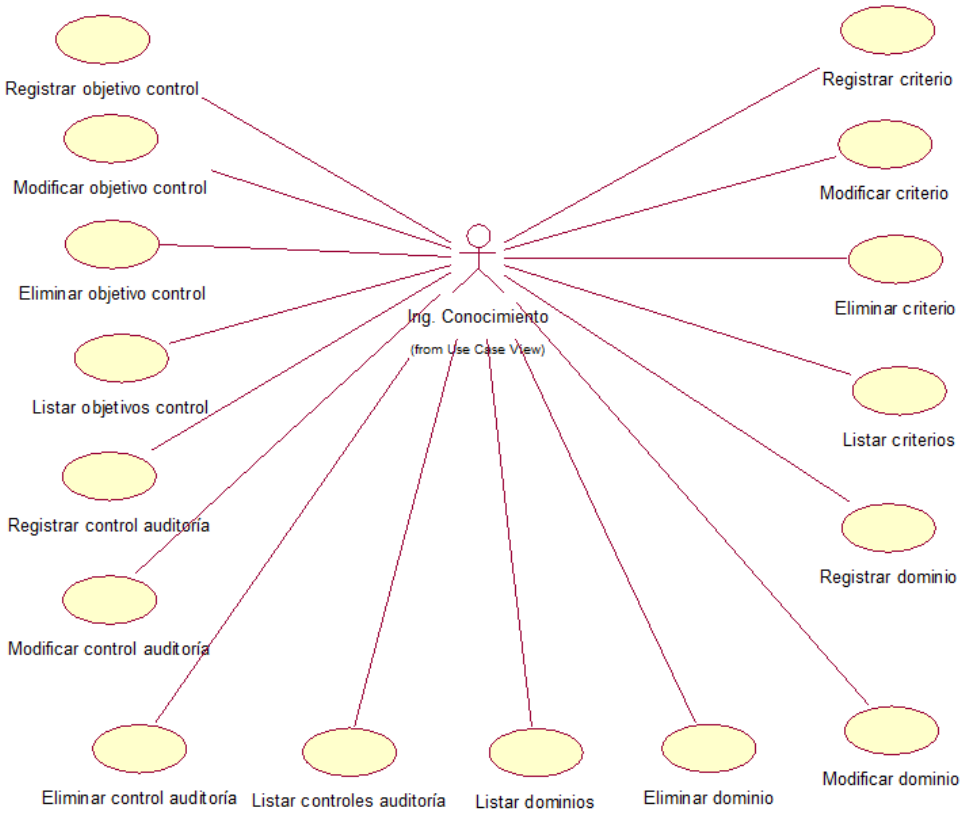

Modificar acción página
Registrar acción de página
Registrar permiso rol
Eliminar acción de página
Modificar permiso rol
Listar acciones página
Eliminar permiso rol
Administrador
(from Use Case View)
Registrar tipo acción de página
Listar permisos roles
Modificar tipo acción de página
Listar tipo acciones de página
Listar páginas
Modificar página
Eliminar página
Registrar página
Eliminar tipo de acción de página

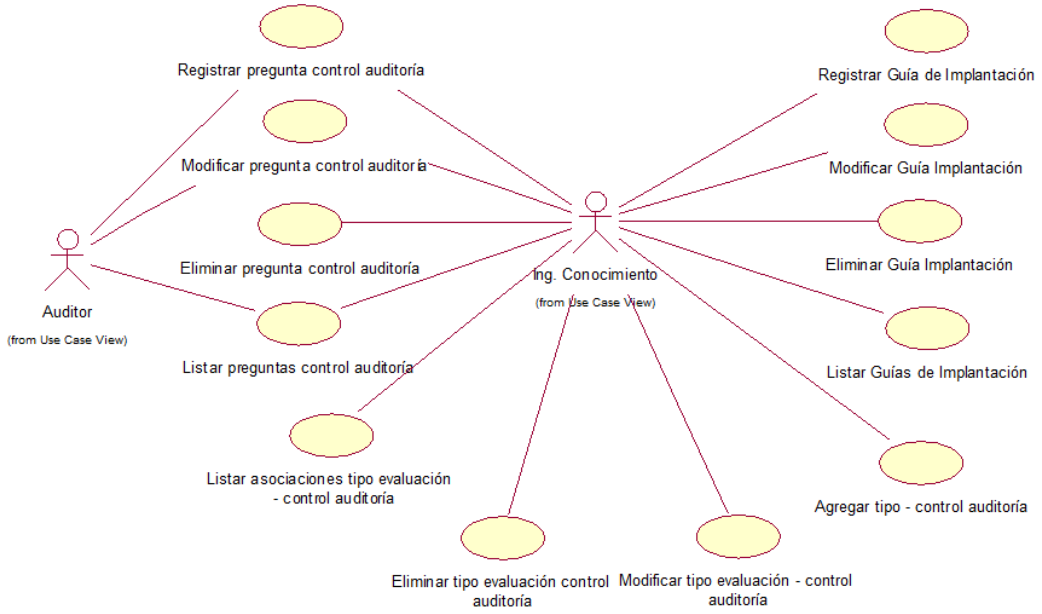

Registrar tipo archivo
Registrar tipo teléfono
Modificar tipo archivo
Modificar tipo teléfono
Administrador
(from Use Case View)
Eliminar tipo archivo
Eliminar tipo teléfono
Listar tipos archivo
Listar tipos teléfono
Registrar tipo documento de identidad
Listar tipos documento de identidad
Modificar tipo documento de identidad
Eliminar tipo documento de identidad

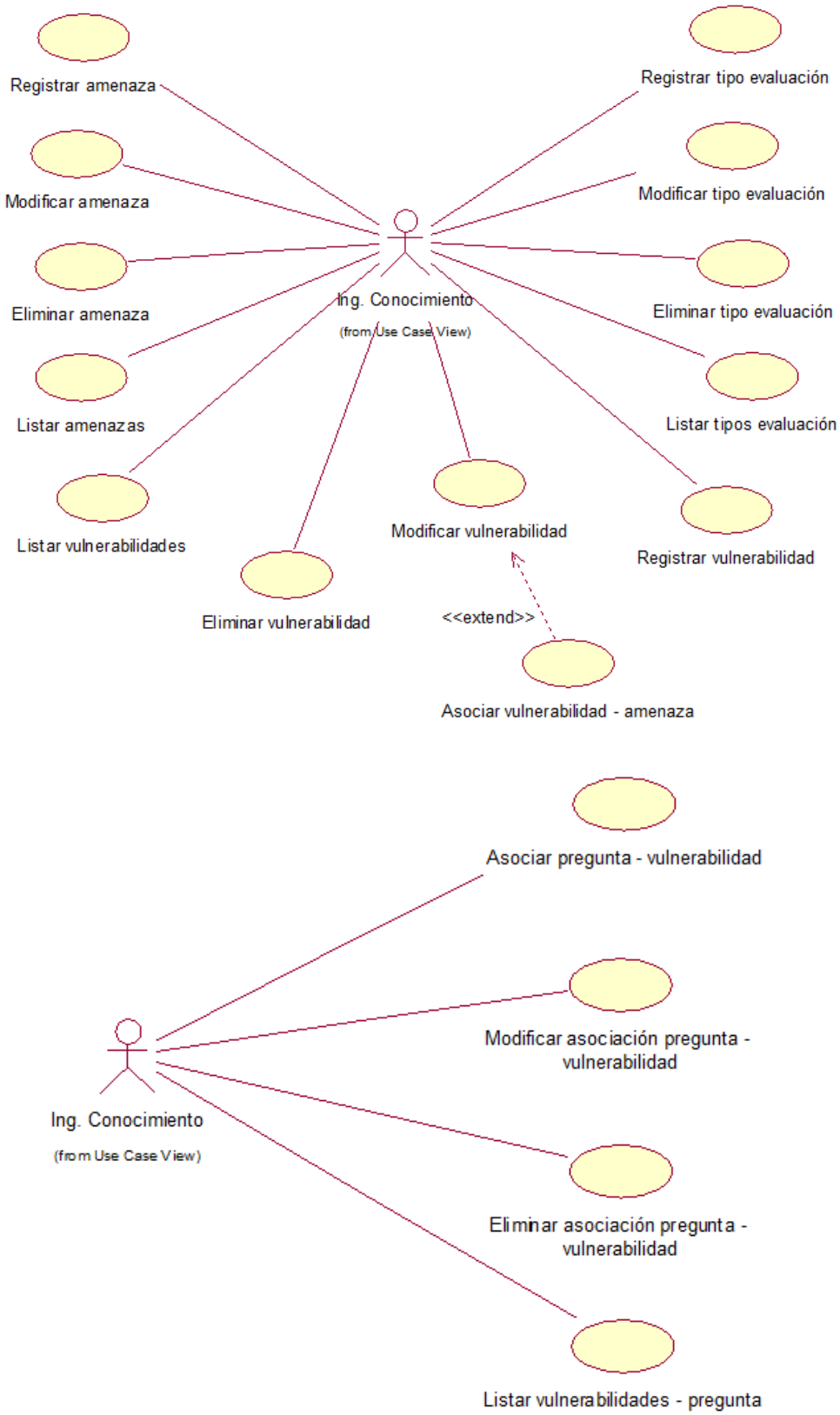

Registrar perfil
Listar personas
Registrar módulo
Modificar perfil
Modificar módulo
Eliminar Perfil
Listar perfiles
Listar módulos
Administrador
(from Use Case View)
Registrar correo
<<extend>>
Registrar persona
Eliminar módulo
<<extend>>
Modificar correo
Eliminar persona
<<extend>>
Modificar persona
Registrar rol
Eliminar correo
<<extend>>
Eliminar rol
<<extend>>
<<extend>>
Listar roles
Modificar rol
Listar correos persona
<<extend>>
<<extend>>
Listar teléfonos persona
Modificar teléfono
Eliminar teléfono
Registrar teléfono


Registrar rol auditoría
Modificar rol auditoría
Eliminar rol auditoría
Listar roles auditoría
Registrar término
Modifcar término
Registrar metodología
Modificar metodología
Listar metodologías
Eliminar metología
Registrar actividad
Modificar actividad
Ing. Conocimiento
(from Use Case View)
Eliminar término
Listar términos
Listar actividades
Eliminar actividad

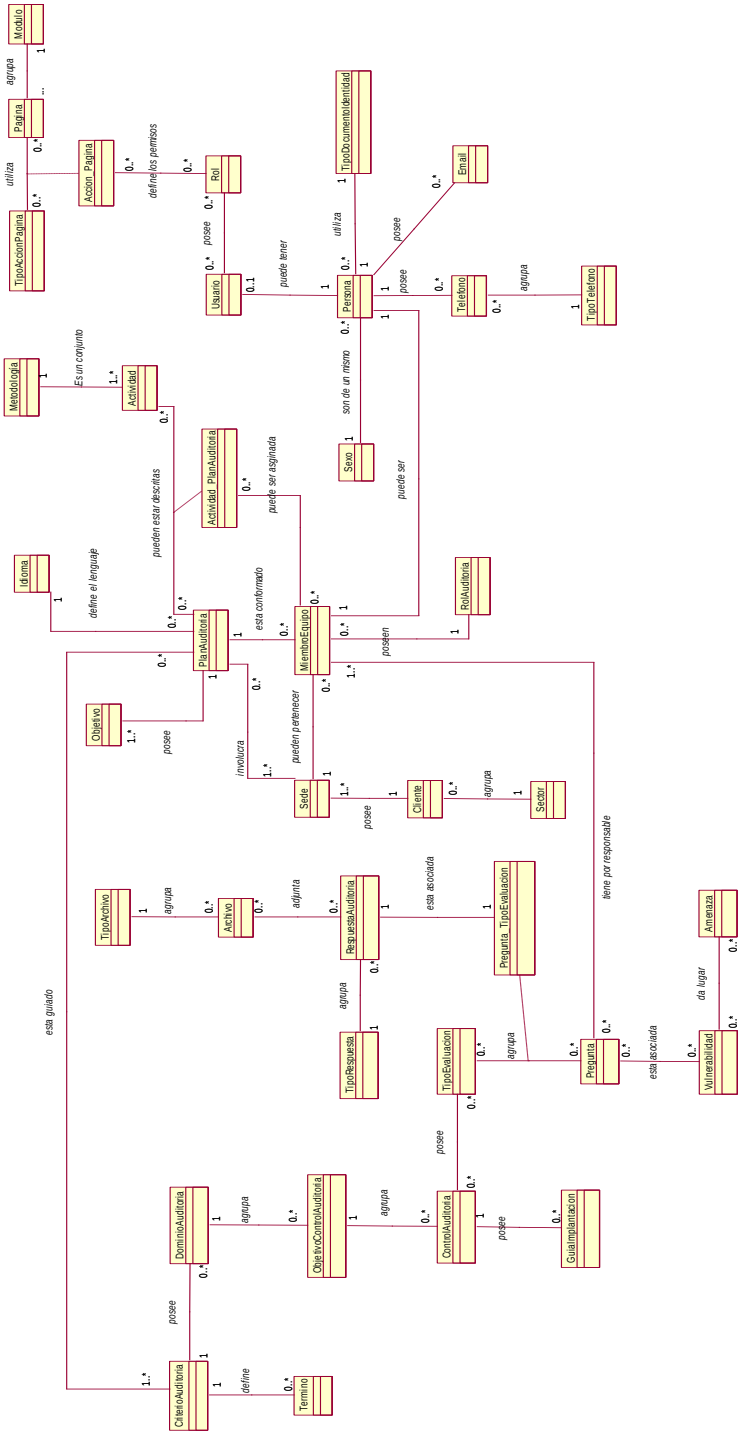

Registrar idioma
Modificar idioma
Eliminar idioma
Listar idiomas
Registrar sector
Modificar sector
Eliminar Sector
Listar sectores
Registrar cliente
Eliminar cliente
Administrador
(from Use Case View)
Modificar cliente
<<extend>>
<<extend>>
<<extend>>
<<extend>>
<<extend>>
Registrar sede
Modificar sede
Eliminar sede
Listar sedes
Listar clientes


Registrar objetivo control
Modificar objetivo control
Eliminar objetivo control
Listar objetivos control
Registrar control auditoría
Modificar control auditoría
Eliminar control auditoría
Listar controles auditoría
Listar dominios
Eliminar dominio
Modificar dominio
Registrar dominio
Listar criterios
Eliminar criterio
Modificar criterio
Registrar criterio
Ing. Conocimiento
(from Use Case View)


Registrar pregunta control auditoría
Modificar pregunta control auditoría
Eliminar pregunta control auditoría
Listar preguntas control auditoría
Listar asociaciones tipo evaluación - control auditoría
Eliminar tipo evaluación control auditoría
Modificar tipo evaluación - control auditoría
Agregar tipo - control auditoría
Listar Guías de Implantación
Eliminar Guía Implantación
Modificar Guía Implantación
Registrar Guía de Implantación
Auditor
(from Use Case View)
Ing. Conocimiento
(from Use Case View)


Registrar amenaza
Modificar amenaza
Eliminar amenaza
Listar amenazas
Listar vulnerabilidades
Eliminar vulnerabilidad
Modificar vulnerabilidad
<<extend>>
Asociar vulnerabilidad - amenaza
Registrar vulnerabilidad
Registrar tipo evaluación
Modificar tipo evaluación
Eliminar tipo evaluación
Listar tipos evaluación
Ing. Conocimiento
(from Use Case View)
Asociar pregunta - vulnerabilidad
Modificar asociación pregunta - vulnerabilidad
Eliminar asociación pregunta - vulnerabilidad
Listar vulnerabilidades - pregunta
Ing. Conocimiento
(from Use Case View)

4.2.3 Modelo de Dominio



4.3 Diseño

4.3.1 Descripción de Casos de Uso

A continuación se describirán los principales casos de uso.

Módulo de Base de Conocimiento

a. Metodología

- **Registrar metodología**

Número	:	67
Caso de Uso	:	Registrar metodología
Actor	:	Ing. Conocimiento
Descripción	:	Permite el registro de una nueva metodología para el desarrollo de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Nombre. b. Descripción. c. Autor. 2. Listar metodologías.
Flujo alternativo	:	Ninguno.
Post Condición	:	Metodología registrada.

- **Modificar metodología**

Número	:	68
Caso de Uso	:	Modificar metodología
Actor	:	Ing. Conocimiento
Descripción	:	Permite modificar el registro de metodología.
Pre Condición	:	Metodología registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Nombre.

		b. Descripción. c. Autor. 2. Listar metodologías.
Flujo alternativo	:	Ninguno.
Post Condición	:	Metodología modificada.

- **Eliminar metodología**

Número	:	69
Caso de Uso	:	Eliminar metodología.
Actor	:	Ing. Conocimiento
Descripción	:	Permite eliminar una metodología registrada.
Pre Condición	:	Metodología registrada.
Flujo de eventos	:	1. Eliminar metodología.
Flujo alternativo	:	Ninguno.
Post Condición	:	Metodología eliminada.

- **Listar metodologías**

Número	:	70
Caso de Uso	:	Listar metodologías.
Actor	:	Ing. Conocimiento
Descripción	:	Lista metodologías.
Pre Condición	:	Ninguna.
Flujo de eventos	:	2. Listar metodología.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

b. Roles auditoría

- **Registrar rol auditoría**

Número	:	75
Caso de Uso	:	Registrar rol auditoría
Actor	:	Administrador
Descripción	:	Permite el registro de un rol (papel dentro de la auditoría).
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Descripción. 2. Listar roles auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Rol auditoría registrado.

- **Modificar rol auditoría**

Número	:	76
Caso de Uso	:	Modificar rol auditoría
Actor	:	Administrador
Descripción	:	Permite la modificación de un rol auditoría registrada.
Pre Condición	:	Rol auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Descripción. 2. Listar roles auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Rol auditoría modificado.

- **Eliminar rol auditoría**

Número	:	77
Caso de Uso	:	Eliminar rol auditoría
Actor	:	Administrador
Descripción	:	Permite eliminar un rol de auditoría registrado.
Pre Condición	:	Rol auditoría registrado.
Flujo de eventos	:	1. Eliminar rol auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Rol auditoría eliminado.

- **Listar roles auditoría**

Número	:	78
Caso de Uso	:	Listar roles auditoría
Actor	:	Administrador
Descripción	:	Lista roles auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	2. Listar roles auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

c. Criterios

- **Registrar criterio**

Número	:	83
Caso de Uso	:	Registrar criterio.
Actor	:	Ing. Conocimiento.

Descripción	:	Permite registrar criterios de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Nombre. b. Descripción. 2. Listar términos.
Flujo alternativo	:	Ninguno.
Post Condición	:	Criterio registrado.

- **Modificar criterio**

Número	:	84
Caso de Uso	:	Modificar criterio.
Actor	:	Ing. Conocimiento.
Descripción	:	Criterio registrado
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Nombre. b. Descripción. 2. Listar criterios.
Flujo alternativo	:	Ninguno.
Post Condición	:	Criterio modificado.

- **Eliminar criterio**

Número	:	85
Caso de Uso	:	Eliminar criterio.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite eliminar un criterio registrado.
Pre Condición	:	Criterio registrado.

Flujo de eventos	:	1. Eliminar criterio.
Flujo alternativo	:	Ninguno.
Post Condición	:	Criterio eliminado.

- **Listar criterios**

Número	:	86
Caso de Uso	:	Listar criterios.
Actor	:	Ing. Conocimiento.
Descripción	:	Lista criterios de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	2. Listar criterios.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

d. Dominios

- **Registrar dominio**

Número	:	87
Caso de Uso	:	Registrar dominio
Actor	:	Ing. Conocimiento.
Descripción	:	Permite registrar dominios de auditoría.
Pre Condición	:	Criterio registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Criterio de auditoría. b. Código. c. Nombre 2. Listar dominios.
Flujo alternativo	:	Ninguno.

Post Condición	:	Dominio registrado.

- **Modificar dominio**

Número	:	88
Caso de Uso	:	Modificar dominio
Actor	:	Ing. Conocimiento.
Descripción	:	Permite modificar dominios de auditoría registrados.
Pre Condición	:	Criterio registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Criterio de auditoría. b. Código. c. Nombre 2. Listar dominios.
Flujo alternativo	:	Ninguno.
Post Condición	:	Dominio modificado.

- **Eliminar dominio**

Número	:	89
Caso de Uso	:	Eliminar dominio.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite eliminar un dominio registrado.
Pre Condición	:	Dominio registrado.
Flujo de eventos	:	1. Eliminar dominio.
Flujo alternativo	:	Ninguno.
Post Condición	:	Dominio eliminado.

- **Listar dominios**

Número	:	90
Caso de Uso	:	Listar dominios.
Actor	:	Ing. Conocimiento.
Descripción	:	Lista dominios de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	2. Listar dominios.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

e. Objetivos de control de auditoría

- **Registrar objetivo de control**

Número	:	91
Caso de Uso	:	Registrar objetivo de control
Actor	:	Ing. Conocimiento.
Descripción	:	Permite registrar objetivos de control de auditoría.
Pre Condición	:	Dominio de auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Dominio de auditoría. b. Código. c. Nombre. d. Descripción. 2. Listar objetivos de control.
Flujo alternativo	:	Ninguno.
Post Condición	:	Objetivo de control registrado.

- **Modificar objetivo de control**

Número	:	92
Caso de Uso	:	Modificar objetivo de control
Actor	:	Ing. Conocimiento.
Descripción	:	Permite modificar objetivos de control registrados.
Pre Condición	:	Objetivo de control registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Dominio de auditoría. b. Código. c. Nombre. d. Descripción. 2. Listar objetivos de control.
Flujo alternativo	:	Ninguno.
Post Condición	:	Objetivo de control modificado.

- **Eliminar objetivo de control**

Número	:	93
Caso de Uso	:	Eliminar objetivo de control.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite eliminar un objetivo de control registrado.
Pre Condición	:	Objetivo de control registrado.
Flujo de eventos	:	1. Eliminar objetivo de control.
Flujo alternativo	:	Ninguno.
Post Condición	:	Objetivo de control eliminado.

- **Listar objetivos de control**

Número	:	94
Caso de Uso	:	Listar objetivos de control.
Actor	:	Ing. Conocimiento.
Descripción	:	Lista objetivos de control.
Pre Condición	:	Ninguna.
Flujo de eventos	:	2. Listar objetivos de control.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

f. Control de Auditoría

- **Registrar Control Auditoría**

Número	:	95
Caso de Uso	:	Registrar Control Auditoría.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite registrar controles de auditoría.
Pre Condición	:	Objetivo de control registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Objetivo de control. b. Código. c. Nombre. d. Descripción. e. Información adicional. 2. Listar controles de auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Control de auditoría registrado.

- **Modificar control de Auditoría**

Número	:	96
Caso de Uso	:	Modificar control de auditoría.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite modificar registro de controles de auditoría.
Pre Condición	:	Control de auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Objetivo de control. b. Código. c. Nombre. d. Descripción. e. Información adicional. 2. Listar controles de auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Control de auditoría modificado.

- **Eliminar Control de Auditoría**

Número	:	97
Caso de Uso	:	Eliminar Control de auditoría.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite eliminar un Control de Auditoría registrado.
Pre Condición	:	Control Auditoría registrado.
Flujo de eventos	:	1. Eliminar Control de auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Control de Auditoría eliminado.

- **Listar controles de Auditoría**

Número	:	98
Caso de Uso	:	Listar controles de auditoría.
Actor	:	Ing. Conocimiento.
Descripción	:	Lista controles de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	2. Listar controles de auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

g. Guía de Implantación

- **Registrar guía de implantación**

Número	:	99
Caso de Uso	:	Registrar guía de implantación.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite registrar la guía de implantación de un control de auditoría.
Pre Condición	:	Control de auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Guía de implantación. 2. Listar guía de implantación.
Flujo alternativo	:	Ninguno.
Post Condición	:	Guía de implantación registrada.

- **Modificar guía de implantación**

Número	:	100
Caso de Uso	:	Modificar guía de implantación.
Actor	:	Ing. Conocimiento.
Descripción	:	Permite modificar las guías de implantación registradas.
Pre Condición	:	Guía de implantación registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Guía de implantación. 2. Listar guía de implantación.
Flujo alternativo	:	Ninguno.
Post Condición	:	Guía de implantación modificada.

- **Eliminar guía de implantación**

Número	:	101
Caso de Uso	:	Ing. Conocimiento.
Actor	:	Administrador.
Descripción	:	Permite eliminar las guías de implantación registradas.
Pre Condición	:	Guía de implantación registrada.
Flujo de eventos	:	1. Eliminar guía de implantación.
Flujo alternativo	:	Ninguno.
Post Condición	:	Guía de implantación eliminada.

- **Listar guías de implantación**

Número	:	102
Caso de Uso	:	Listar guías de implantación.

Actor	:	Ing. Conocimiento.
Descripción	:	Lista guías de implantación.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar guías de implantación.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

h. Pregunta – Tipo Evaluación

- **Agregar tipo de evaluación - pregunta**

Número	:	103
Caso de Uso	:	Agregar tipo de evaluación - pregunta
Actor	:	Ing. Conocimiento
Descripción	:	Permite asociar los tipos de evaluaciones que tiene una pregunta.
Pre Condición	:	Pregunta registrada.
Flujo de eventos	:	1. Validar datos enviados: a. Requerimiento. b. Tipo de evaluación. 2. Listar tipos de evaluaciones asociadas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Pregunta. – Tipo Evaluación registrada.

- **Modificar tipo de evaluación - pregunta**

Número	:	104
Caso de Uso	:	Modificar tipo de evaluación - pregunta
Actor	:	Ing. Conocimiento
Descripción	:	Permite modificar las asociaciones tipo de evaluación

		– pregunta registradas
Pre Condición	:	Asociación Tipo Evaluación - Pregunta registrada.
Flujo de eventos	:	1. Validar datos enviados: a. Requerimiento. b. Tipo de evaluación. 2. Listar tipos de evaluaciones asociadas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Pregunta. – Tipo Evaluación modificada.

- **Eliminar tipo de evaluación - pregunta**

Número	:	105
Caso de Uso	:	Eliminar tipo de evaluación – pregunta.
Actor	:	Ing. Conocimiento
Descripción	:	Permite eliminar las asociaciones entre tipo de evaluación – pregunta.
Pre Condición	:	Asociación Tipo Evaluación - Pregunta registrada.
Flujo de eventos	:	1. Eliminar asociación Tipo evaluación – Pregunta.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación Tipo evaluación – Pregunta eliminada.

- **Listar tipo de evaluación - pregunta**

Número	:	106
Caso de Uso	:	Listar asociaciones tipo de evaluación - pregunta.
Actor	:	Ing. Conocimiento.
Descripción	:	Lista asociaciones tipo de evaluación - pregunta registradas.
Pre Condición	:	Ninguna.

Flujo de eventos	:	1. Listar asociaciones tipo de evaluación - pregunta.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

i. Pregunta – control auditoría

- **Registrar pregunta control auditoría**

Número	:	107
Caso de Uso	:	Registrar pregunta control auditoría.
Actor	:	Ing. Conocimiento / Auditor
Descripción	:	Permite registrar preguntas de evaluación de los controles de auditoría.
Pre Condición	:	Control de auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Peso de ítem. b. Código. c. Pregunta. d. Observación. e. Recomendación. 2. Listar preguntas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Pregunta registrada.

- **Modificar pregunta control auditoría**

Número	:	108
Caso de Uso	:	Modificar pregunta control auditoría.
Actor	:	Ing. Conocimiento / Auditor
Descripción	:	Permite modificar preguntas de auditoría registradas.
Pre Condición	:	Pregunta registrada.

Flujo de eventos	:	1. Validar datos enviados. a. Peso de ítem. b. Código. c. Pregunta. d. Observación. e. Recomendación. 2. Listar preguntas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Pregunta modificada.

- **Eliminar pregunta control auditoría**

Número	:	109
Caso de Uso	:	Eliminar pregunta control auditoría.
Actor	:	Ing. Conocimiento
Descripción	:	Permite eliminar preguntas de auditoría registradas. Para el rol de auditor solo puede eliminarse preguntas registradas por el mismo.
Pre Condición	:	Pregunta registrada.
Flujo de eventos	:	1. Eliminar pregunta auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Pregunta eliminada.

- **Listar preguntas control auditoría**

Número	:	110
Caso de Uso	:	Listar preguntas control auditoría.
Actor	:	Ing. Conocimiento / Auditor.
Descripción	:	Lista preguntas auditoría.
Pre Condición	:	Ninguna.

Flujo de eventos	:	1. Listar preguntas control auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

j. Pregunta - Vulnerabilidad

- **Asociar pregunta - vulnerabilidad**

Número	:	111
Caso de Uso	:	Asociar pregunta - vulnerabilidad.
Actor	:	Ing. Conocimiento
Descripción	:	Permite asociar vulnerabilidades registradas a una pregunta.
Pre Condición	:	Vulnerabilidad registrada. Pregunta registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Vulnerabilidad. 2. Listar vulnerabilidades.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación pregunta – vulnerabilidad registrada.

- **Modificar asociación pregunta – vuln.**

Número	:	112
Caso de Uso	:	Modificar pregunta- vulnerabilidad.
Actor	:	Ing. Conocimiento
Descripción	:	Permite modificar una asociación pregunta-vulnerabilidad registrada.
Pre Condición	:	Asociación pregunta – vulnerabilidad registrada.

Flujo de eventos	:	1. Validar datos enviados. a. Vulnerabilidad. 2. Listar vulnerabilidades.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación pregunta – vulnerabilidad modificada.

- **Eliminar asociación pregunta - vulnerabilidad**

Número	:	113
Caso de Uso	:	Eliminar asociación pregunta – vulnerabilidad.
Actor	:	Ing. Conocimiento
Descripción	:	Permite eliminar una asociación pregunta-vulnerabilidad registrada.
Pre Condición	:	Asociación pregunta – vulnerabilidad registrada.
Flujo de eventos	:	1. Eliminar asociación pregunta - vulnerabilidad. 2. Listar vulnerabilidades.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación pregunta – vulnerabilidad eliminada.

- **Listar vulnerabilidades - pregunta**

Número	:	114
Caso de Uso	:	Listar vulnerabilidades - pregunta
Actor	:	Ing. Conocimiento
Descripción	:	Lista vulnerabilidades asociadas a una pregunta de un control de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar vulnerabilidades – pregunta.
Flujo alternativo	:	Ninguno.

Post Condición	:	Ninguna.

k. Tipos de Evaluación

- **Registrar tipo evaluación**

Número	:	115
Caso de Uso	:	Registrar tipo evaluación.
Actor	:	Ing. Conocimiento
Descripción	:	Permite registrar un tipo de evaluación de los controles de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Orden b. Nombre c. Descripción. 2. Listar tipo de evaluaciones.
Flujo alternativo	:	Ninguno.
Post Condición	:	Tipo evaluación registrada.

- **Modificar tipo evaluación**

Número	:	116
Caso de Uso	:	Modificar tipo evaluación.
Actor	:	Ing. Conocimiento
Descripción	:	Permite modificar un tipo de evaluación registrada.
Pre Condición	:	Tipo de Evaluación registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Orden b. Nombre c. Descripción. 2. Listar tipo de evaluaciones.

Flujo alternativo	:	Ninguno.
Post Condición	:	Tipo evaluación modificada.

- **Eliminar tipo evaluación**

Número	:	117
Caso de Uso	:	Eliminar tipo evaluación.
Actor	:	Ing. Conocimiento
Descripción	:	Permite eliminar un tipo de evaluación registrada.
Pre Condición	:	Tipo de Evaluación registrada.
Flujo de eventos	:	1. Eliminar tipo evaluación. 2. Listar tipo de evaluaciones.
Flujo alternativo	:	Ninguno.
Post Condición	:	Tipo evaluación eliminada.

- **Listar tipos de evaluación**

Número	:	118
Caso de Uso	:	Listar tipos de evaluación.
Actor	:	Ing. Conocimiento
Descripción	:	Lista tipos de evaluación.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar tipos de evaluación.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

l. Vulnerabilidad

- **Registrar vulnerabilidad**

Número	:	119
Caso de Uso	:	Registrar vulnerabilidad.
Actor	:	Ing. Conocimiento
Descripción	:	Permite registrar vulnerabilidades.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Descripción. 2. Listar vulnerabilidades.
Flujo alternativo	:	Ninguno.
Post Condición	:	Vulnerabilidad registrada.

- **Modificar vulnerabilidad**

Número	:	120
Caso de Uso	:	Modificar vulnerabilidad.
Actor	:	Ingeniero conocimiento.
Descripción	:	Modificar vulnerabilidades registradas.
Pre Condición	:	Vulnerabilidad registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Descripción. 2. Listar vulnerabilidades.
Flujo alternativo	:	Ninguno.
Post Condición	:	Vulnerabilidad modificada.

- **Eliminar vulnerabilidad**

Número	:	121
Caso de Uso	:	Eliminar vulnerabilidad.
Actor	:	Ingeniero conocimiento.
Descripción	:	Eliminar vulnerabilidades registradas.
Pre Condición	:	Vulnerabilidad registrada.
Flujo de eventos	:	1. Eliminar vulnerabilidad.
Flujo alternativo	:	Ninguno.
Post Condición	:	Vulnerabilidad eliminada.

- **Listar vulnerabilidades**

Número	:	122
Caso de Uso	:	Listar vulnerabilidades.
Actor	:	Ingeniero conocimiento.
Descripción	:	Lista vulnerabilidades registradas.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar vulnerabilidades.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

m. Vulnerabilidad - Amenaza

- **Asociar vulnerabilidad amenaza**

Número	:	123
Caso de Uso	:	Asociar vulnerabilidad amenaza.
Actor	:	Ingeniero conocimiento.

Descripción	:	Asociar vulnerabilidades con amenazas registradas.
Pre Condición	:	Amenaza registrada.
Flujo de eventos	:	1. Validar datos enviados: a. Vulnerabilidad b. Amenaza. 2. Listar amenazas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación vulnerabilidad – amenaza registrada.

- **Modificar asociación vulnerabilidad – amenaza**

Número	:	124
Caso de Uso	:	Asociar vulnerabilidad amenaza.
Actor	:	Ingeniero conocimiento.
Descripción	:	Modificar asociaciones entre vulnerabilidad – amenaza registrada.
Pre Condición	:	Asociación Vulnerabilidad - Amenaza registrada.
Flujo de eventos	:	1. Validar datos enviados: a. Vulnerabilidad b. Amenaza. 2. Listar amenazas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación vulnerabilidad – amenaza modificada.

- **Eliminar asociación vulnerabilidad – amenaza**

Número	:	125
Caso de Uso	:	Asociar vulnerabilidad amenaza.
Actor	:	Ingeniero conocimiento.
Descripción	:	Eliminar asociación vulnerabilidad – amenaza registrada.
Pre Condición	:	Asociación Vulnerabilidad - Amenaza registrada.
Flujo de eventos	:	1. Eliminar asociación vulnerabilidad – amenaza. 2. Listar amenazas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Asociación vulnerabilidad – amenaza eliminada.

- **Listar vulnerabilidades – amenazas**

Número	:	126
Caso de Uso	:	Listar vulnerabilidades - amenazas
Actor	:	Ingeniero conocimiento.
Descripción	:	Listar asociaciones vulnerabilidad – amenaza.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Lista asociaciones vulnerabilidad – amenaza.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

n. Amenazas

- **Registrar amenaza**

Número	:	127
Caso de Uso	:	Registrar amenaza.
Actor	:	Ingeniero conocimiento.
Descripción	:	Permite registrar amenazas.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Validar datos enviados. a. Descripción. 2. Listar amenazas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Amenaza registrada.

- **Modificar amenaza**

Número	:	128
Caso de Uso	:	Modificar amenaza.
Actor	:	Ingeniero conocimiento.
Descripción	:	Permite modificar amenazas registradas.
Pre Condición	:	Amenaza registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Descripción. 2. Listar amenazas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Amenaza modificada.

- **Eliminar amenaza**

Número	:	129
Caso de Uso	:	Eliminar amenaza.
Actor	:	Ingeniero conocimiento.
Descripción	:	Eliminar amenazas registradas.
Pre Condición	:	Vulnerabilidad registrada.
Flujo de eventos	:	1. Eliminar amenaza.
Flujo alternativo	:	Ninguno.
Post Condición	:	Amenaza eliminada.

- **Listar amenazas**

Número	:	130
Caso de Uso	:	Listar amenazas.
Actor	:	Ingeniero conocimiento.
Descripción	:	Lista amenazas registradas.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar amenazas.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

Módulo Auditoría

a. Plan auditoría

- **Crear plan auditoría**

Número	:	139
Caso de Uso	:	Crear plan auditoría.

Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite crear un plan de auditoría.
Pre Condición	:	- Idiomas registrados.
Flujo de eventos	:	1. Validar datos enviados. a. Idioma
Flujo alternativo	:	Ninguno.
Post Condición	:	Plan auditoría registrado.

- **Modificar idioma plan auditoría**

Número	:	140
Caso de Uso	:	Modificar idioma plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite modificar el idioma de un plan de auditoría registrado.
Pre Condición	:	- Plan auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Idioma
Flujo alternativo	:	Ninguno.
Post Condición	:	Plan auditoría modificado.

- **Registrar criterio - plan auditoría**

Número	:	141
Caso de Uso	:	Registrar Criterio – Plan Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite registrar un criterio al plan de auditoría.
Pre Condición	:	- Criterio de Auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados.

		a. Plan Auditoría. b. Criterio de Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Criterio Auditoría – Plan Auditoría registrado.

- **Modificar criterio – plan auditoría**

Número	:	142
Caso de Uso	:	Modificar Criterio – Plan Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite modificar un criterio - plan de auditoría registrado.
Pre Condición	:	- Criterio Auditoría – Plan Auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Criterio de Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Criterio Auditoría – Plan Auditoría modificado.

- **Eliminar criterio – plan auditoría**

Número	:	143
Caso de Uso	:	Eliminar criterio – plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite eliminar un criterio - plan de auditoría registrado.
Pre Condición	:	- Criterio Auditoría – Plan Auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Criterio de Auditoría.
Flujo alternativo	:	Ninguno.

Post Condición	:	Criterio Auditoría – Plan Auditoría eliminado.

- **Listar criterios – plan auditoría**

Número	:	144
Caso de Uso	:	Listar criterios – plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Listar los criterios de auditoría asociados al plan.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar criterios – plan auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

- **Registrar objetivo del plan auditoría**

Número	:	145
Caso de Uso	:	Registrar Objetivo del Plan Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite registrar objetivos al plan de auditoría.
Pre Condición	:	- Ninguna.
Flujo de eventos	:	2. Validar datos enviados. a. Plan Auditoría. b. Objetivo de Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Objetivo Auditoría registrado.

- **Modificar objetivo del plan auditoría**

Número	:	146

Caso de Uso	:	Modificar Objetivo del Plan Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite modificar un objetivo del plan de auditoría registrado.
Pre Condición	:	- Objetivo registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Objetivo de Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Objetivo Auditoría modificado.

- **Eliminar objetivo del plan de auditoría**

Número	:	147
Caso de Uso	:	Eliminar Objetivo del Plan Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite eliminar un objetivo del plan de auditoría registrado.
Pre Condición	:	- Objetivo registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Objetivo de Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Objetivo Auditoría eliminado.

- **Listar objetivos del plan de auditoría**

Número	:	148
Caso de Uso	:	Eliminar Objetivo del Plan Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor

Descripción	:	Lista objetivos del plan de auditoría.
Pre Condición	:	- Objetivo registrado.
Flujo de eventos	:	1. Listar objetivos.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

- **Registrar sede – plan auditoría**

Número	:	149
Caso de Uso	:	Registrar sede - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite registrar una sede -plan de auditoría.
Pre Condición	:	- Plan de auditoría registrada. - Sede de cliente registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Sede.
Flujo alternativo	:	Ninguno.
Post Condición	:	Sede – Plan Auditoría registrado.

- **Modificar sede – plan auditoría**

Número	:	150
Caso de Uso	:	Registrar sede - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite modificar una sede -plan de auditoría registrada.
Pre Condición	:	- Sede – Plan Auditoría registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría.

		b. Sede.
Flujo alternativo	:	Ninguno.
Post Condición	:	Sede – Plan Auditoría modificada.

- **Eliminar sede – plan auditoría**

Número	:	151
Caso de Uso	:	Eliminar sede - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite eliminar una sede -plan de auditoría registrada.
Pre Condición	:	- Sede – Plan Auditoría registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Sede.
Flujo alternativo	:	Ninguno.
Post Condición	:	Sede – Plan Auditoría eliminada.

- **Listar sedes- plan auditoría**

Número	:	152
Caso de Uso	:	Listar sedes - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Lista sedes asociadas a un plan de auditoría.
Pre Condición	:	- Ninguna.
Flujo de eventos	:	1. Listar sedes – plan auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

- **Registrar miembro equipo – plan auditoría**

Número	:	153
Caso de Uso	:	Registrar miembro equipo - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite registrar miembros del equipo -plan de auditoría.
Pre Condición	:	- Persona registrada. - Plan auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Persona.
Flujo alternativo	:	Ninguno.
Post Condición	:	Equipo – Plan Auditoría registrado.

- **Modificar miembro equipo – plan auditoría**

Número	:	154
Caso de Uso	:	Modificar miembro equipo - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite modificar un miembro del equipo -plan de auditoría registrado.
Pre Condición	:	- Equipo – Plan Auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Persona.
Flujo alternativo	:	Ninguno.
Post Condición	:	Equipo – Plan Auditoría modificado.

- **Eliminar miembro equipo – plan auditoría**

Número	:	155
Caso de Uso	:	Eliminar miembro equipo - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite eliminar un miembro del equipo -plan de auditoría registrado.
Pre Condición	:	- Equipo – Plan Auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Persona.
Flujo alternativo	:	Ninguno.
Post Condición	:	Equipo – Plan Auditoría eliminado.

- **Listar equipo – plan auditoría**

Número	:	156
Caso de Uso	:	Listar equipo - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Lista las personas asociadas al plan de auditoría.
Pre Condición	:	- Equipo – Plan Auditoría registrado.
Flujo de eventos	:	1. Listar equipo.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

- **Registrar actividad – plan auditoría**

Número	:	157
Caso de Uso	:	Registrar actividad - plan auditoría

Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite registrar una asociación actividad - plan de auditoría.
Pre Condición	:	- Actividad registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Plan Auditoría. b. Actividad.
Flujo alternativo	:	Ninguno.
Post Condición	:	Actividad – Plan Auditoría registrada.

- **Modificar actividad – plan auditoría**

Número	:	158
Caso de Uso	:	Modificar actividad - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite modificar una asociación actividad - plan de auditoría registrada.
Pre Condición	:	- Actividad registrada.
Flujo de eventos	:	2. Validar datos enviados. a. Plan Auditoría. b. Actividad.
Flujo alternativo	:	Ninguno.
Post Condición	:	Actividad – Plan Auditoría modificar.

- **Listar actividades – plan auditoría**

Número	:	159
Caso de Uso	:	Listar actividades - plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor

Descripción	:	Lista las actividades asociadas al plan de auditoría.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar actividades – plan auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

- **Finalizar plan auditoría**

Número	:	160
Caso de Uso	:	Finalizar plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite concluir la edición del plan de auditoría.
Pre Condición	:	- Plan auditoría registrado.
Flujo de eventos	:	1. Validar datos enviados. a. Estado. b. Plan Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Plan Auditoría modificado.

b. Cuestionario

- **Listar controles cuestionario**

Número	:	161
Caso de Uso	:	Listar controles cuestionario
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Lista los controles por objetivos y dominios.
Pre Condición	:	- Control Auditoría registrado.
Flujo de eventos	:	1. Listar controles.

Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

- **Completar cuestionario auditoría**

Número	:	162
Caso de Uso	:	Completar cuestionario plan auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite completar los cuestionarios por control de auditoría.
Pre Condición	:	- Preguntas registradas.
Flujo de eventos	:	2. Validar datos enviados. a. Respuesta. b. Comentario c. Pregunta.
Flujo alternativo	:	Ninguno.
Post Condición	:	Respuesta registrada.

- **Adjuntar evidencia pregunta**

Número	:	163
Caso de Uso	:	Adjuntar evidencia respuesta
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite adjuntar evidencia a cada pregunta de auditoría.
Pre Condición	:	- Preguntas registradas.
Flujo de eventos	:	1. Validar datos enviados. a. Nombre. b. Descripción c. Tipo Evidencia. d. Evidencia.

Flujo alternativo	:	Ninguno.
Post Condición	:	Evidencia registrada.

- **Eliminar evidencia pregunta**

Número	:	164
Caso de Uso	:	Eliminar evidencia respuesta
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Permite eliminar evidencia registrada.
Pre Condición	:	- Evidencia registrada.
Flujo de eventos	:	1. Validar datos enviados. a. Evidencia.
Flujo alternativo	:	Ninguno.
Post Condición	:	Evidencia eliminada.

- **Listar evidencias pregunta**

Número	:	165
Caso de Uso	:	Listar evidencia pregunta
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Lista las evidencias de una pregunta.
Pre Condición	:	Ninguna.
Flujo de eventos	:	1. Listar evidencia pregunta.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

c. Informe auditoría

- **Generar informe de Auditoría**

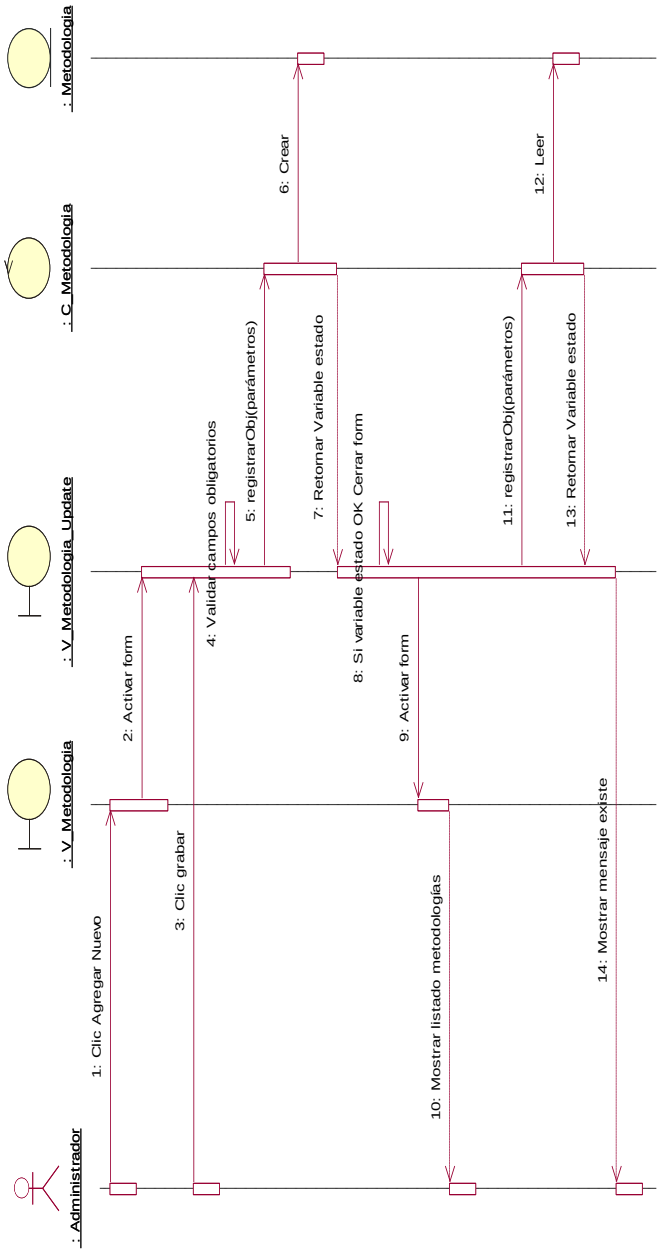
Número	:	166
Caso de Uso	:	Generar informe de Auditoría
Actor	:	Ing. Conocimiento/ Administrador/ Auditor
Descripción	:	Genera el informe de Auditoría.
Pre Condición	:	Respuesta registrada.
Flujo de eventos	:	1. Generar informe de Auditoría.
Flujo alternativo	:	Ninguno.
Post Condición	:	Ninguna.

4.3.2 Diagramas de Secuencia

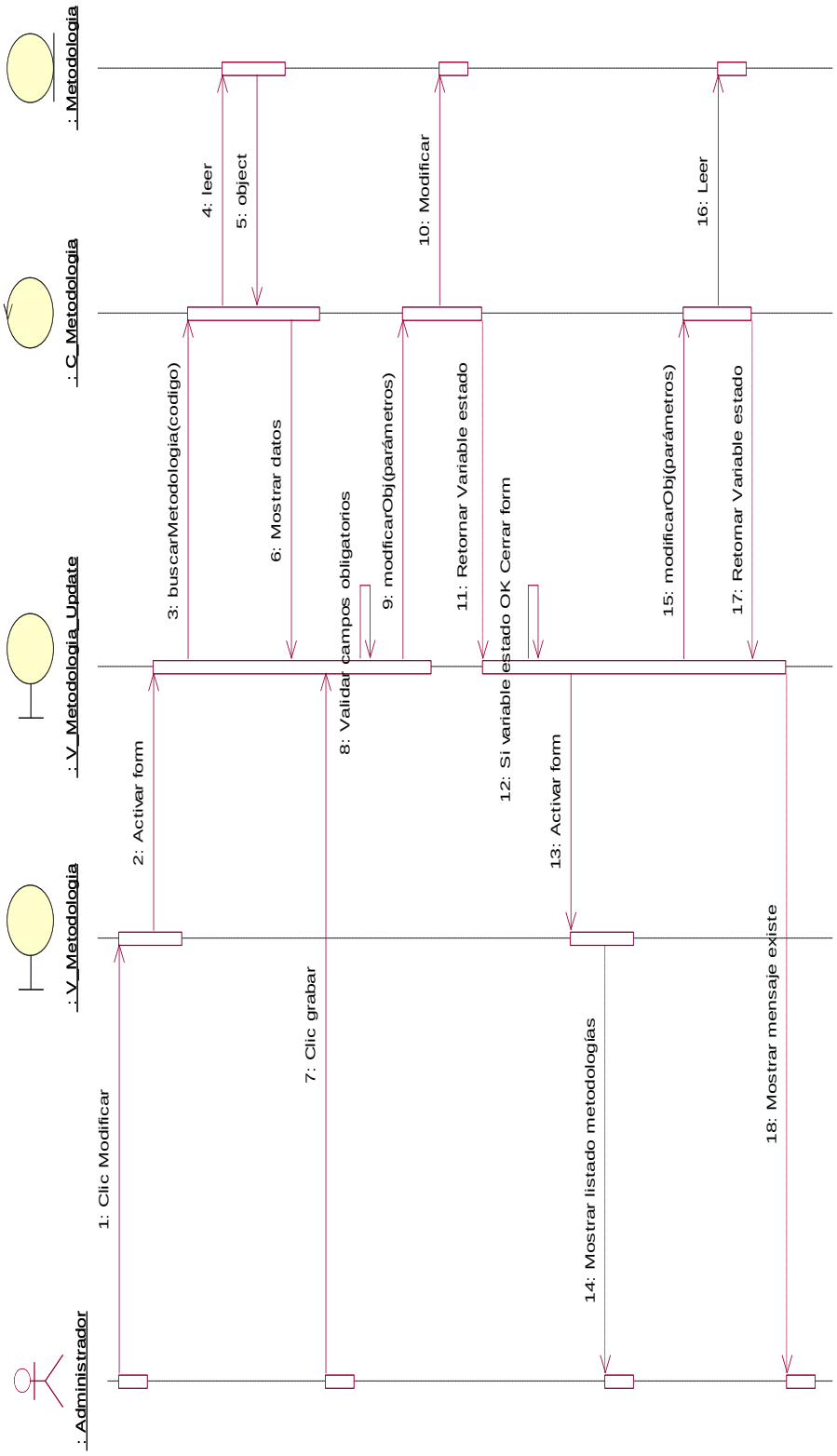
Módulo de Base de Conocimiento

a. Metodología

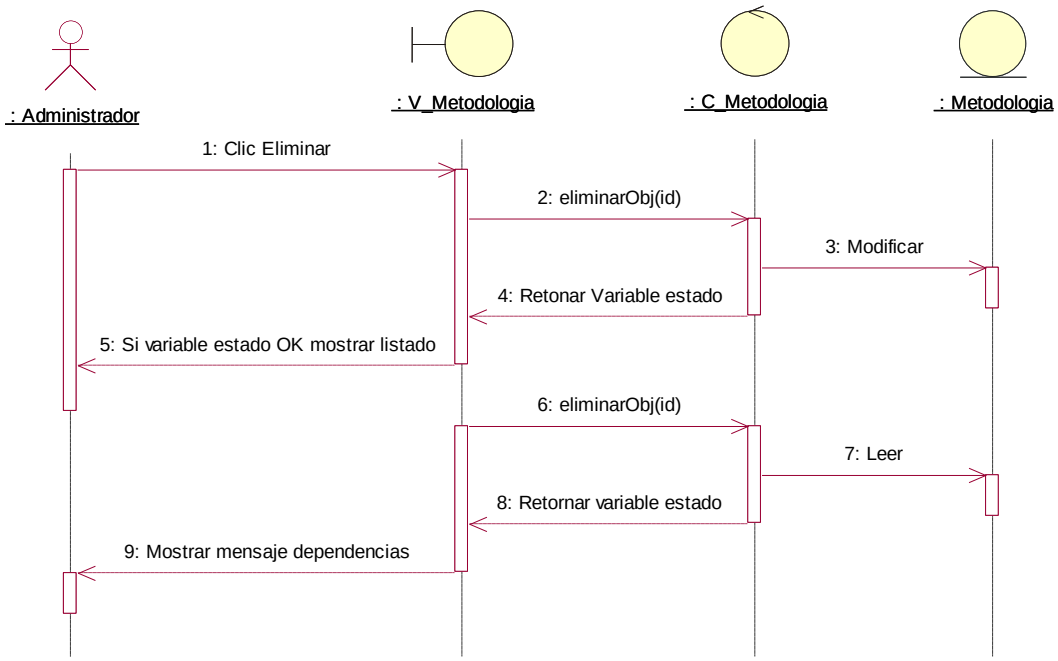
- **Registrar metodología**



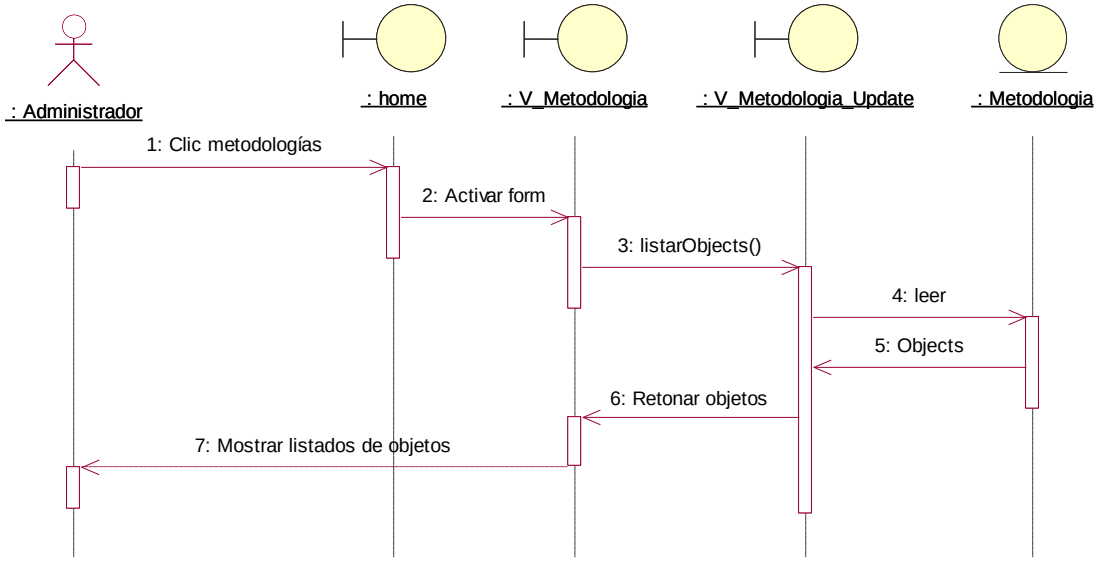
- **Modificar metodología**



- **Eliminar metodología**

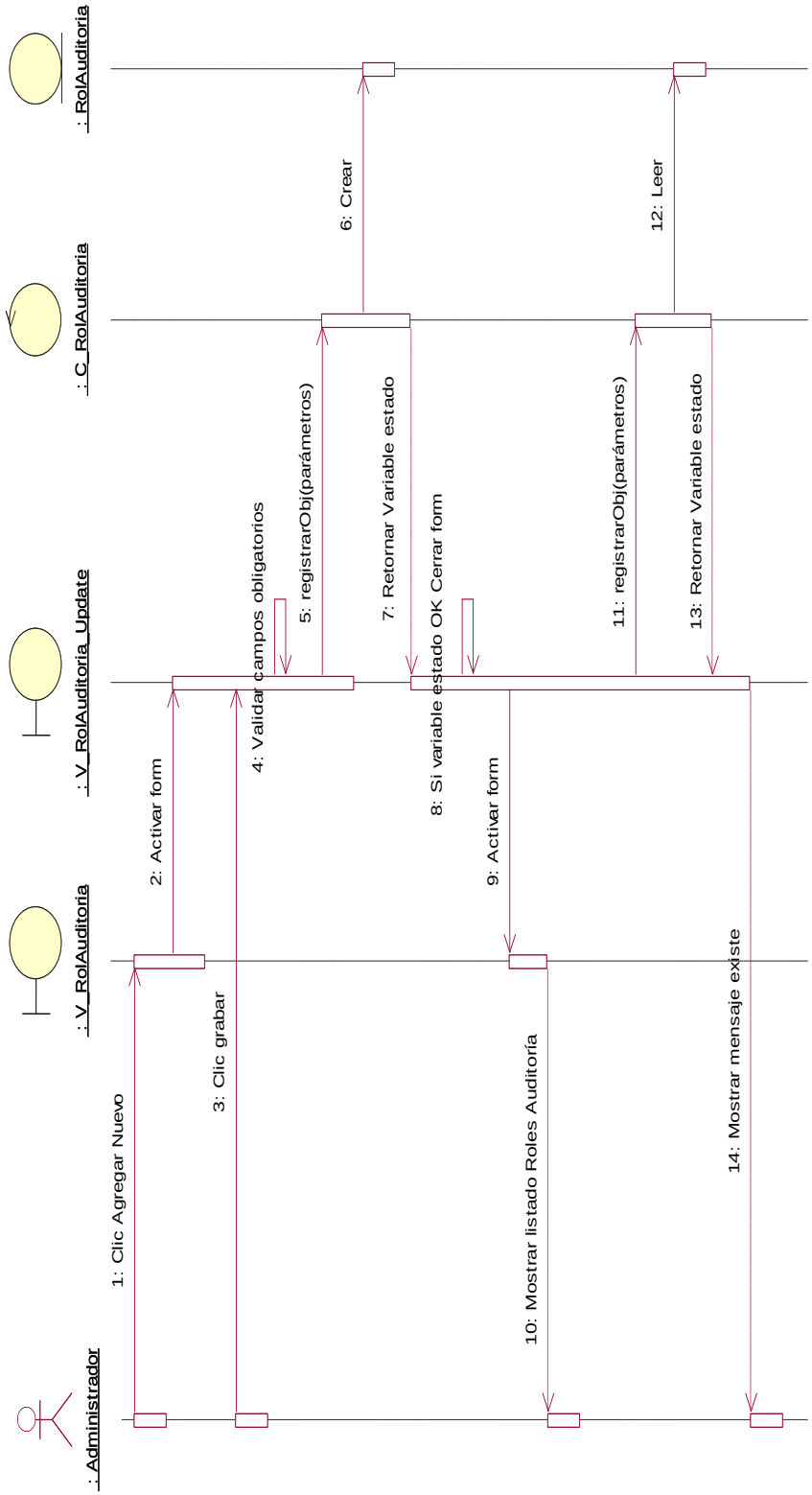


- **Listar metodologías**

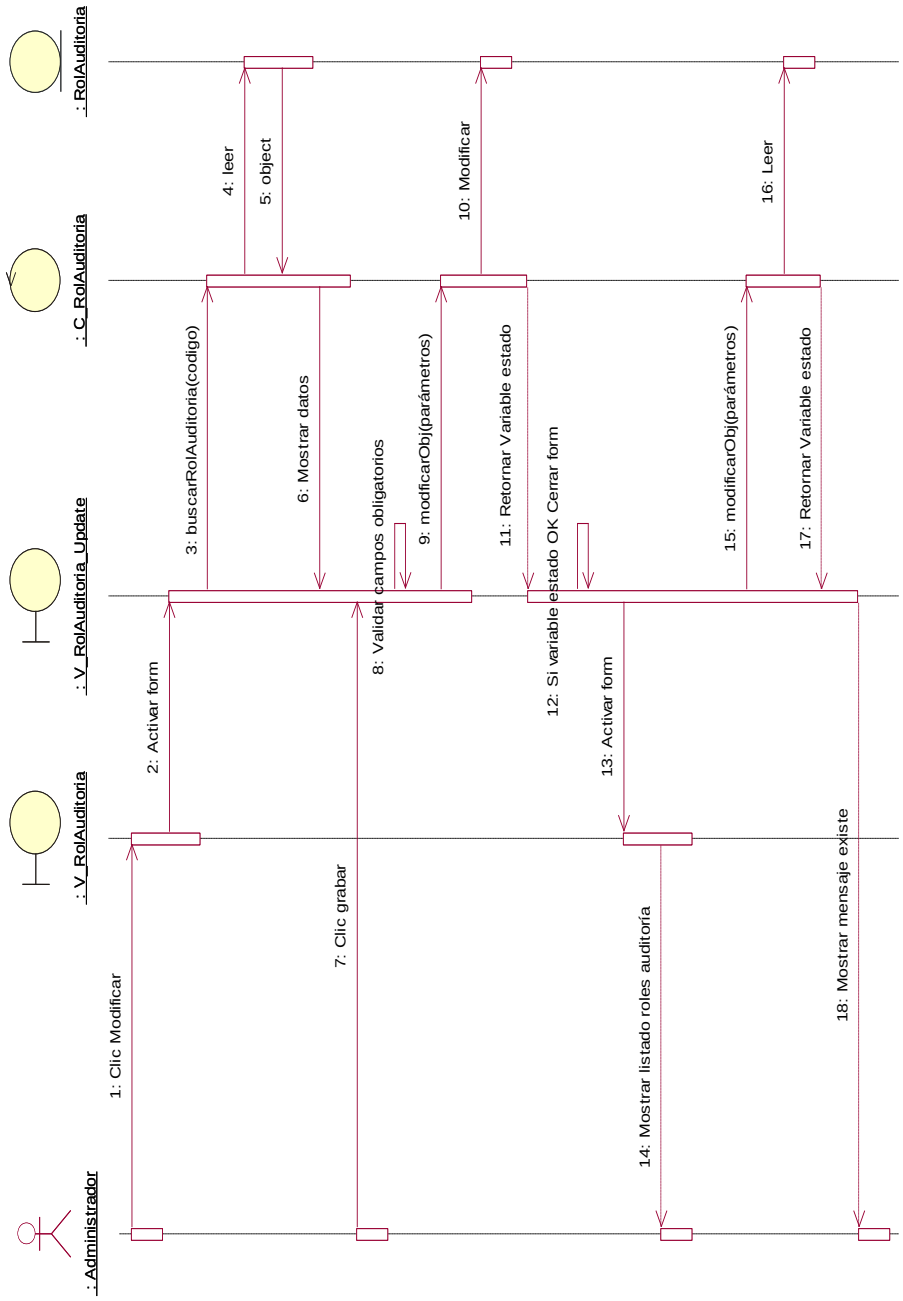


b. Roles auditoría

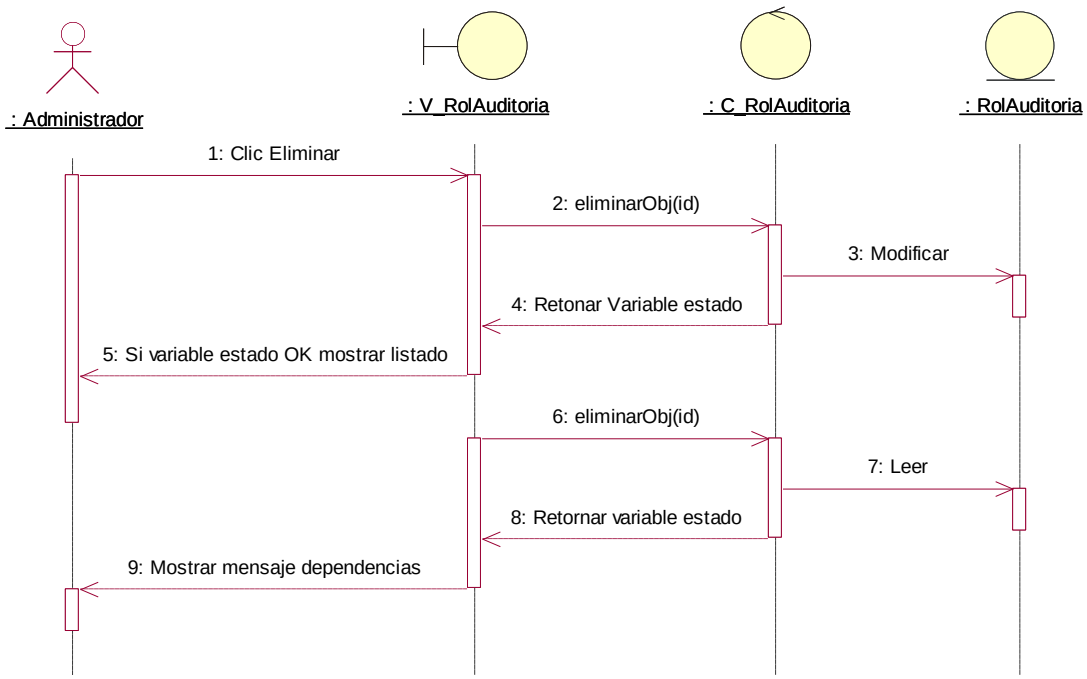
- **Registrar rol auditoría**



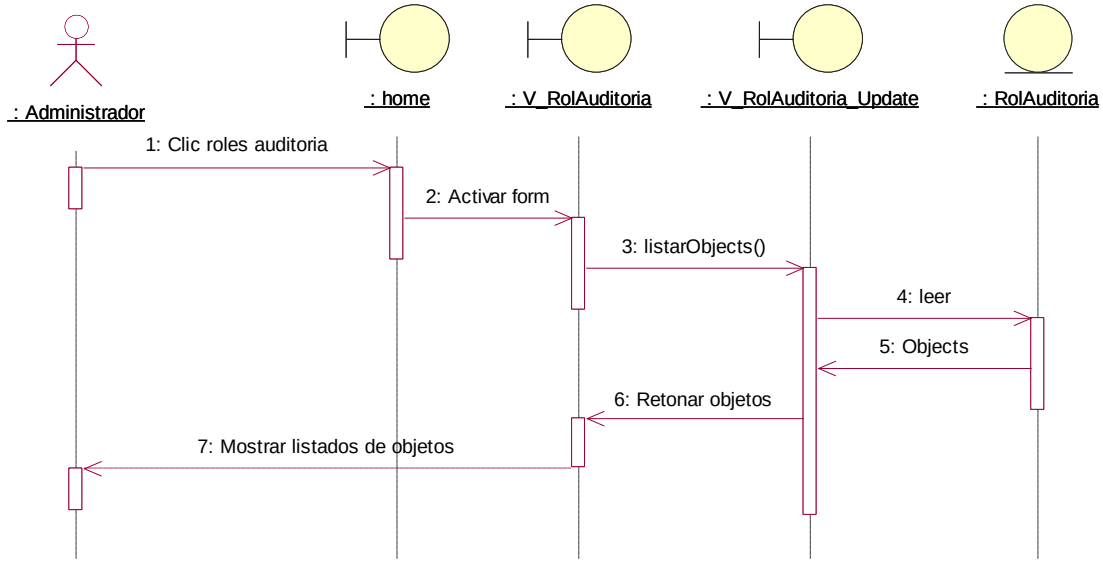
- **Modificar rol auditoría**



- **Eliminar rol auditoría**

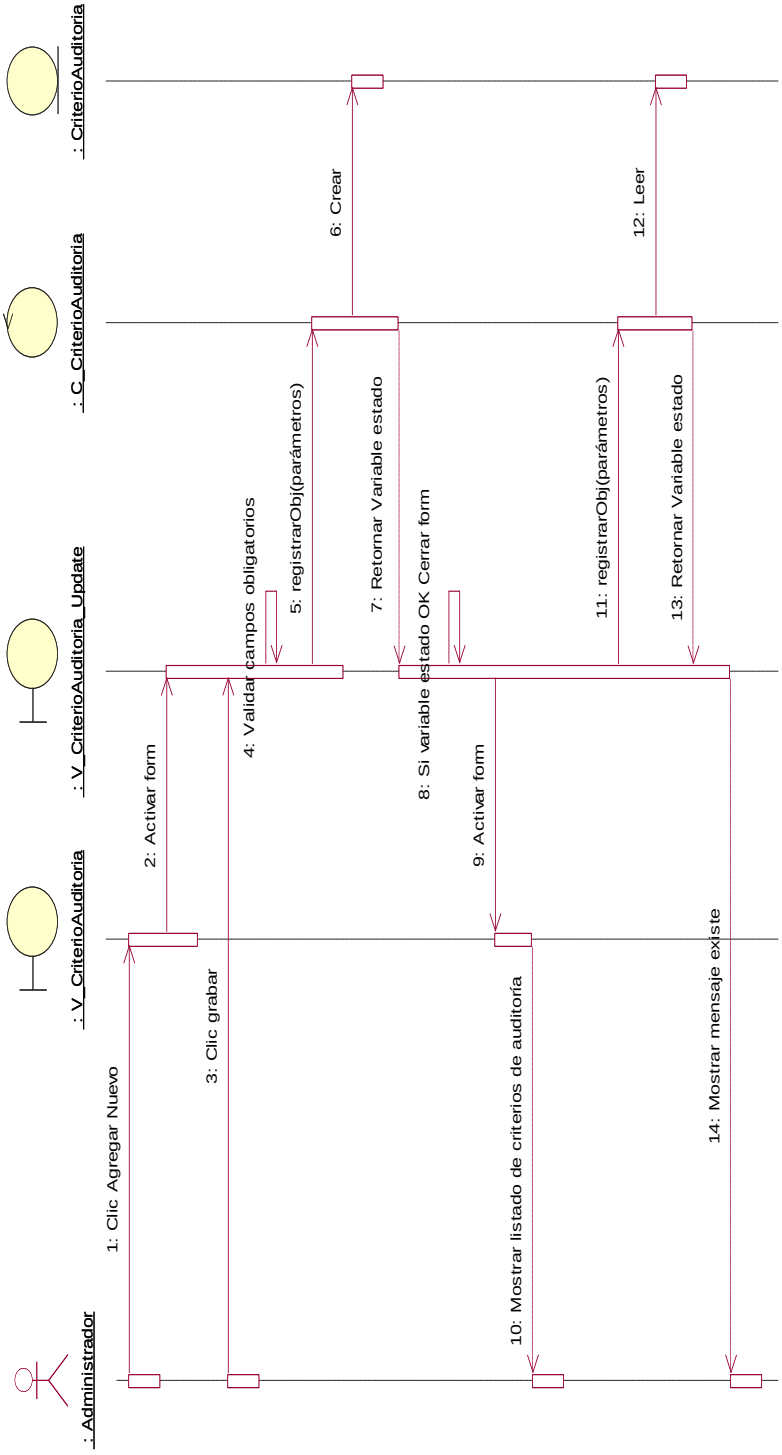


- **Listar roles auditoría**

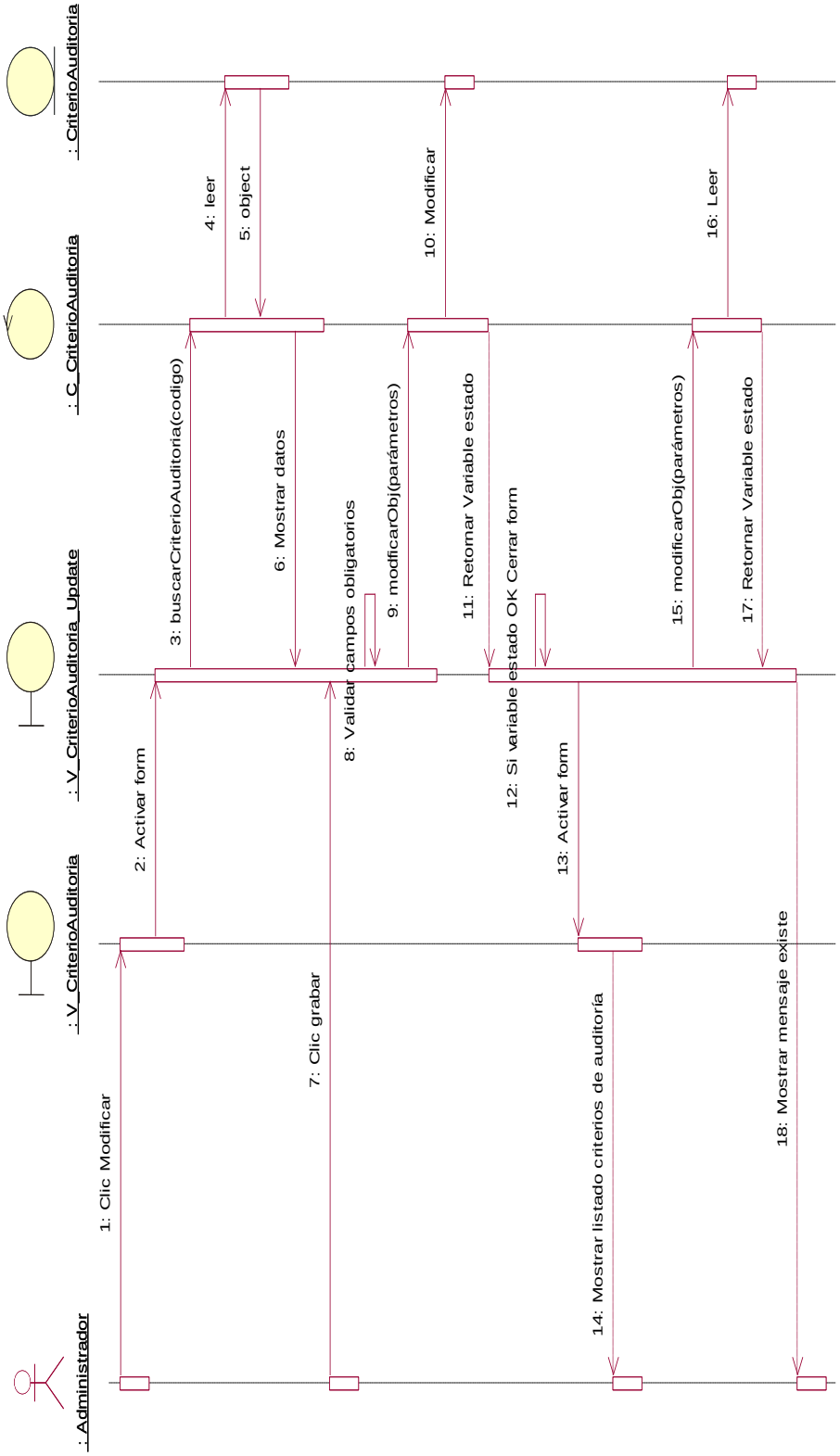


c. Criterios

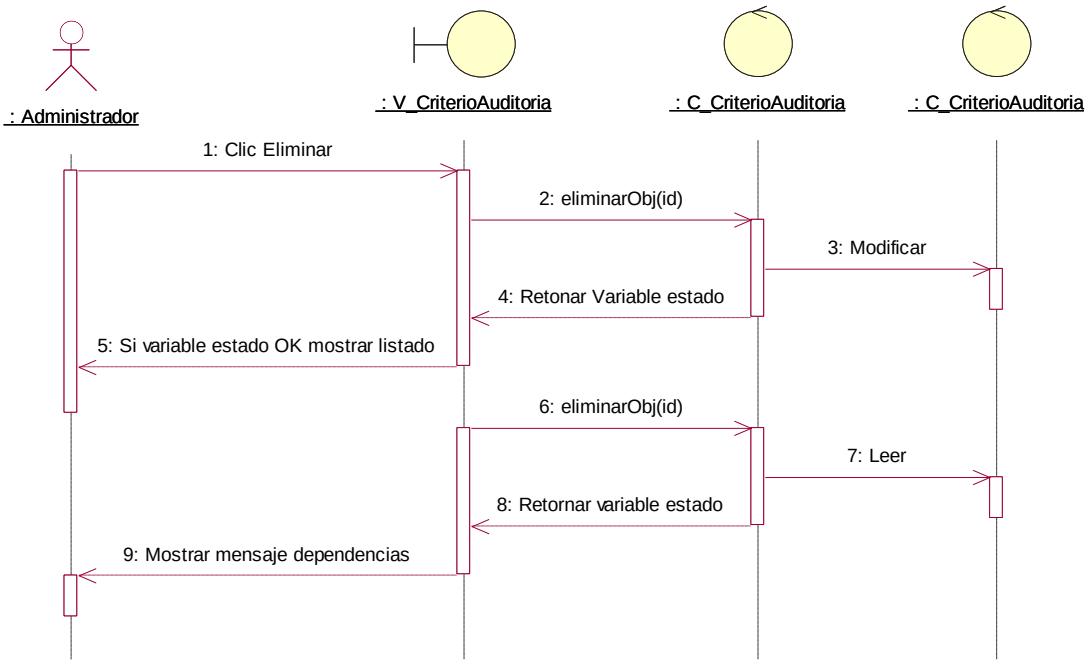
- Registrar criterio



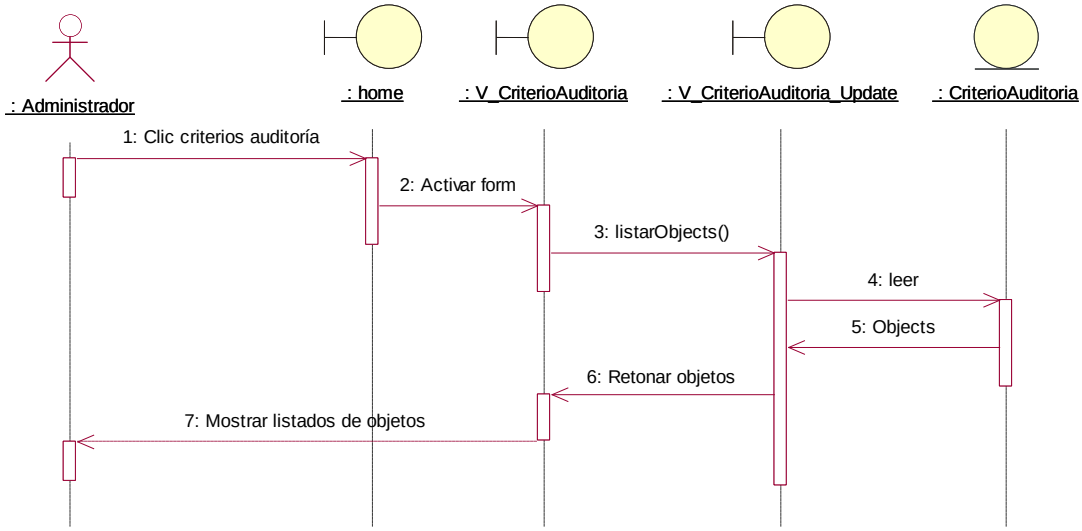
- **Modificar criterio**



- **Eliminar criterio**

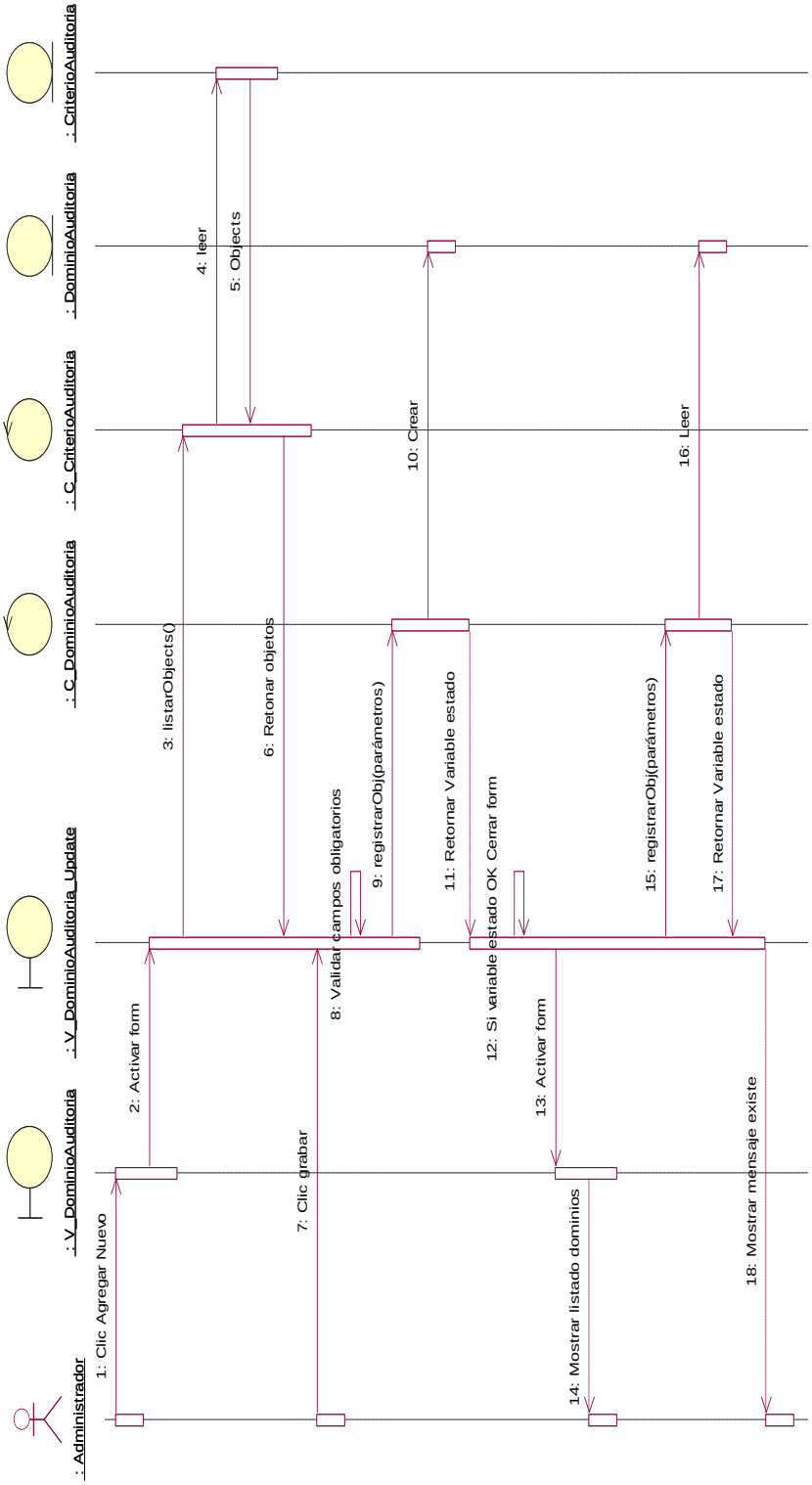


- **Listar criterios**

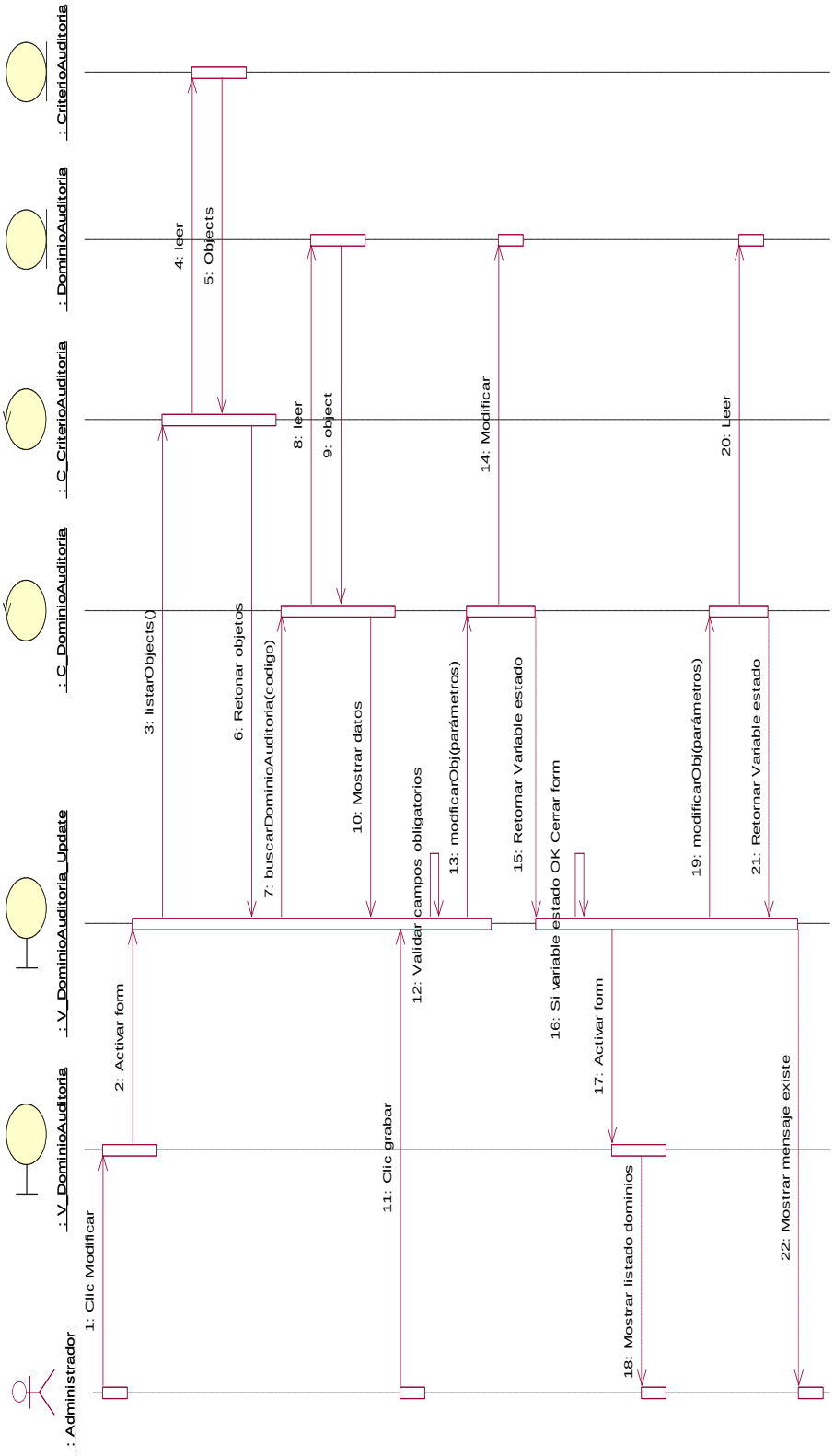


d. Dominios

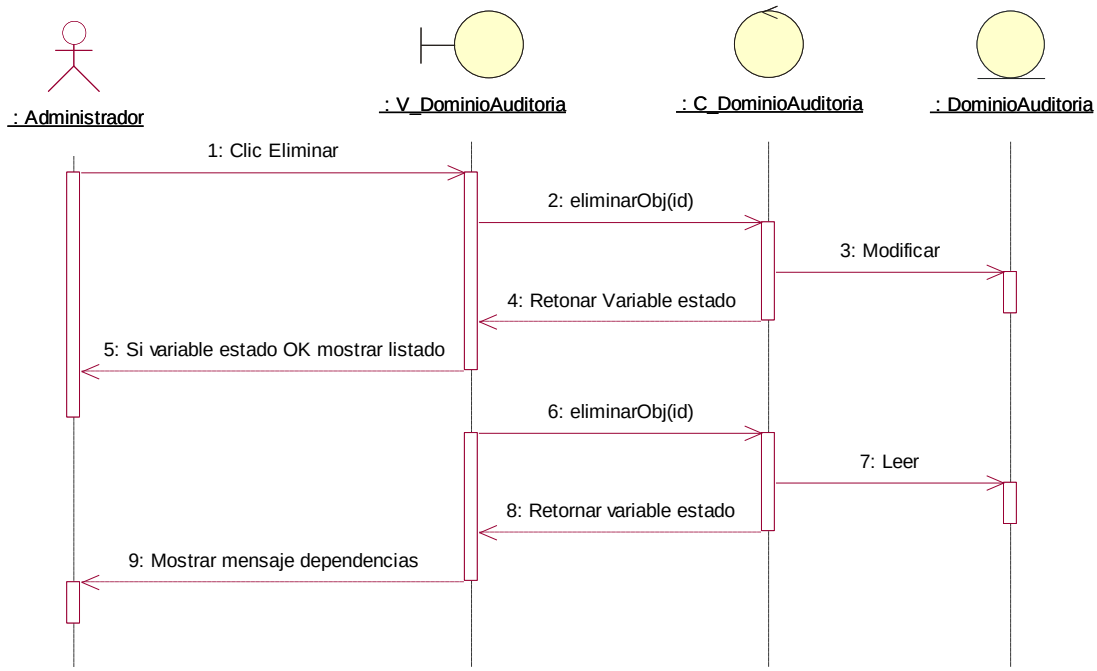
- **Registrar dominio**



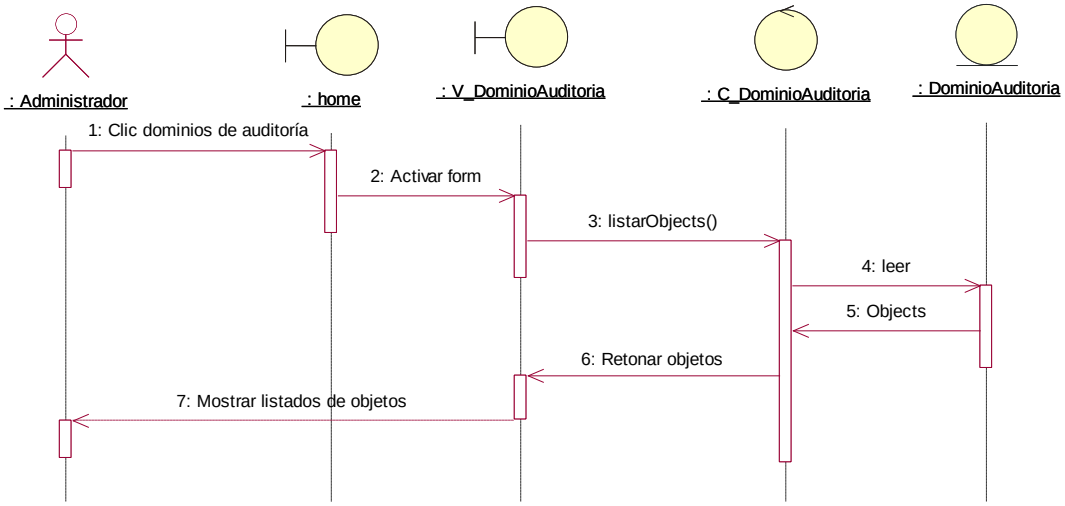
- **Modificar dominio**



- **Eliminar dominio**

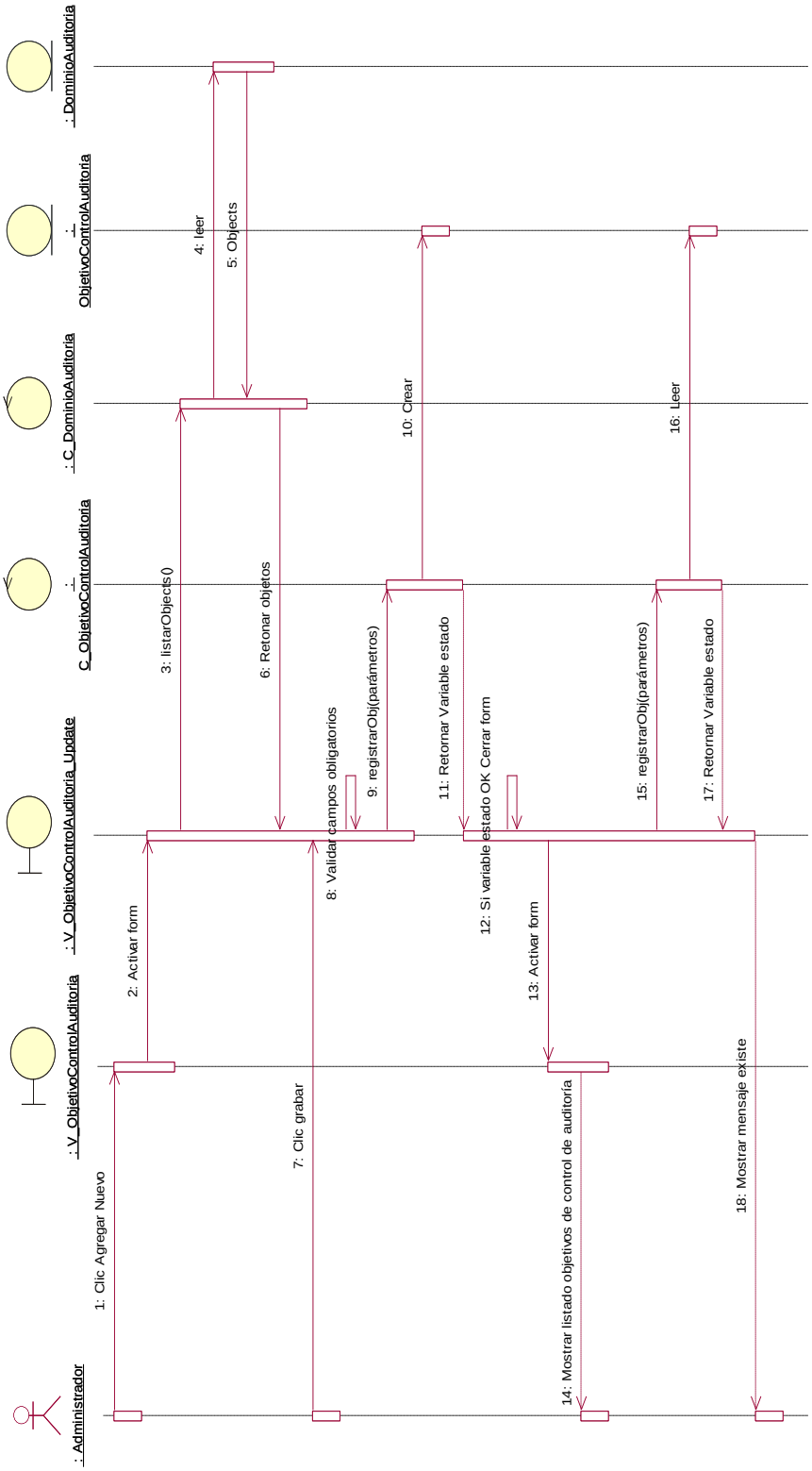


- **Listar dominios**

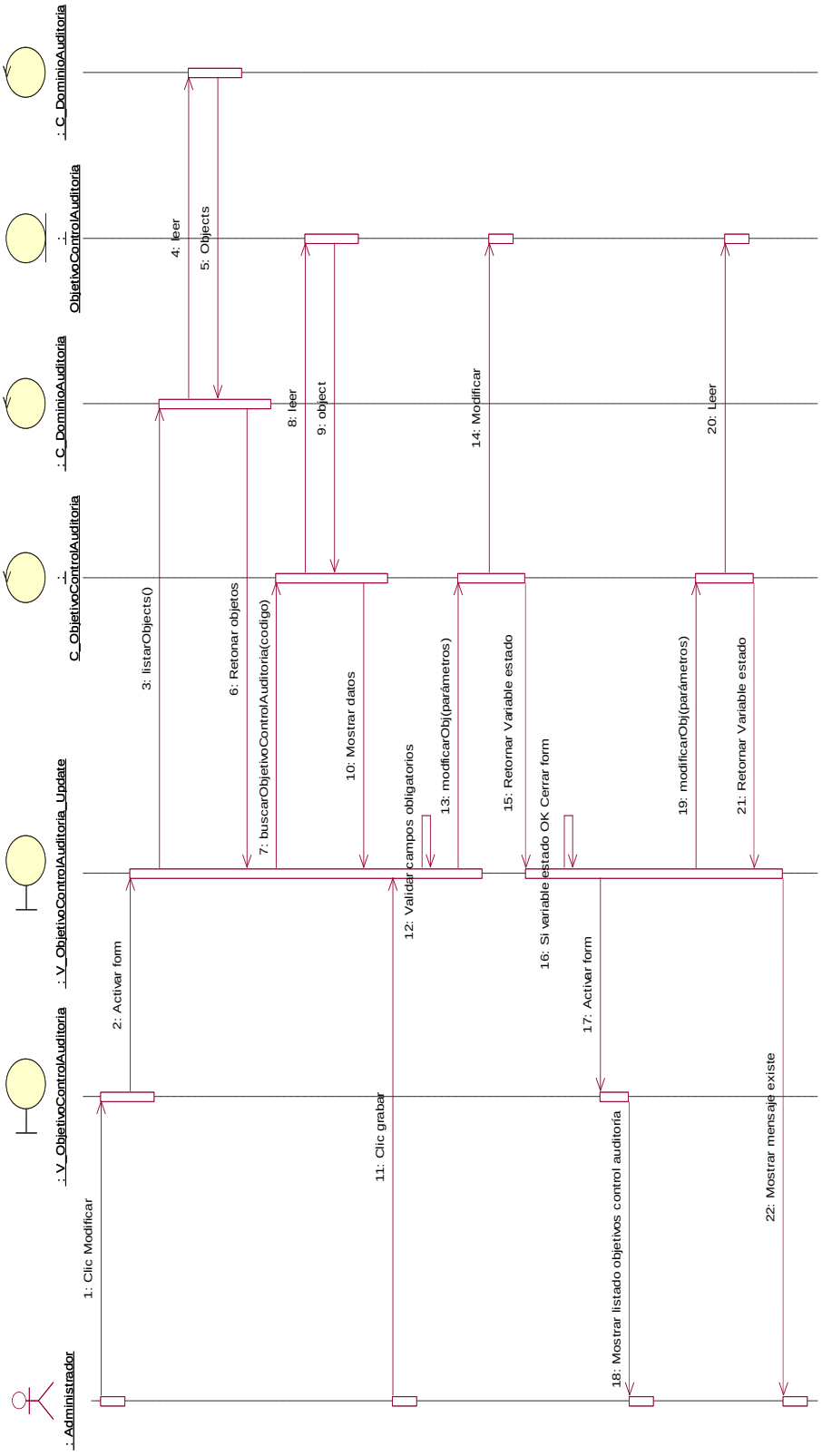


e. Objetivos de control de auditoría

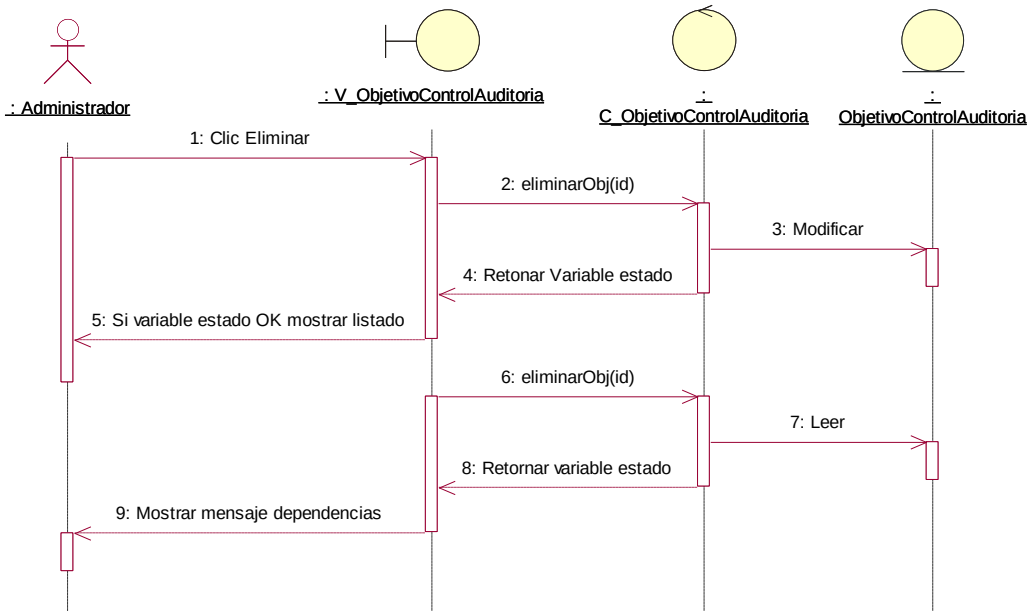
- **Registrar objetivo de control**



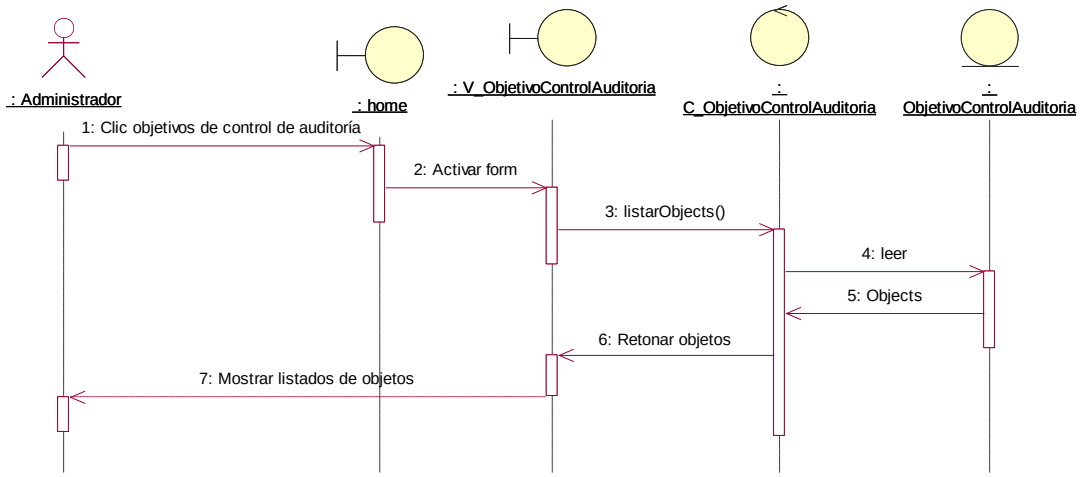
- **Modificar objetivo de control**



- **Eliminar objetivo de control**

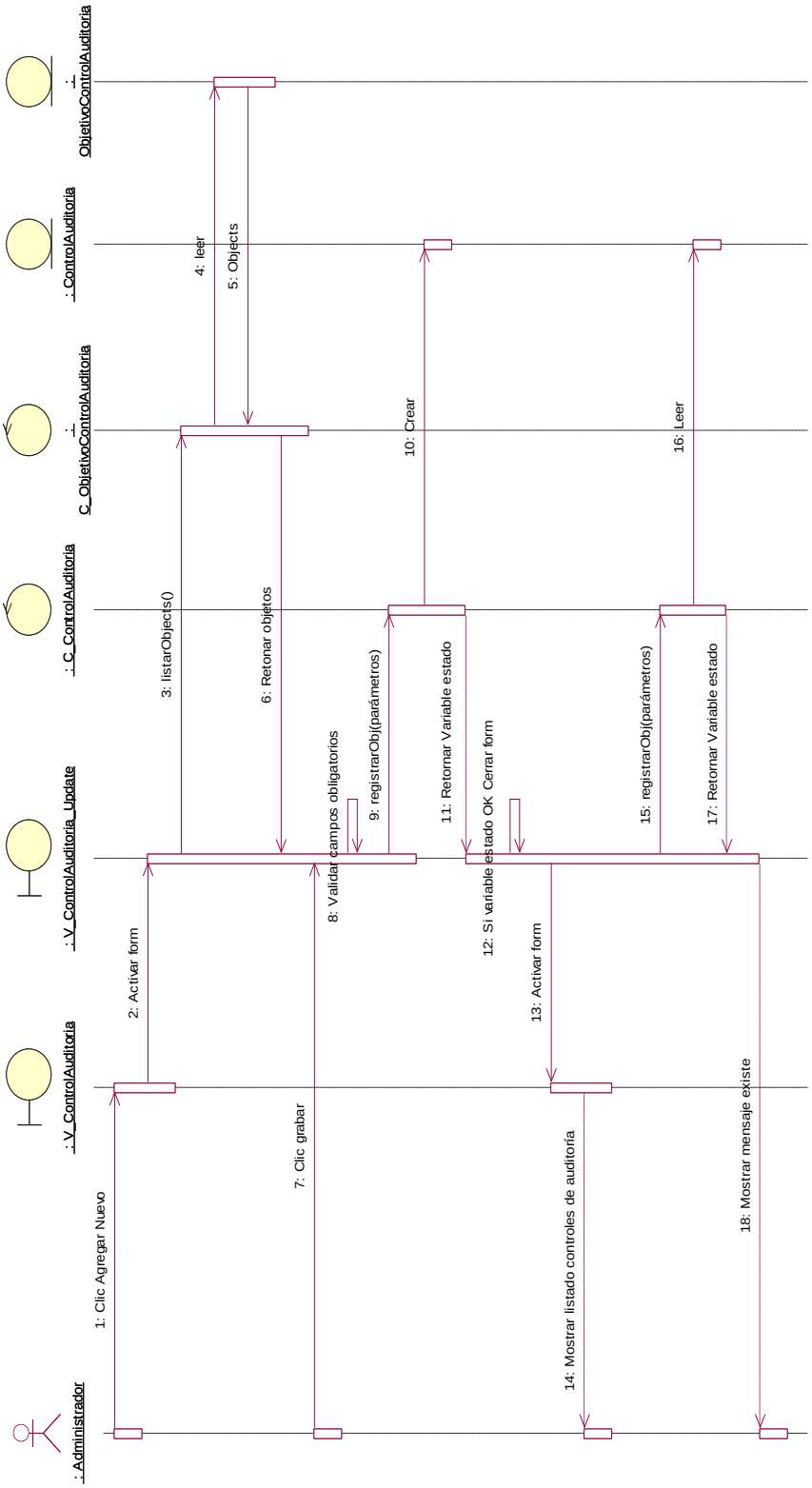


- **Listar objetivos de control**

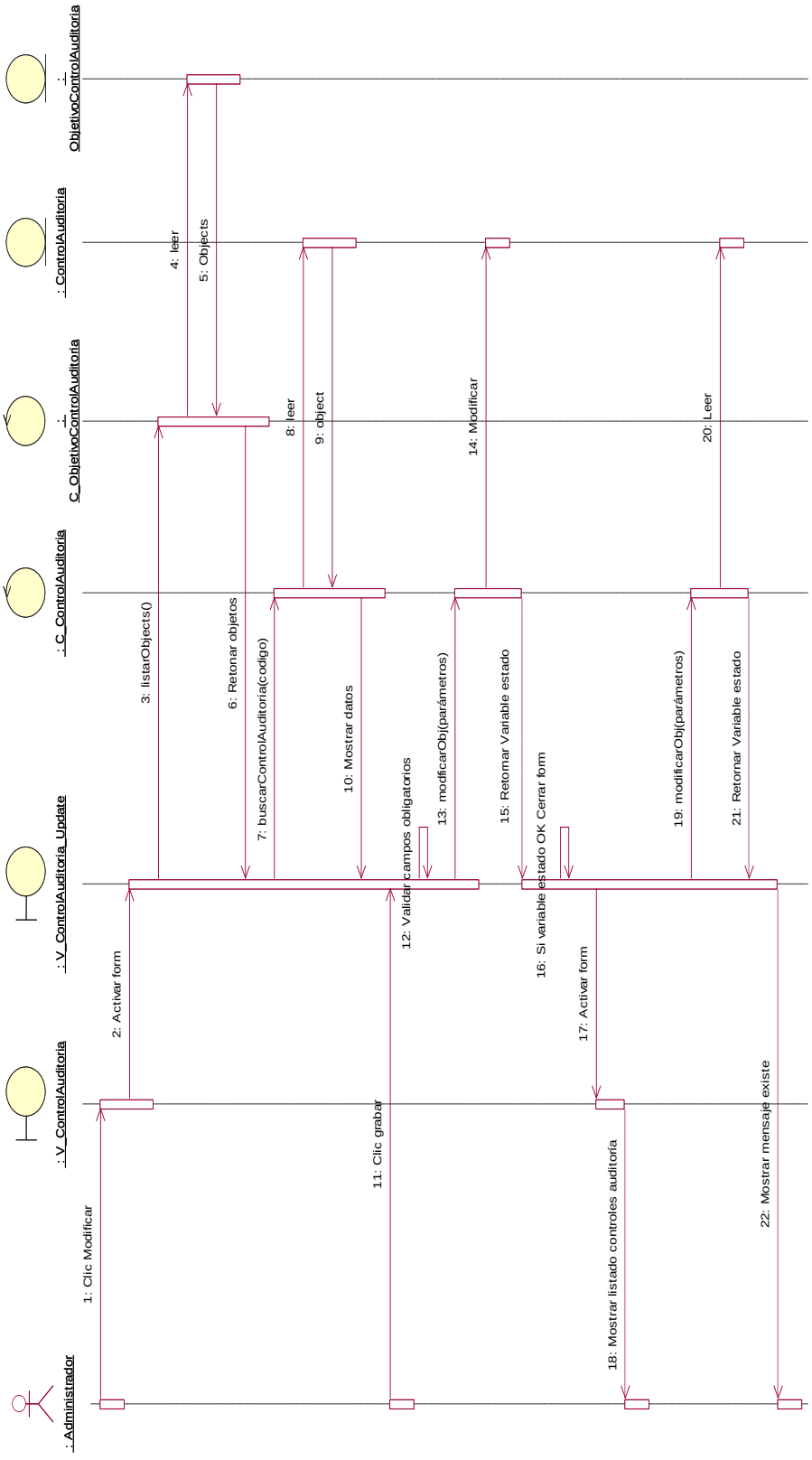


f. Control de Auditoría

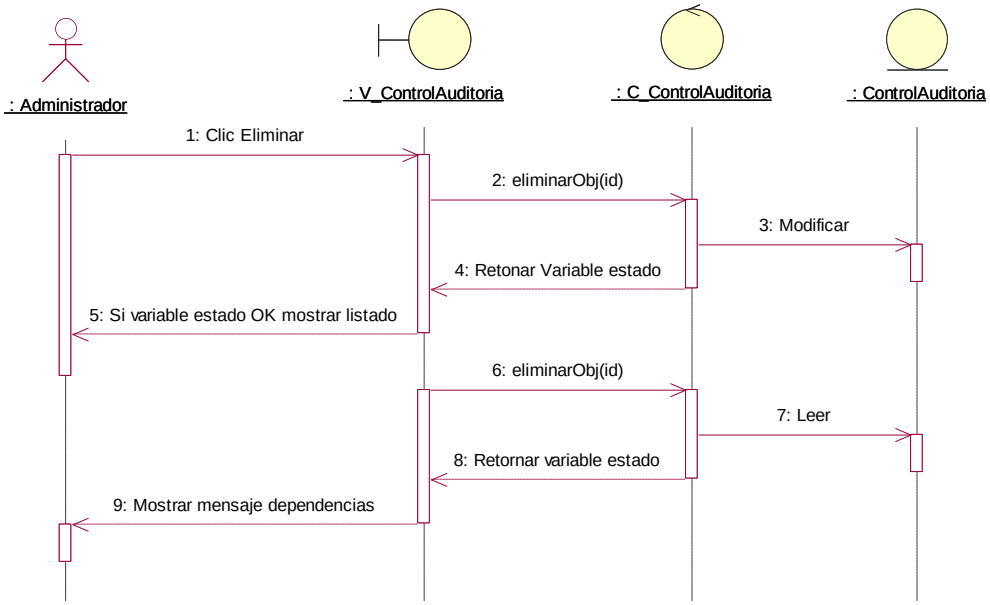
- Registrar Control Auditoría



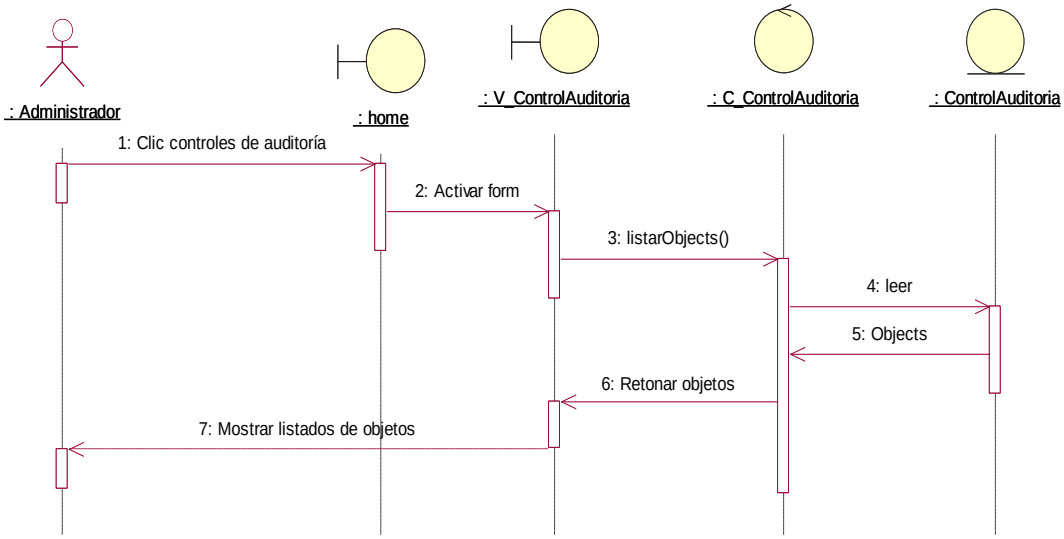
- **Modificar control de Auditoría**



- **Eliminar Control de Auditoría**

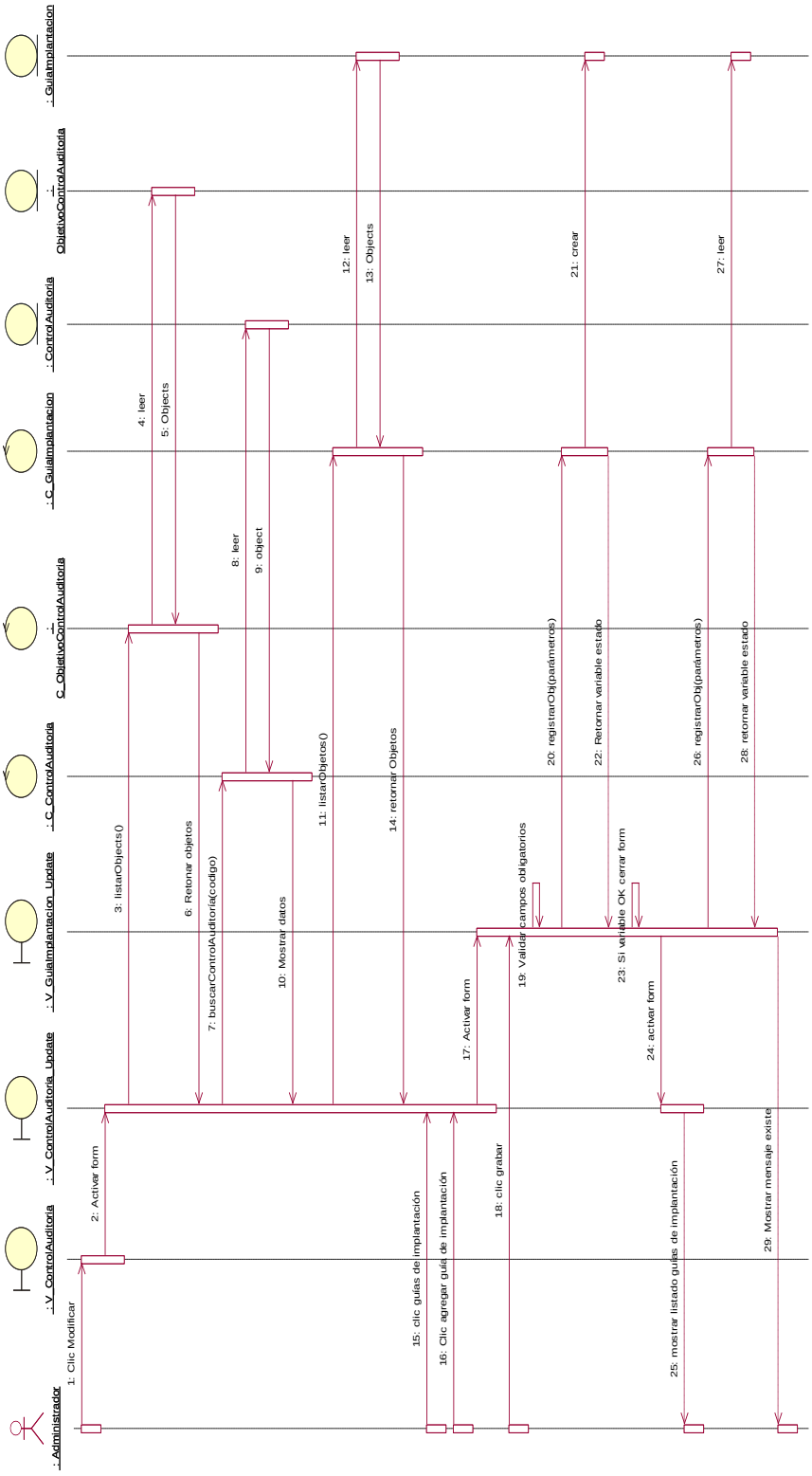


- **Listar controles de Auditoría**

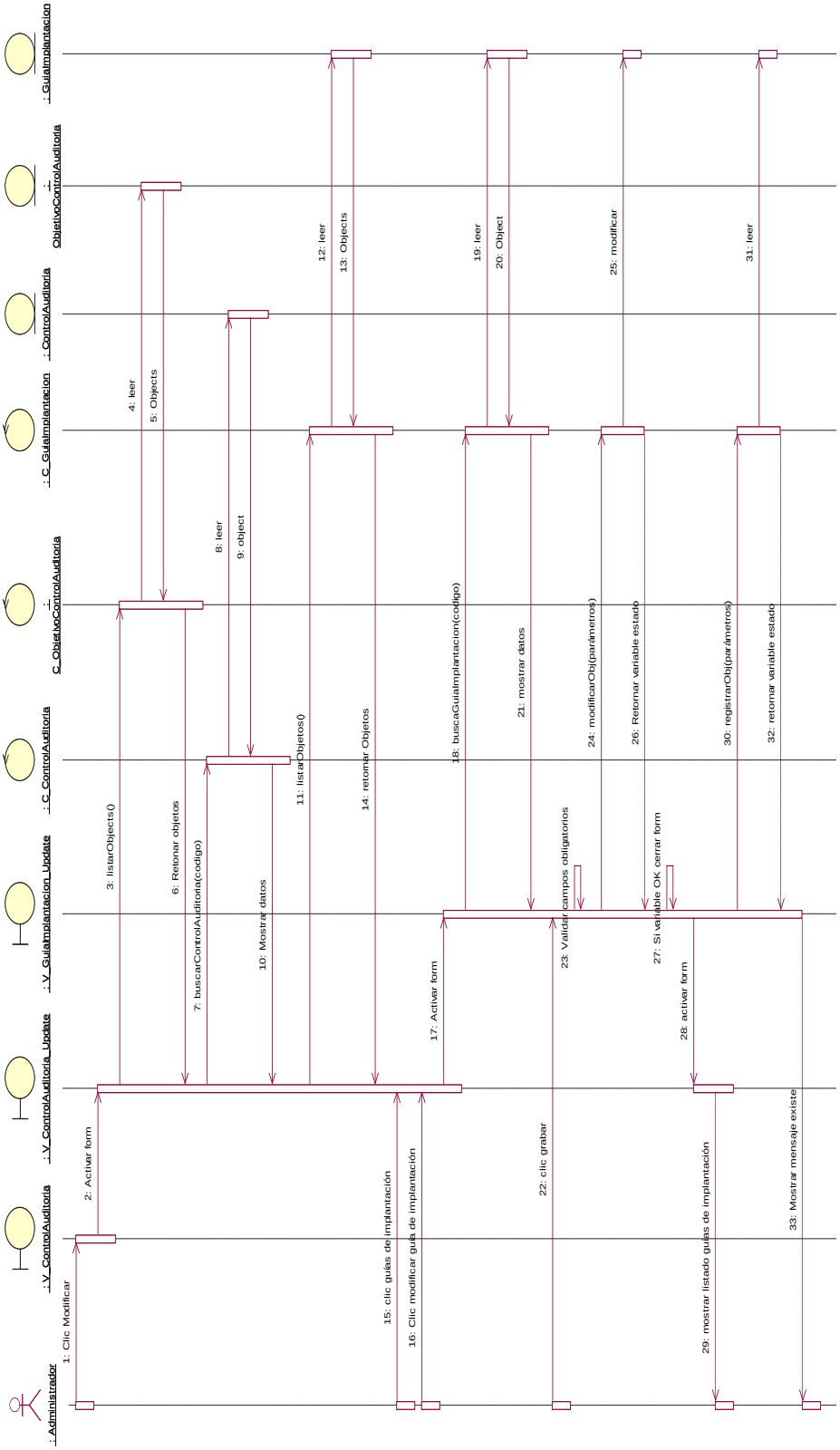


g. Guía de Implantación

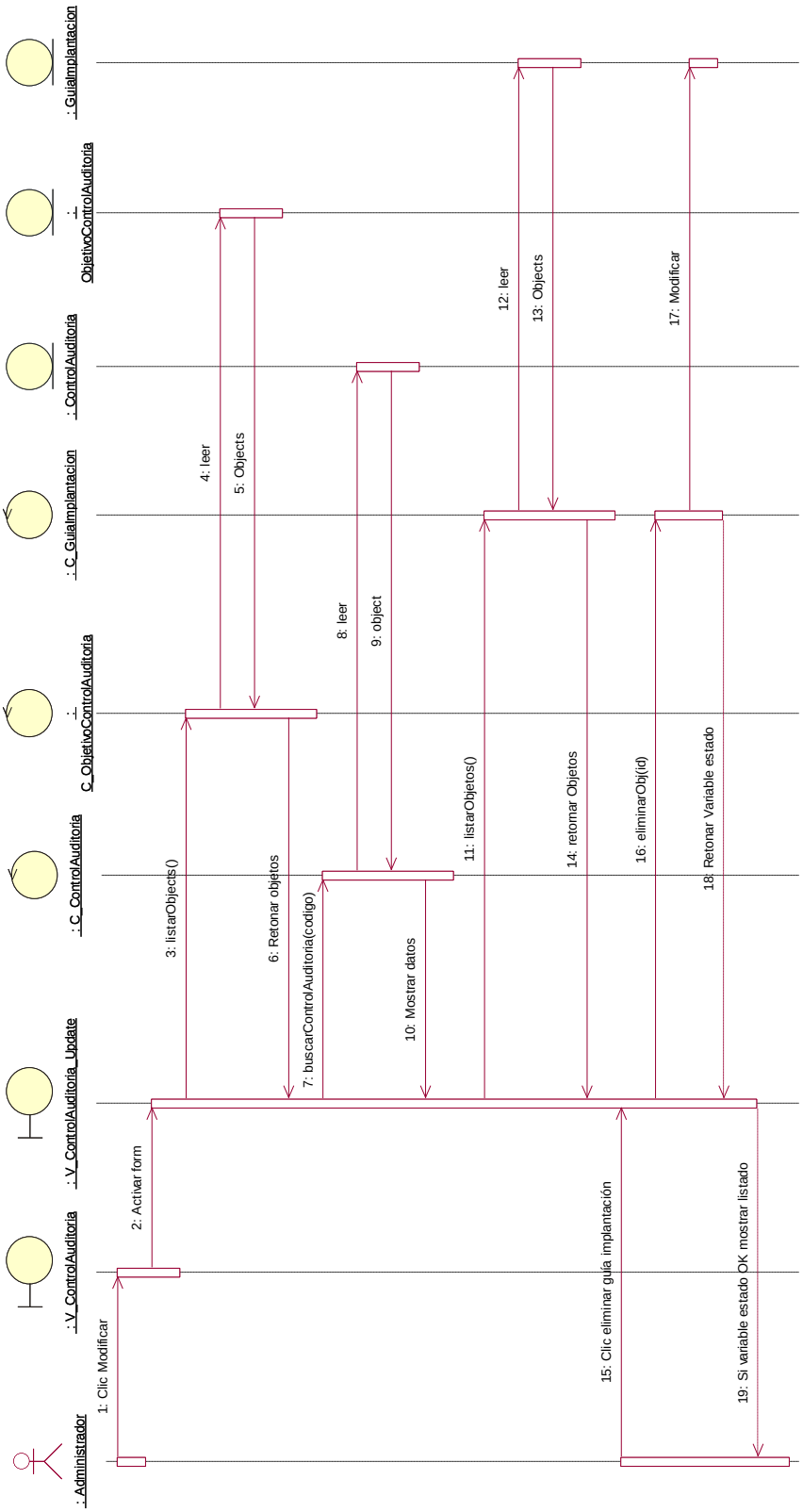
- Registrar guía de implantación



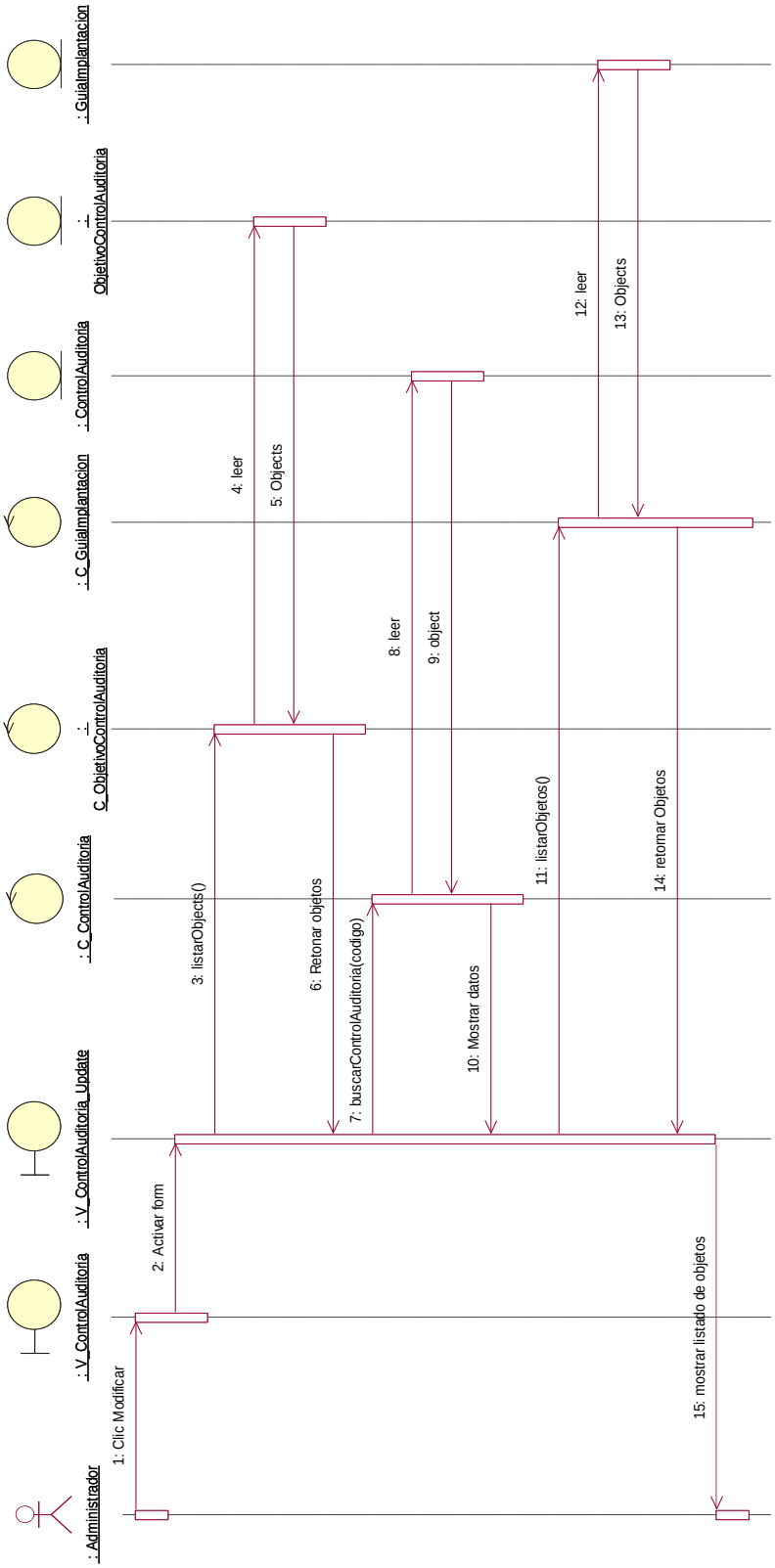
- **Modificar guía de implantación**



- **Eliminar guía de implantación**

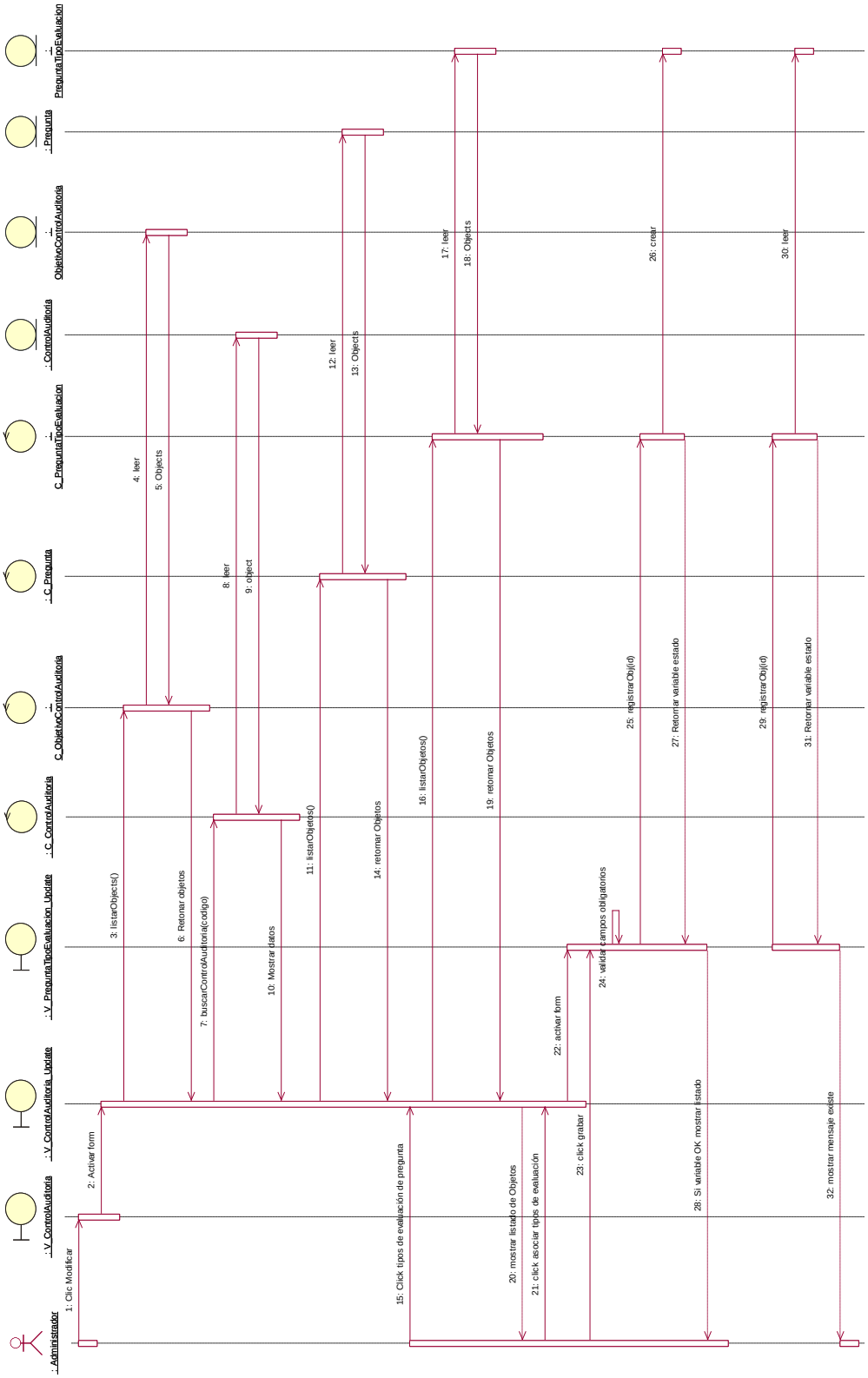


- **Listar guías de implantación**

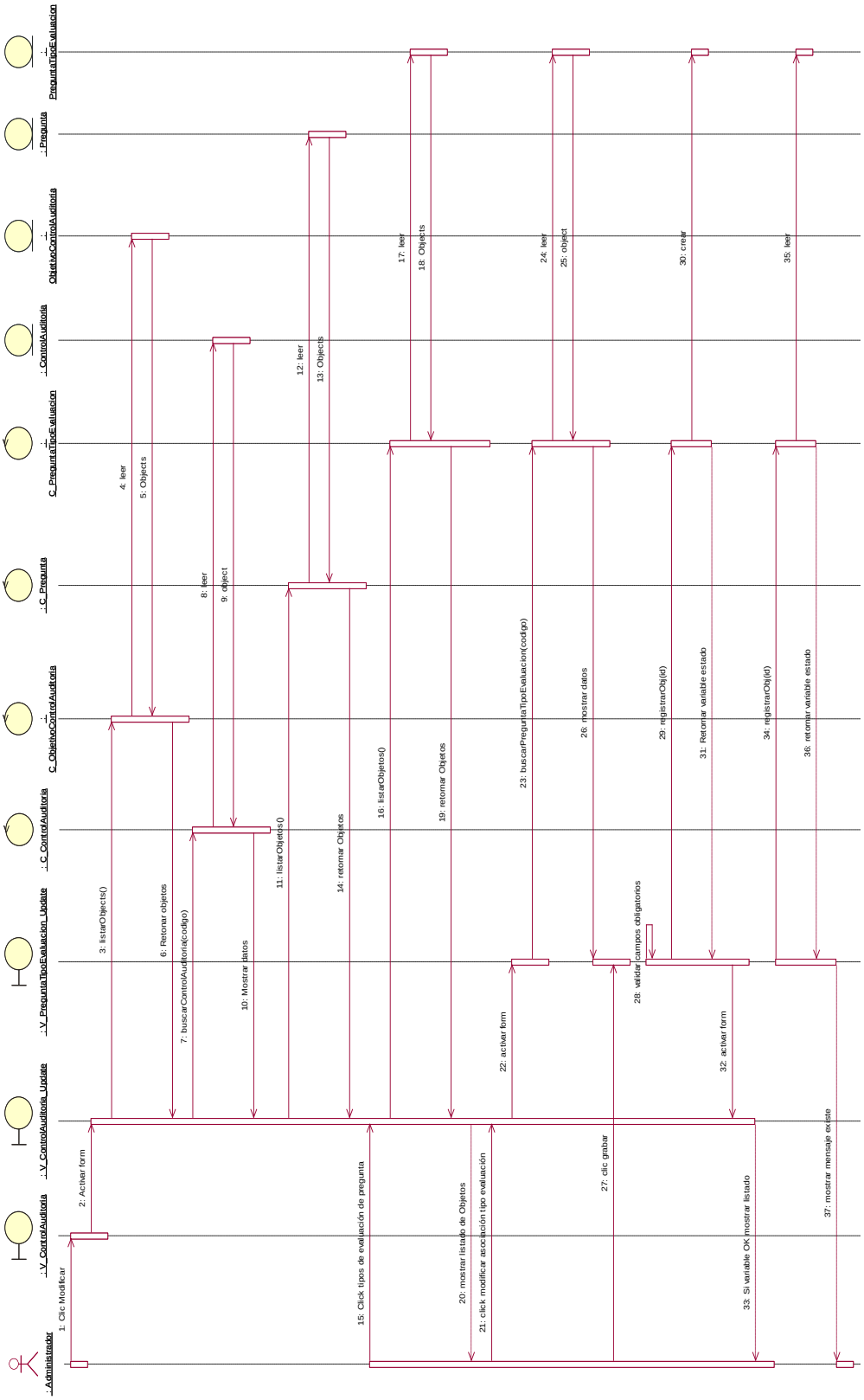


h. Pregunta – Tipo Evaluación

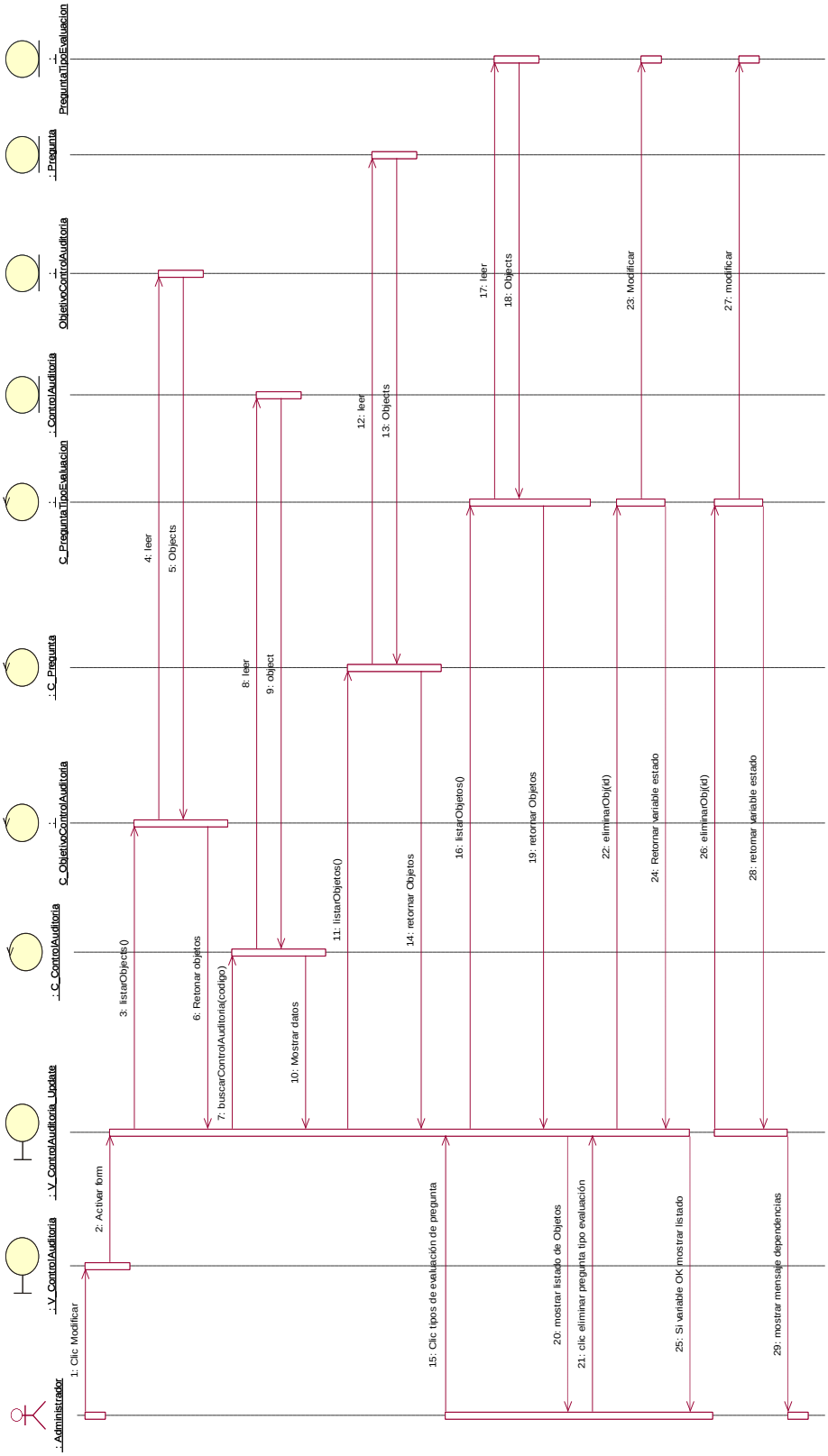
- Agregar tipo de evaluación – pregunta



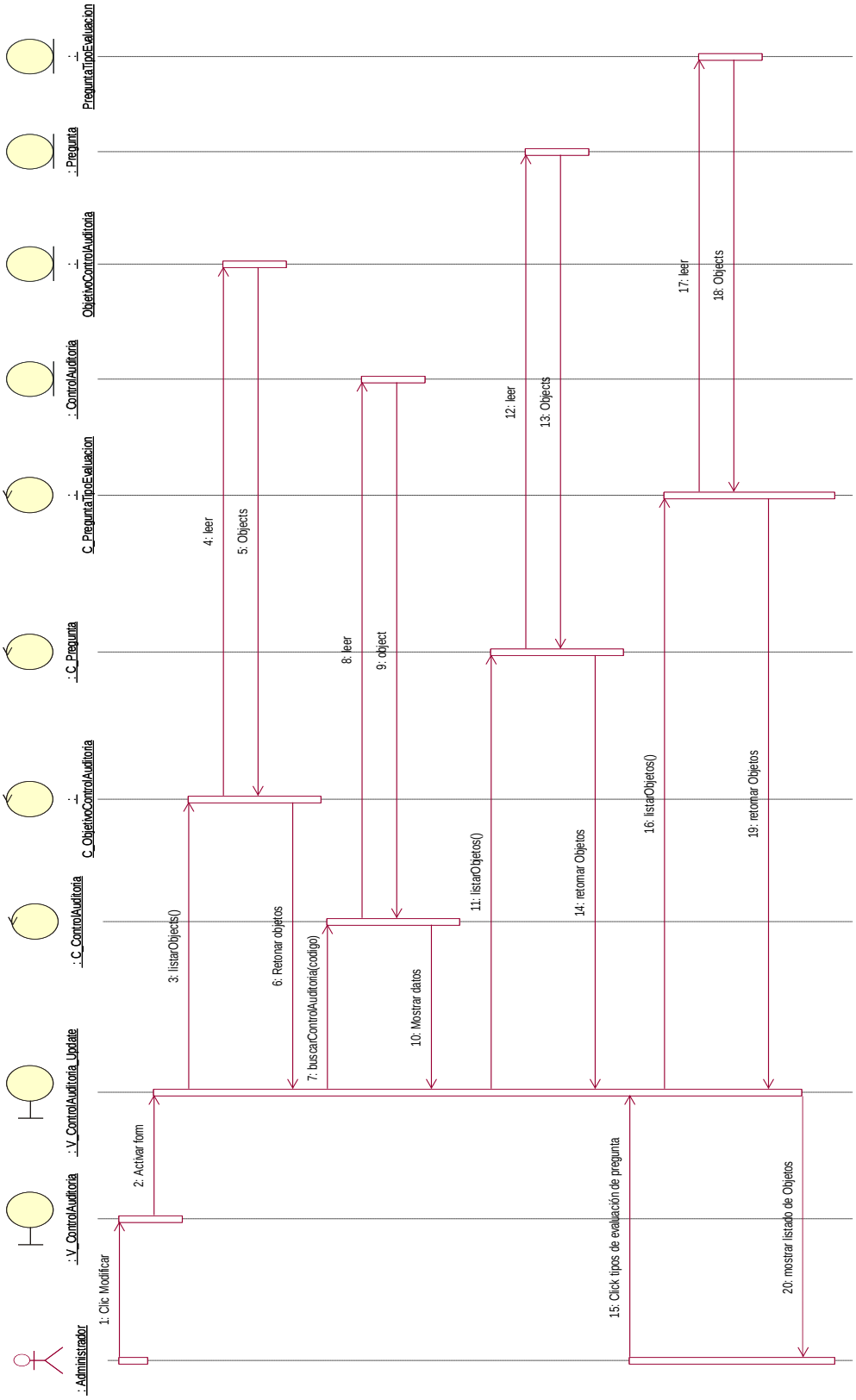
- **Modificar tipo de evaluación – pregunta**



- **Eliminar tipo de evaluación – pregunta**

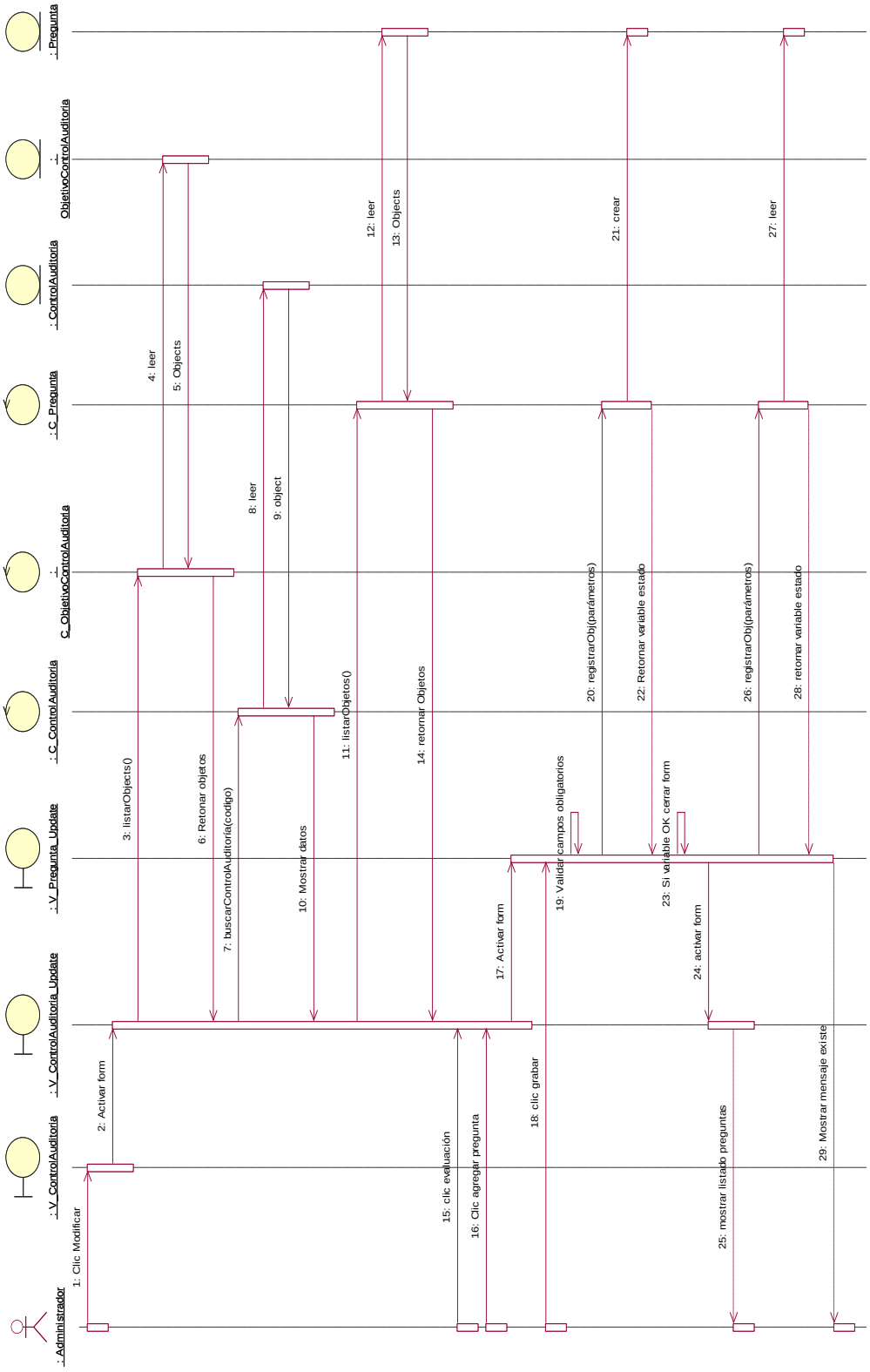


- **Listar tipo de evaluación – pregunta**

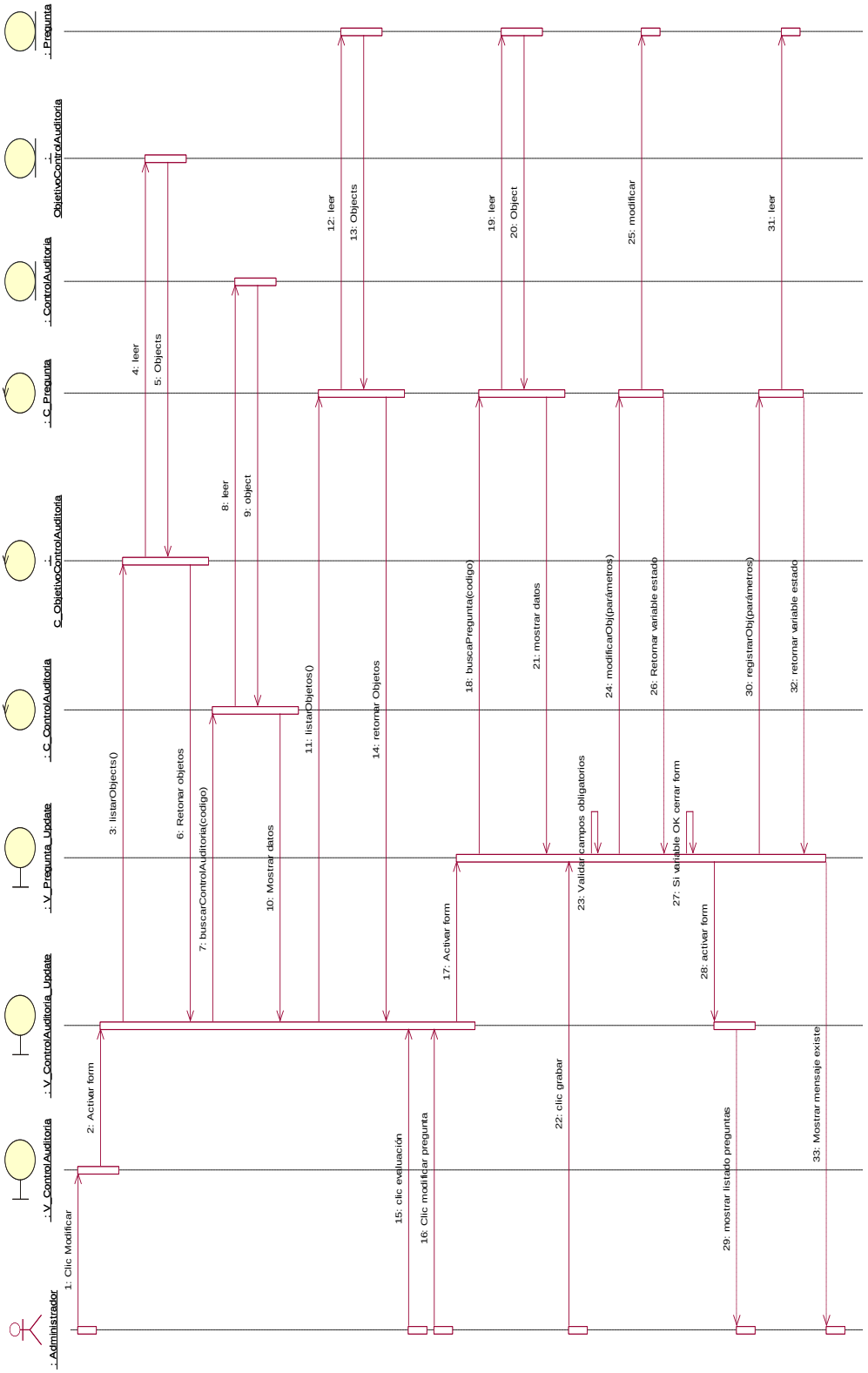


i. Pregunta – control auditoría

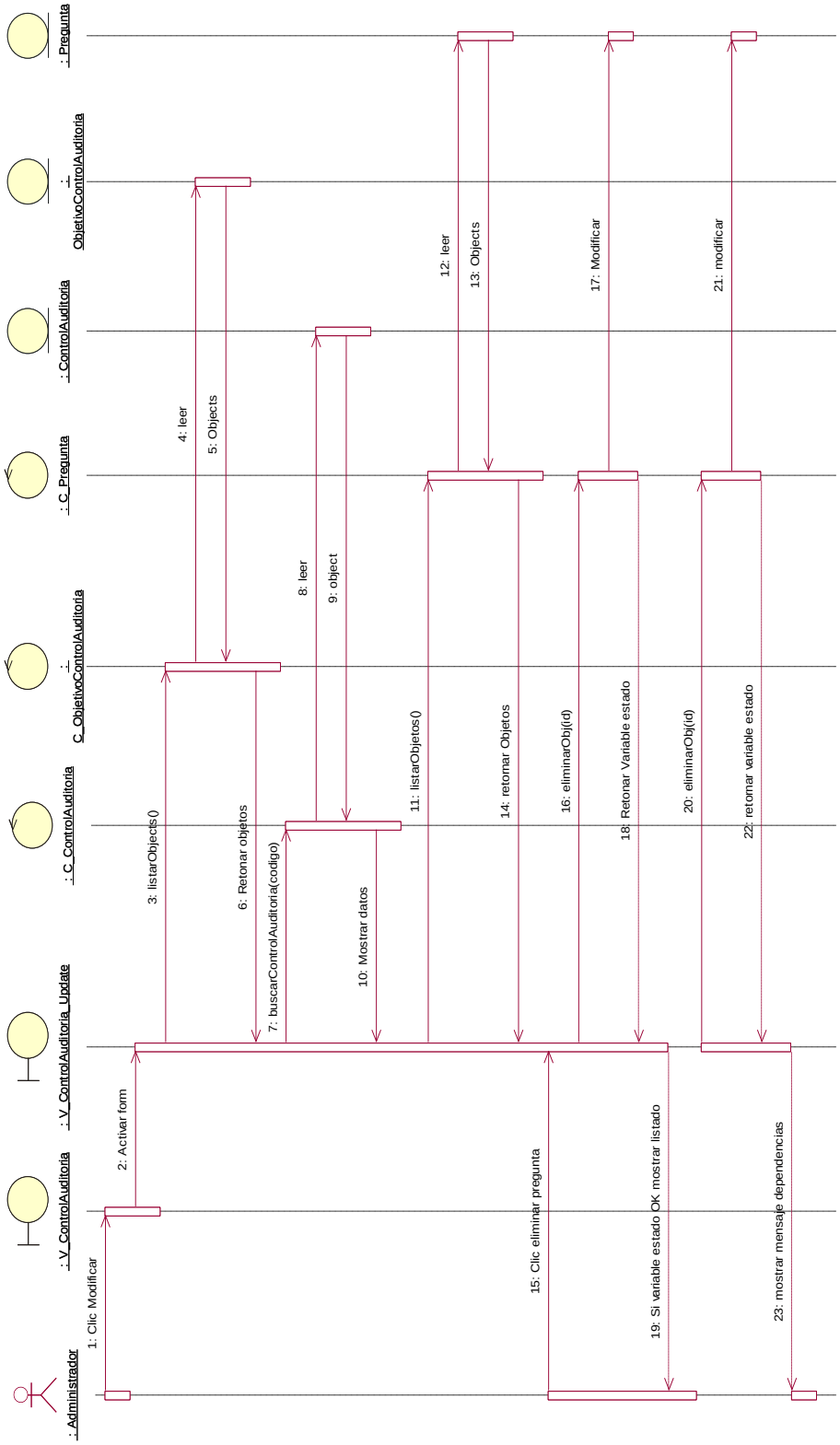
- Registrar pregunta control auditoría



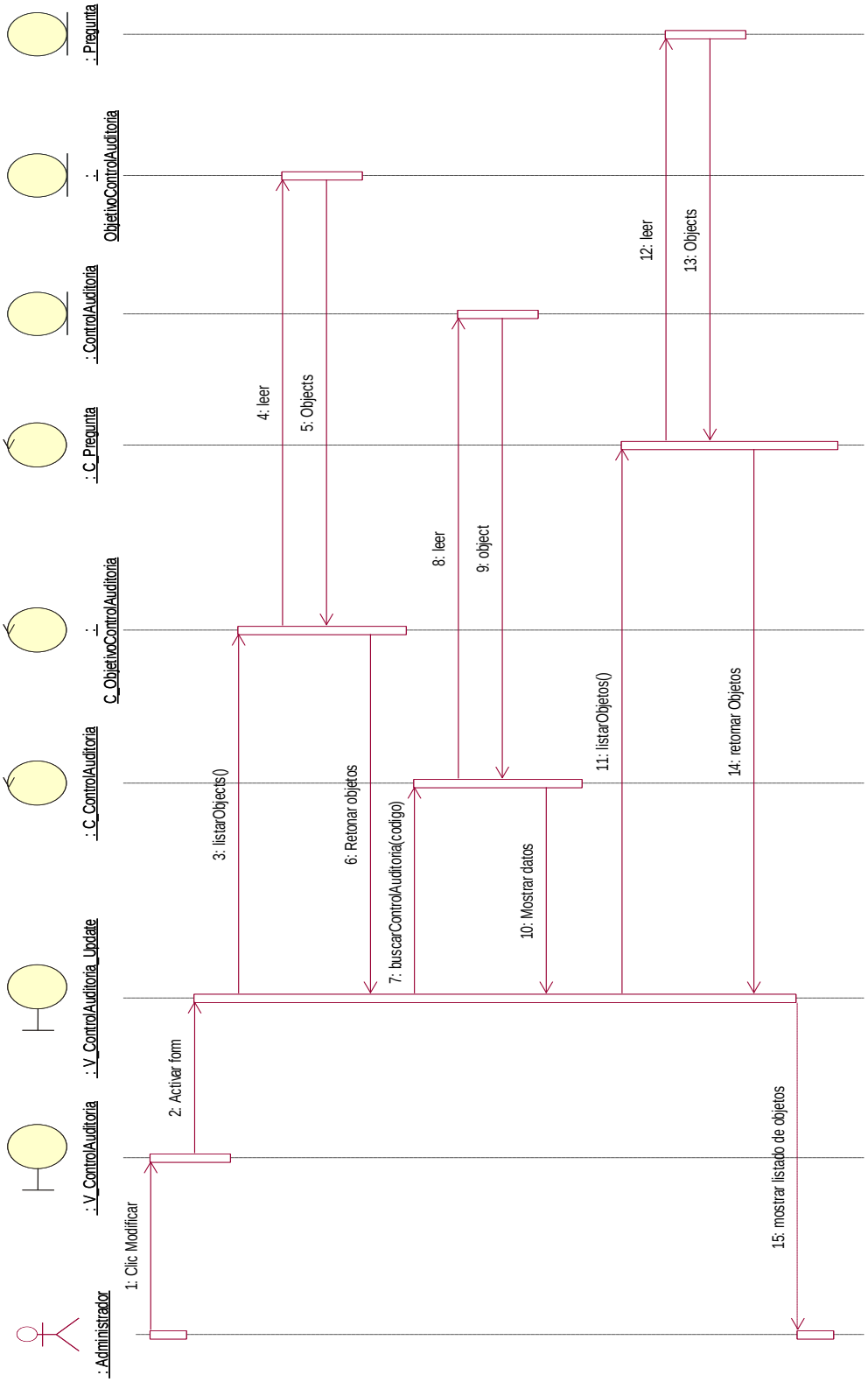
- **Modificar pregunta control auditoría**



- **Eliminar pregunta control auditoría**

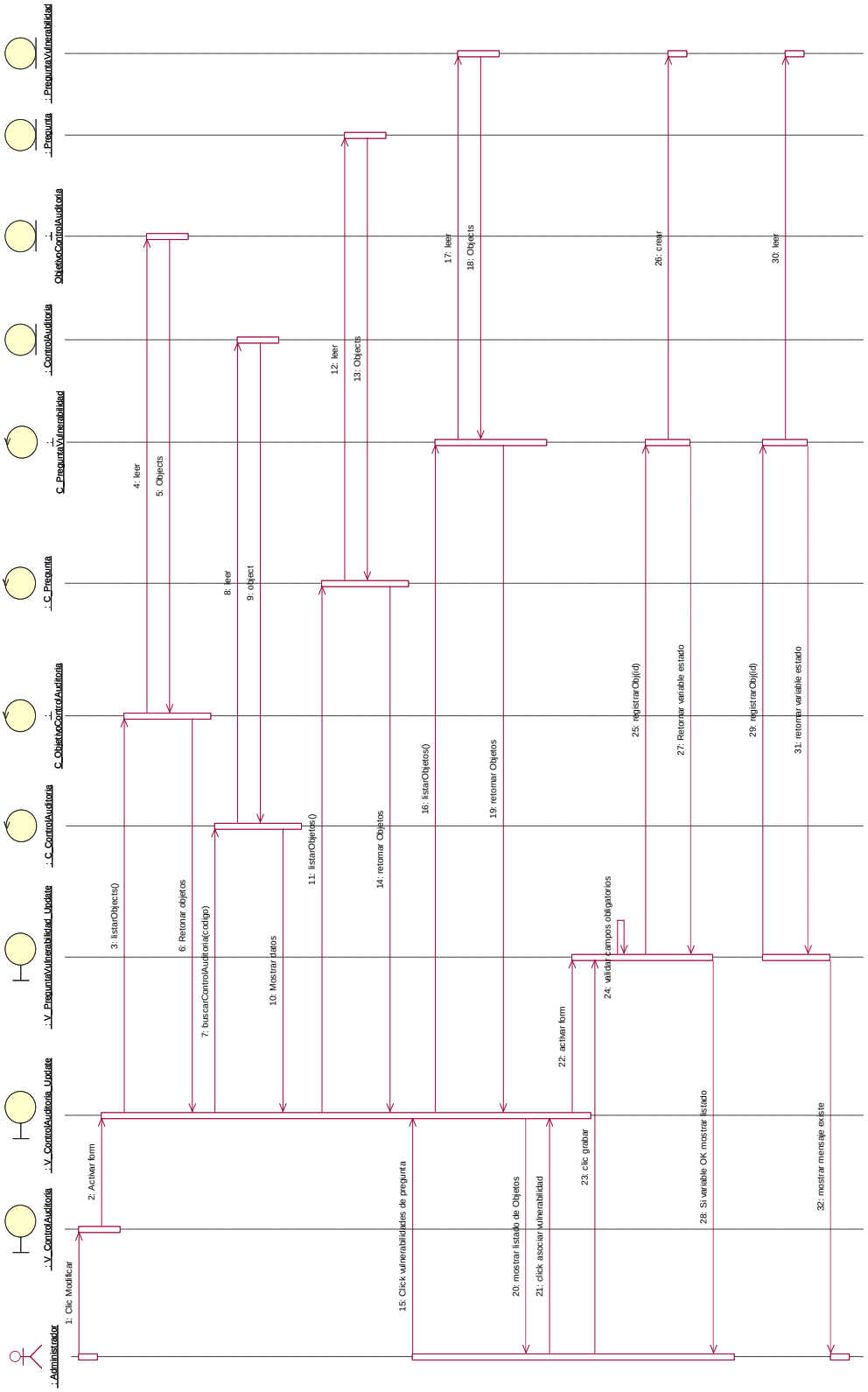


- **Listar preguntas control auditoría**

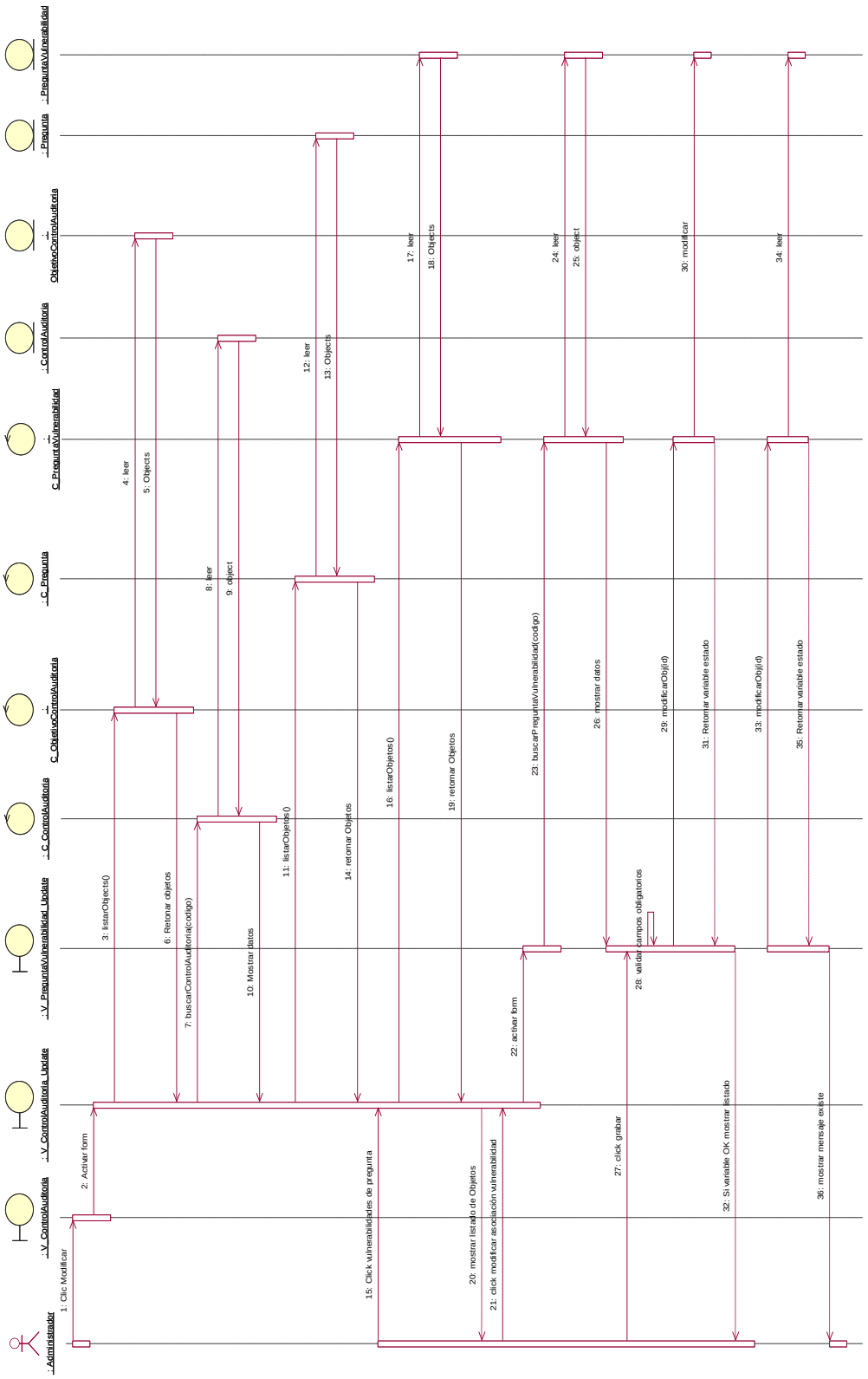


j. Pregunta - Vulnerabilidad

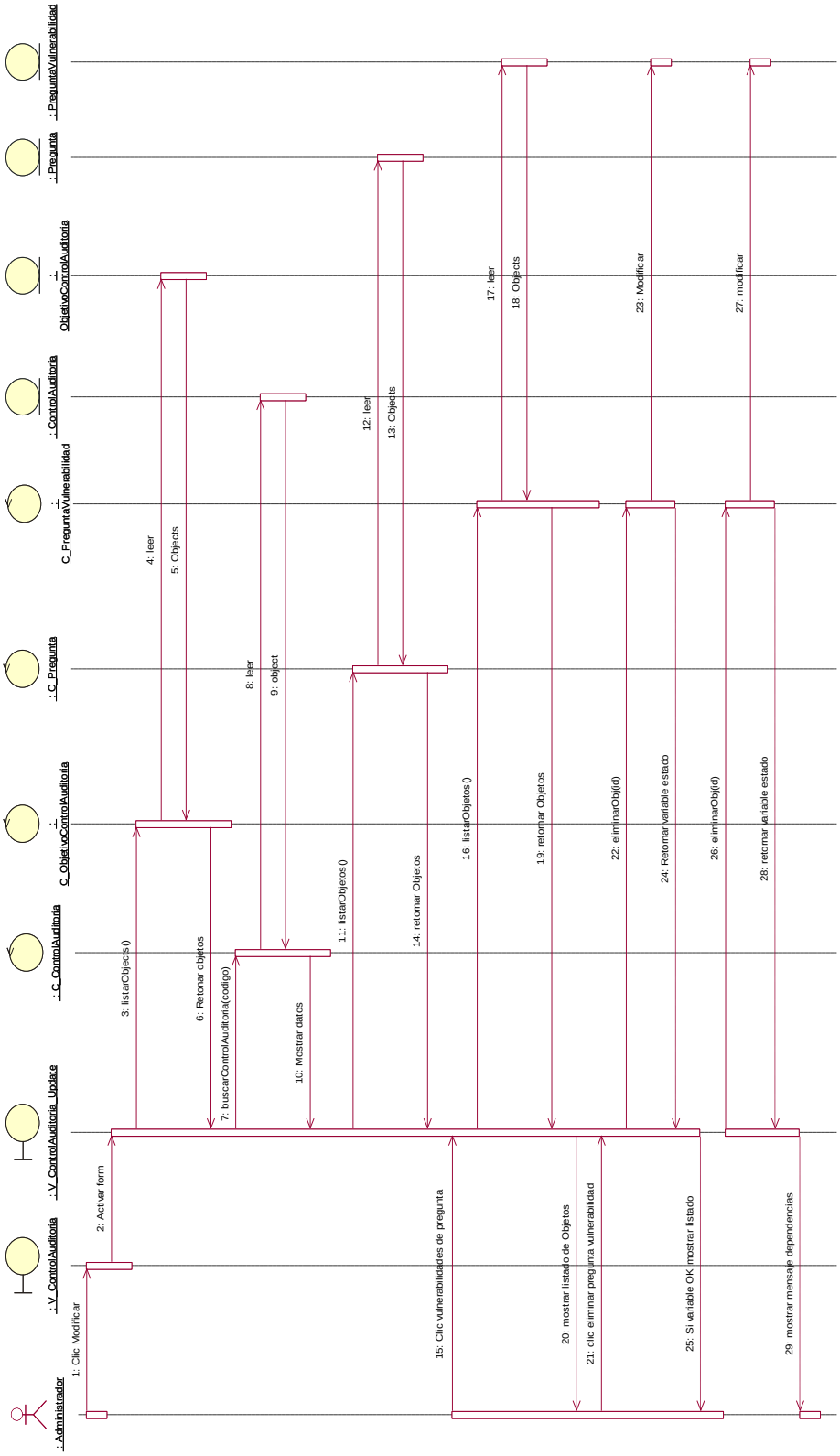
- Asociar pregunta – vulnerabilidad



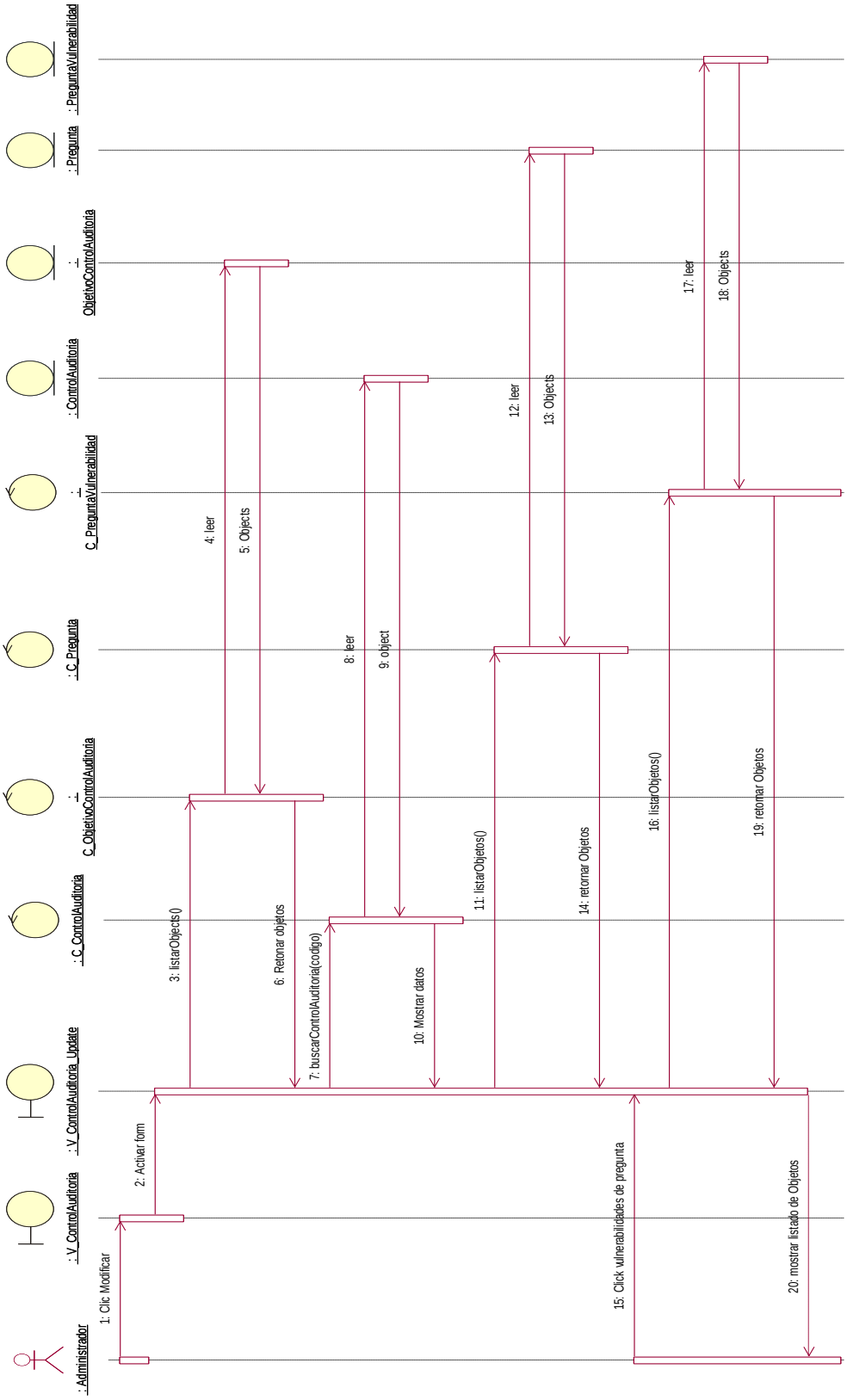
- **Modificar asociación pregunta – vulnerabilidad**



- **Eliminar asociación pregunta – vulnerabilidad**

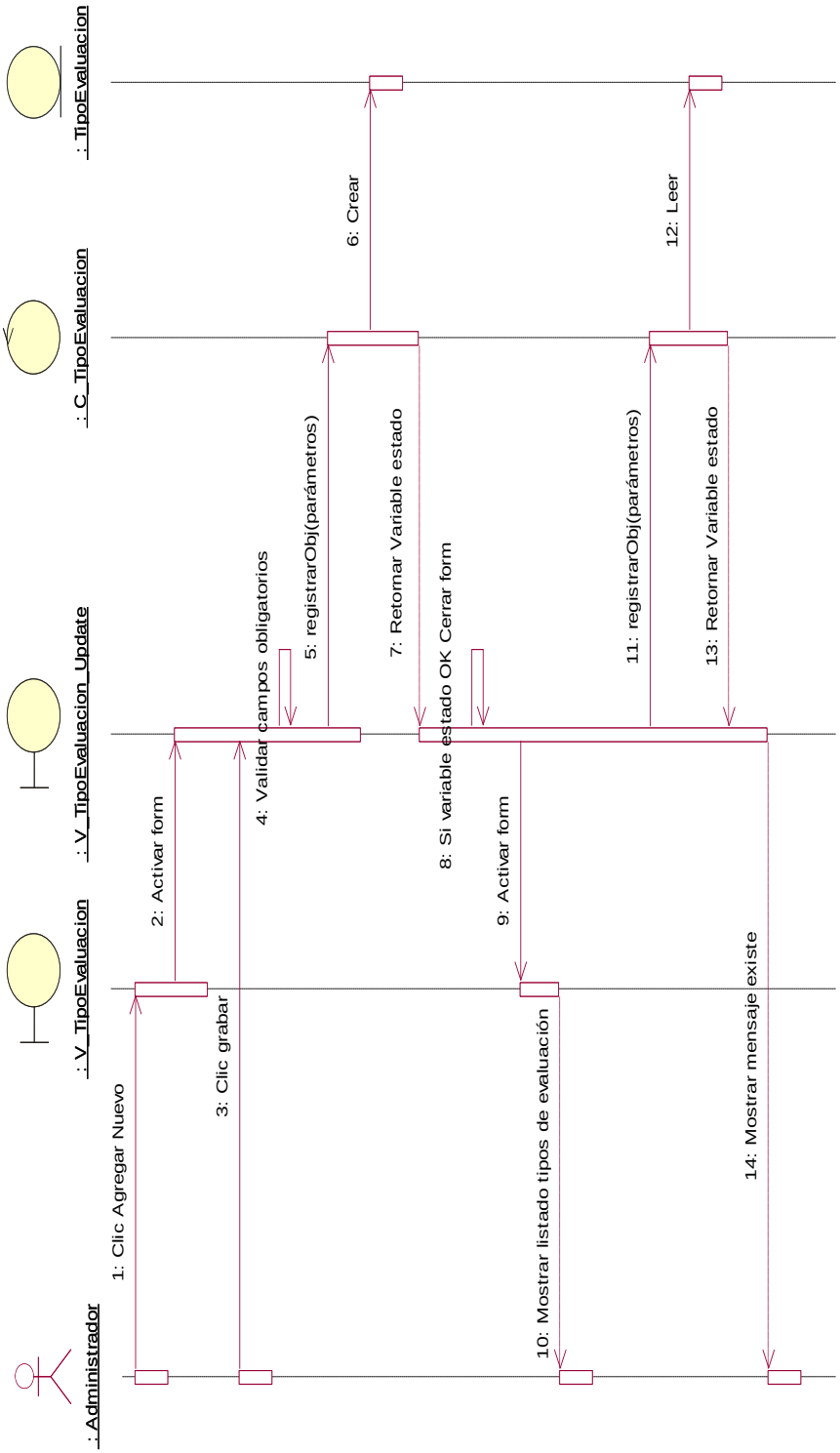


- **Listar vulnerabilidades - pregunta**

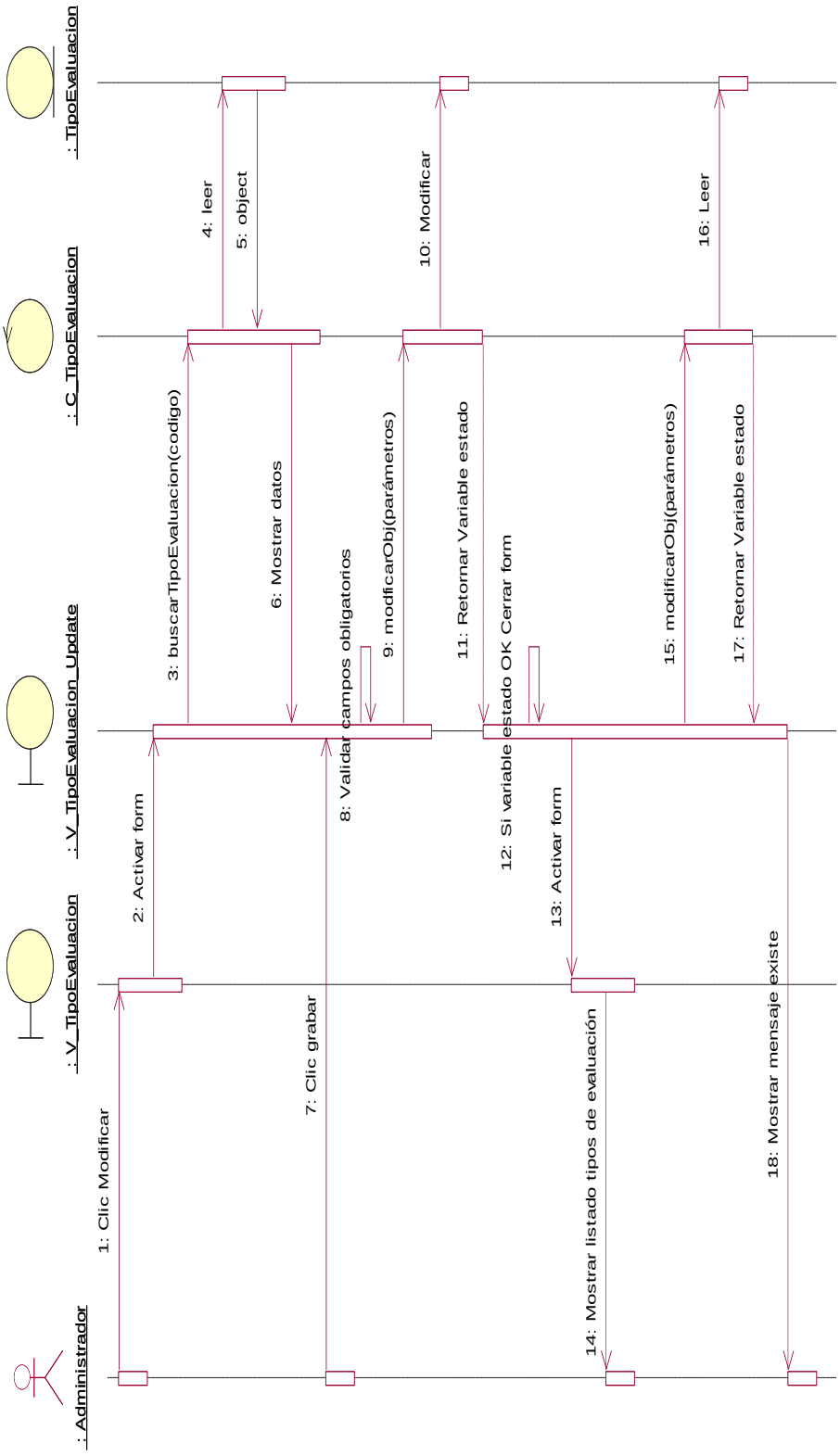


k. Tipos de Evaluación

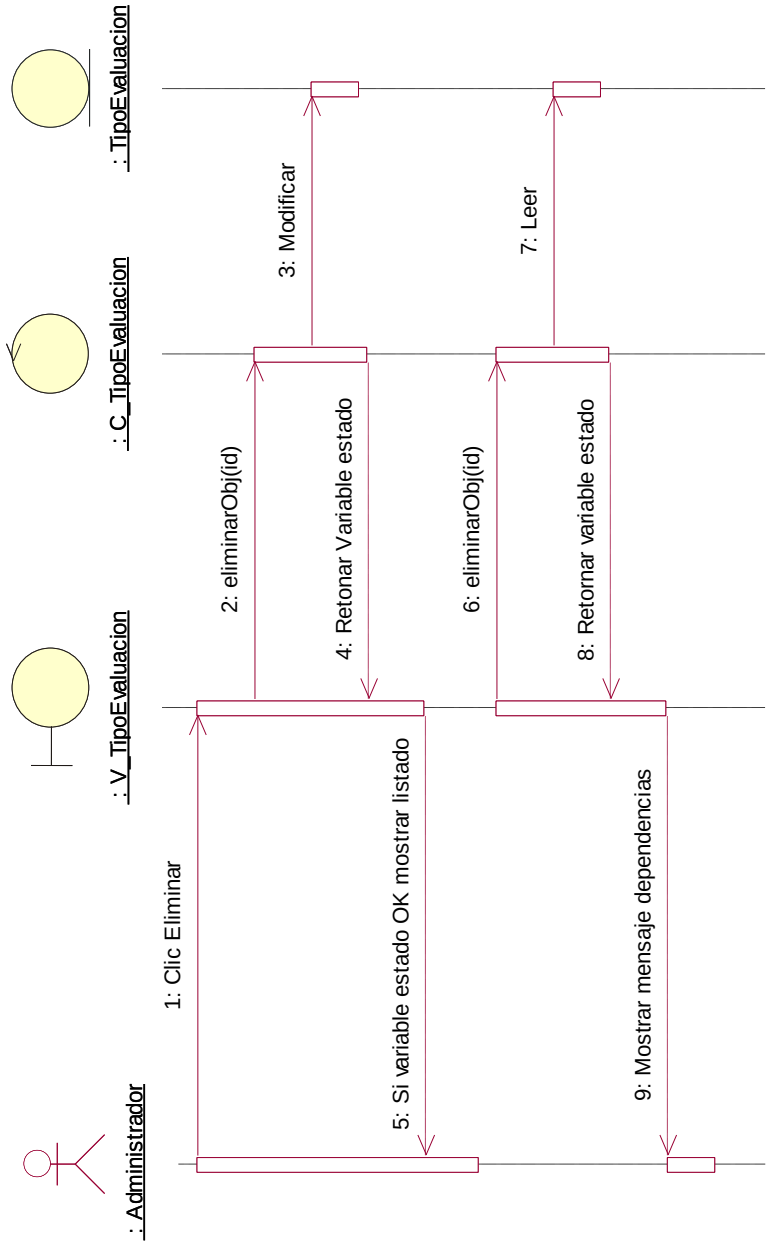
- Registrar tipo evaluación



- **Modificar tipo evaluación**

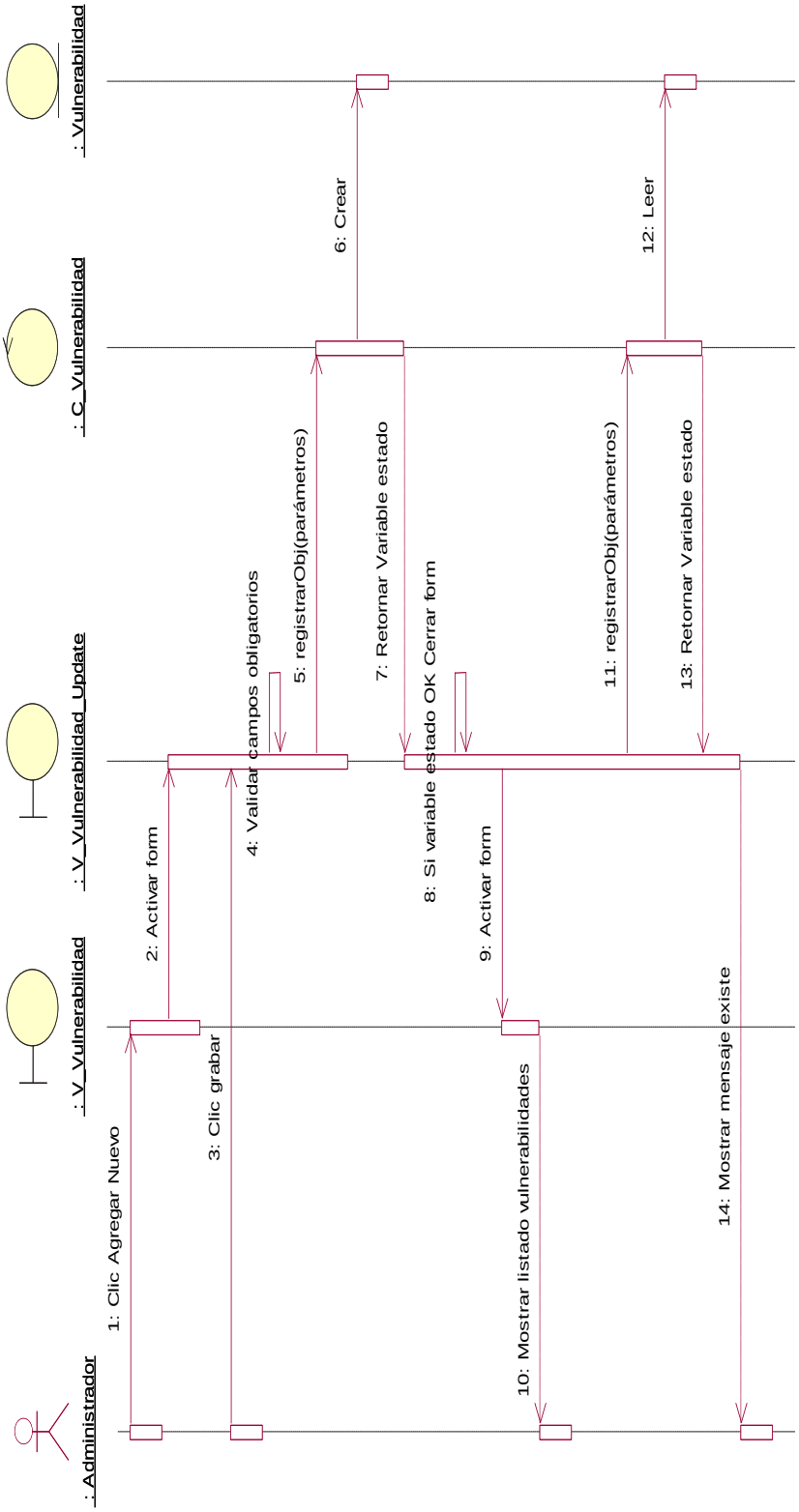


- **Eliminar tipo evaluación**

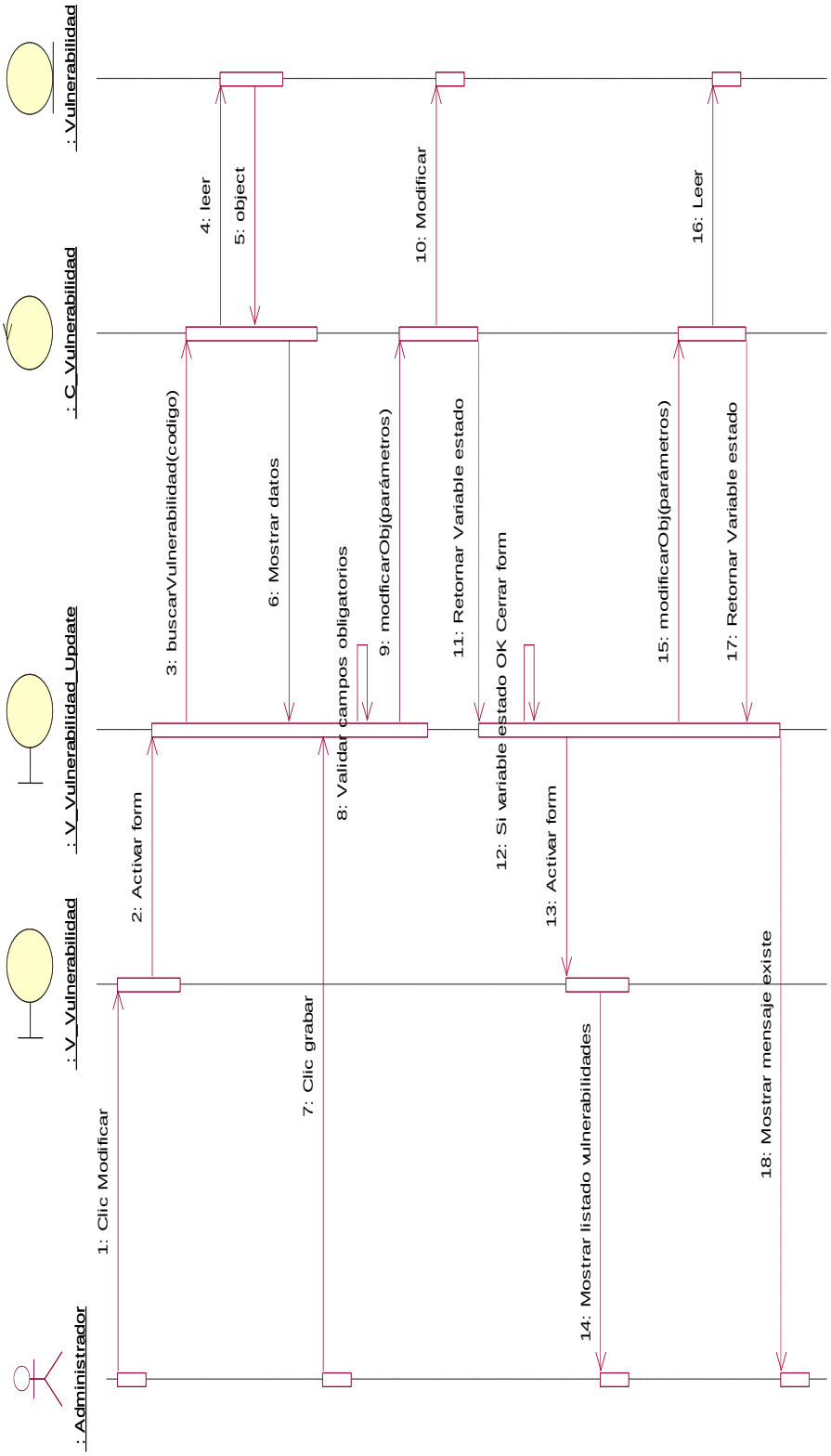


l. Vulnerabilidad

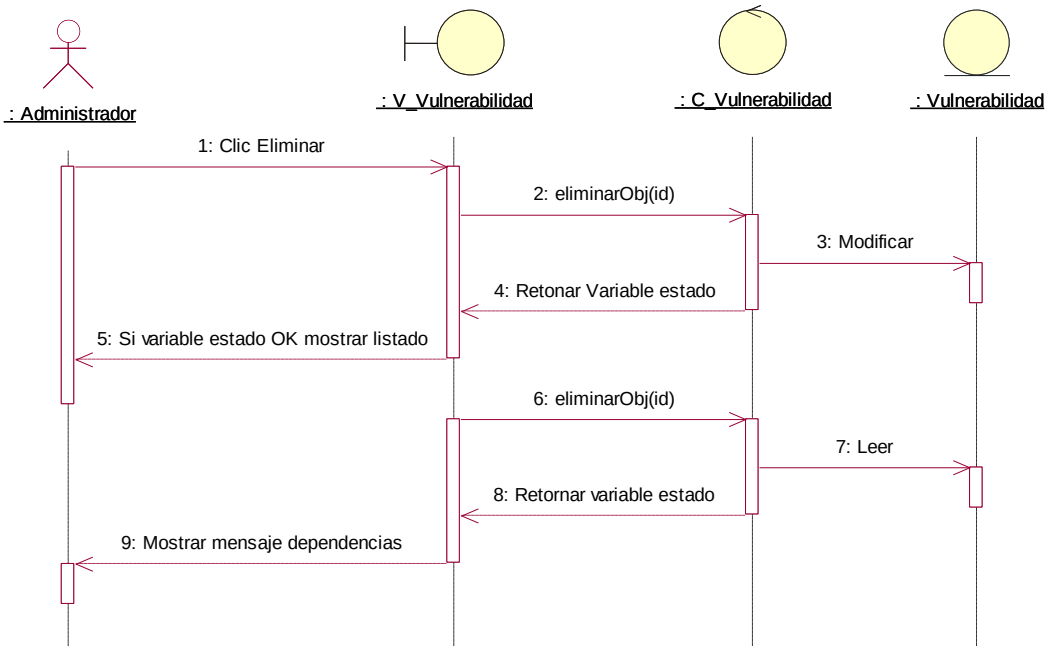
- Registrar vulnerabilidad



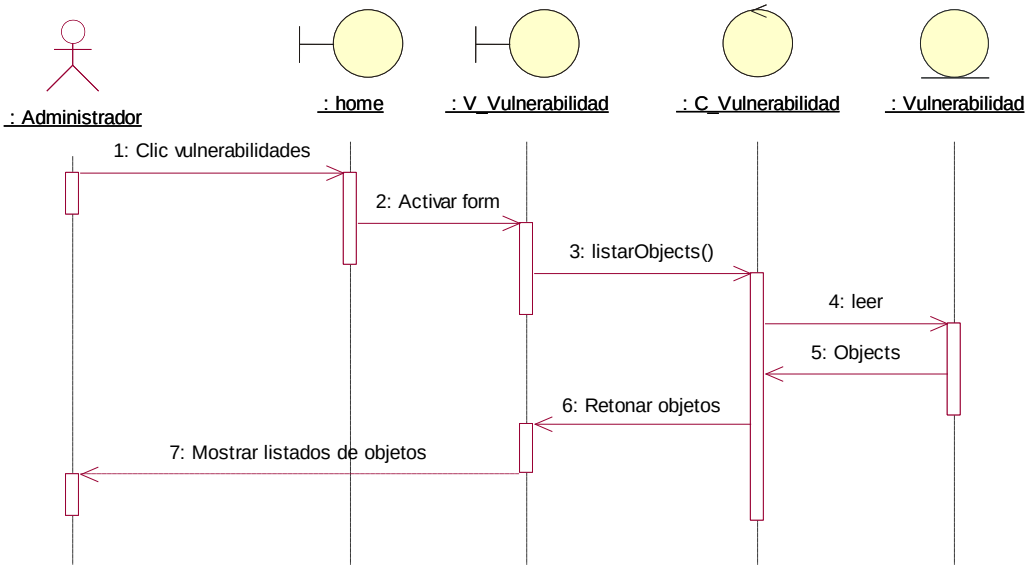
- **Modificar vulnerabilidad**



- **Eliminar vulnerabilidad**

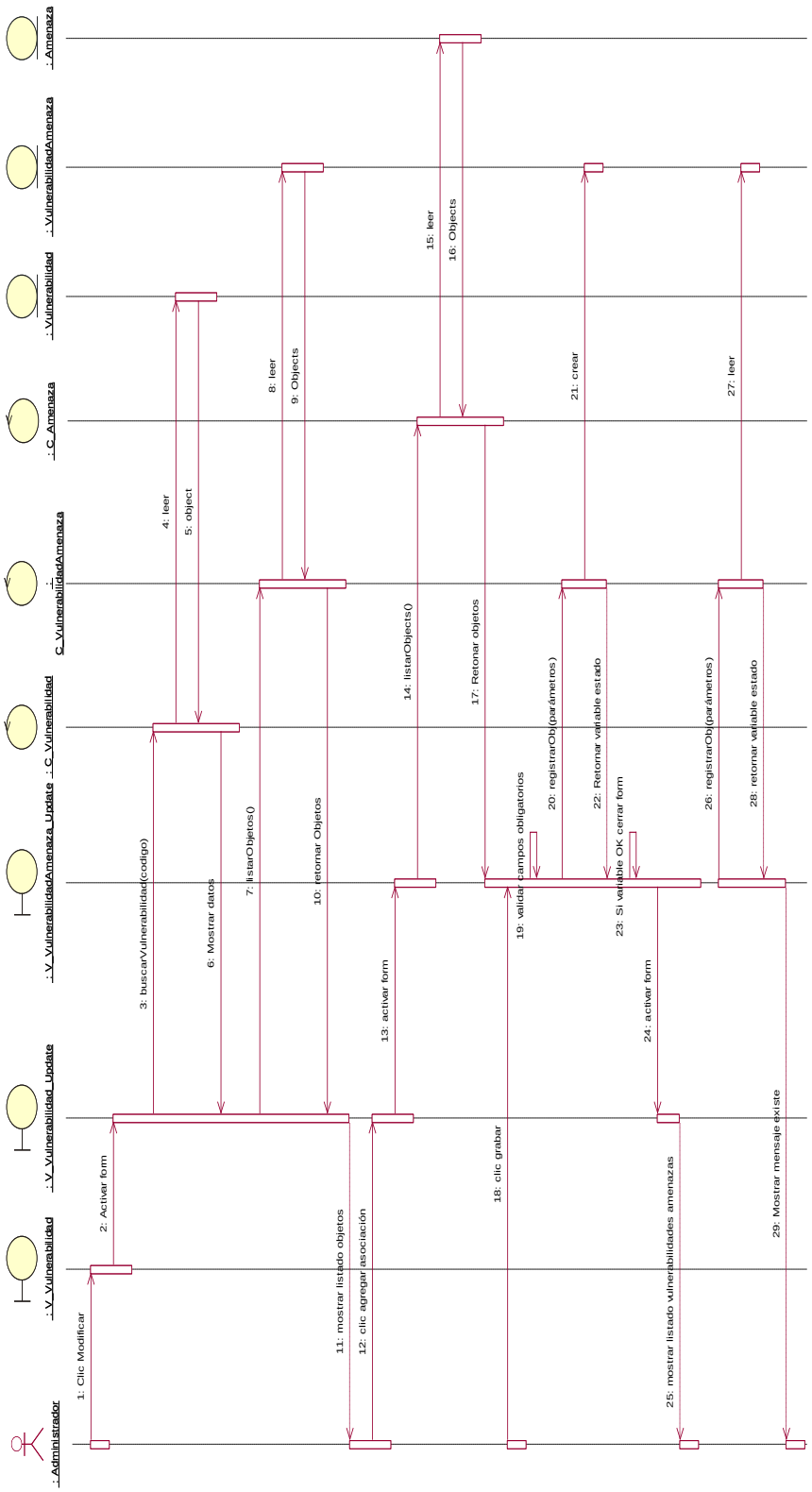


- **Listar vulnerabilidades**

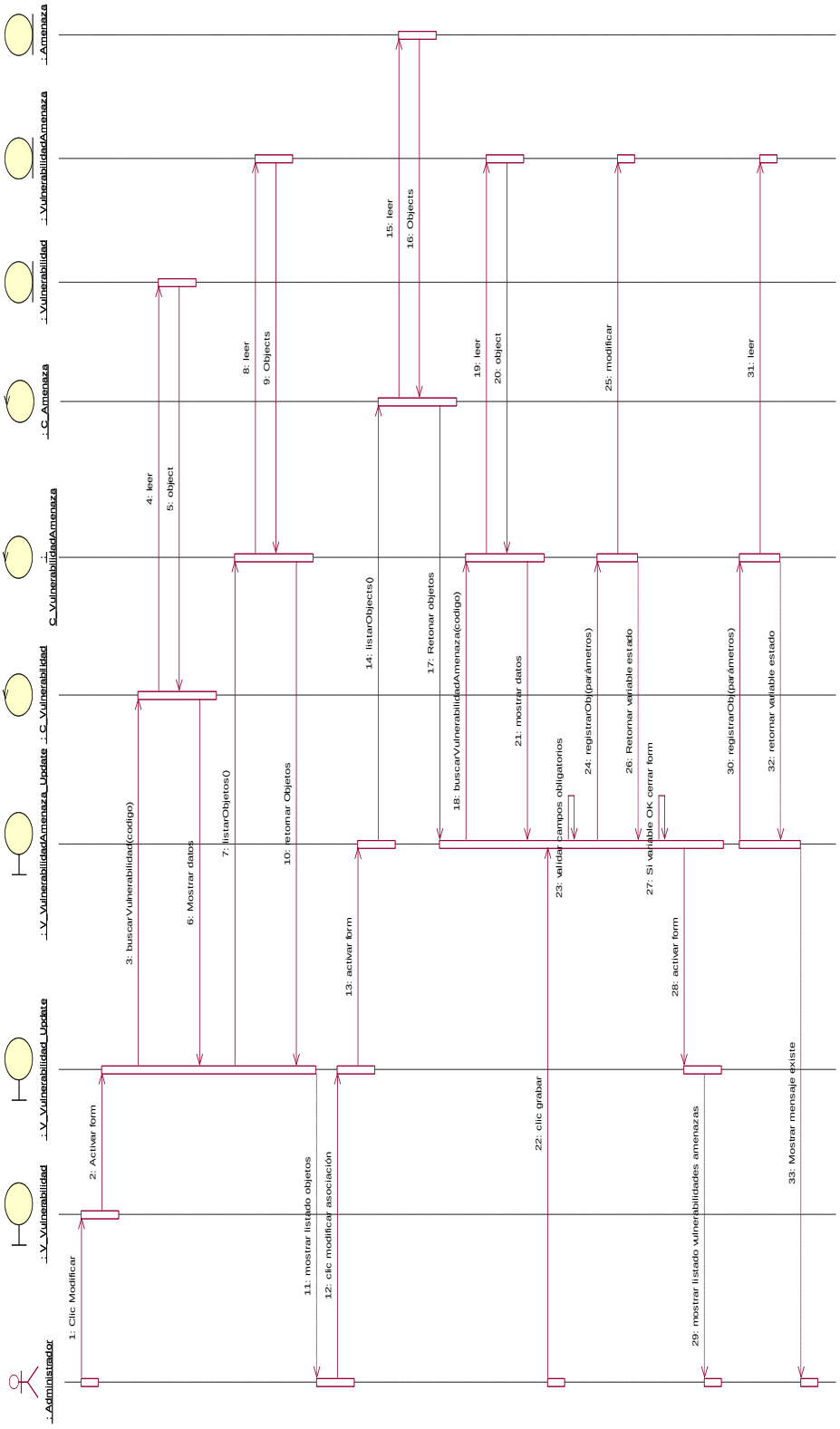


m. Vulnerabilidad - Amenaza

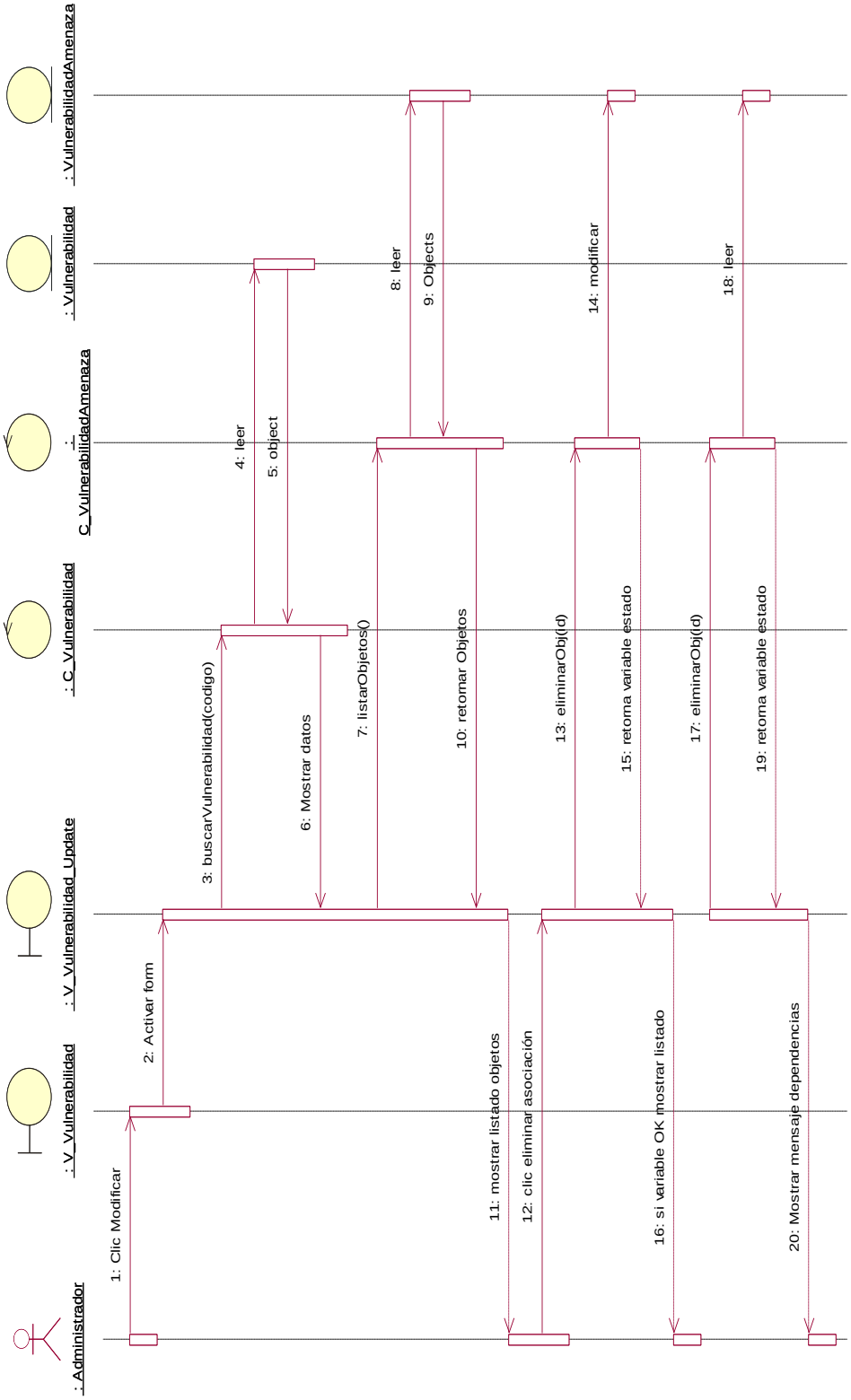
- Asociar vulnerabilidad amenaza



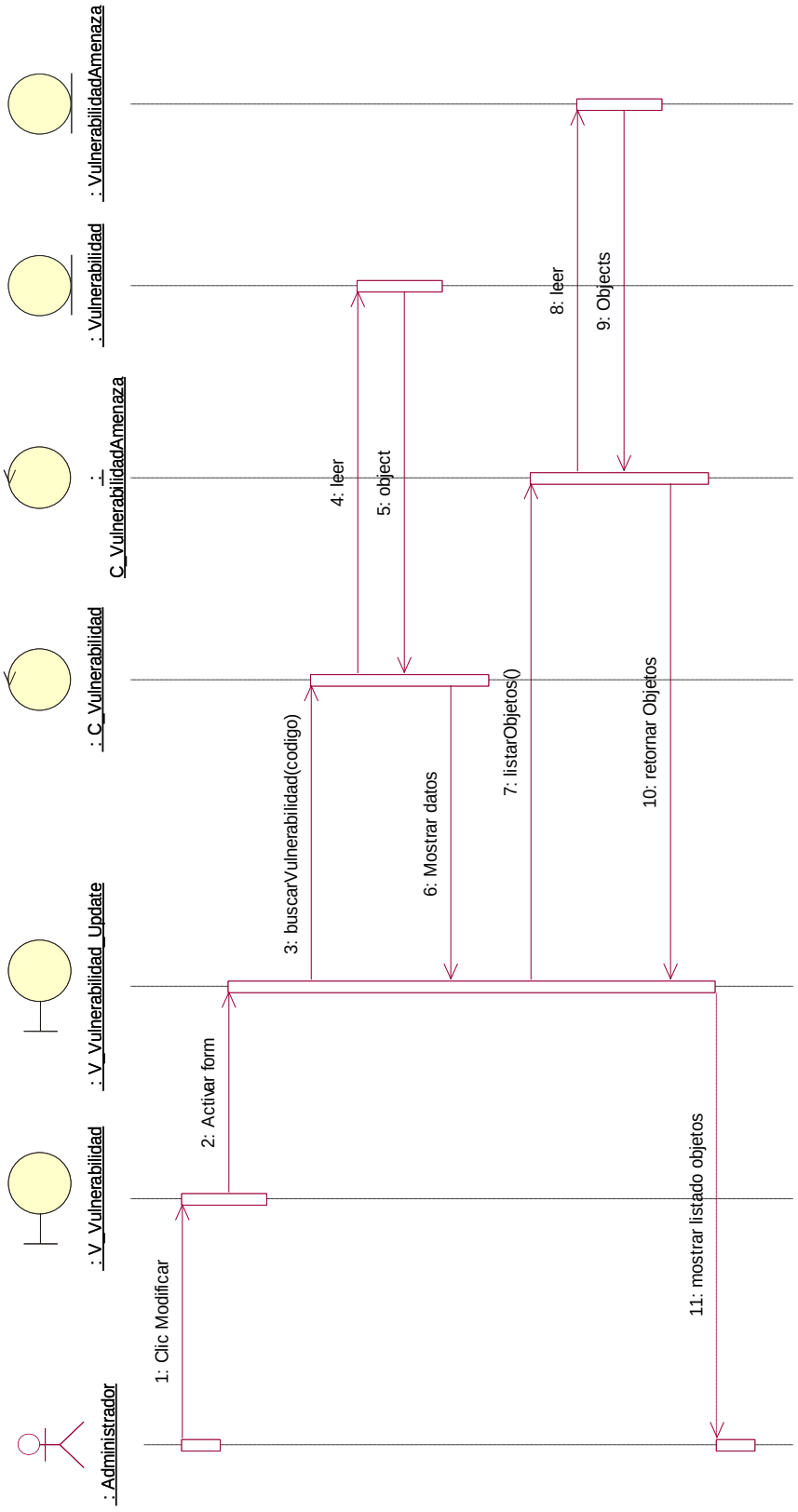
- **Modificar asociación vulnerabilidad – amenaza**



- **Eliminar asociación vulnerabilidad – amenaza**

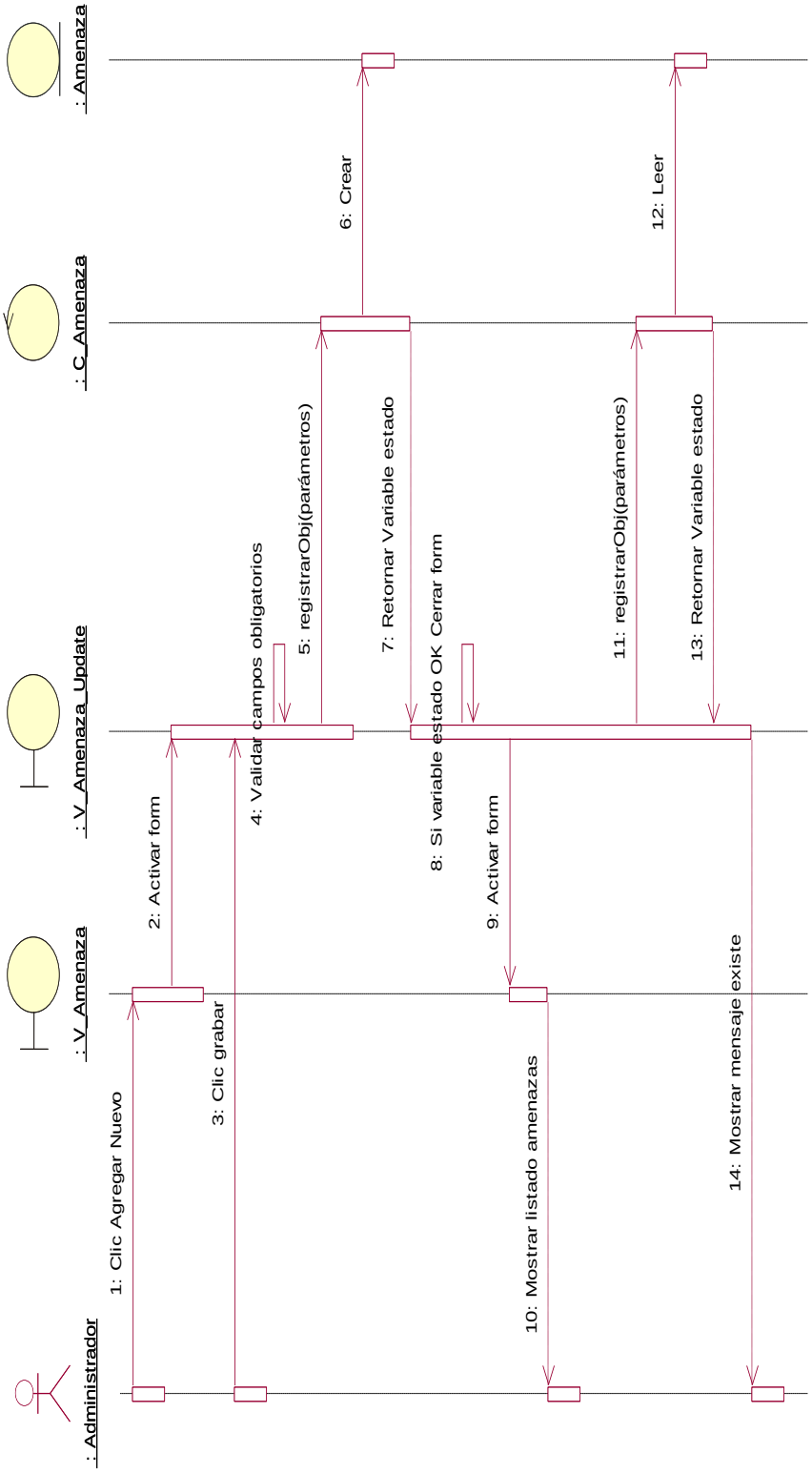


- **Listar vulnerabilidades – amenazas**

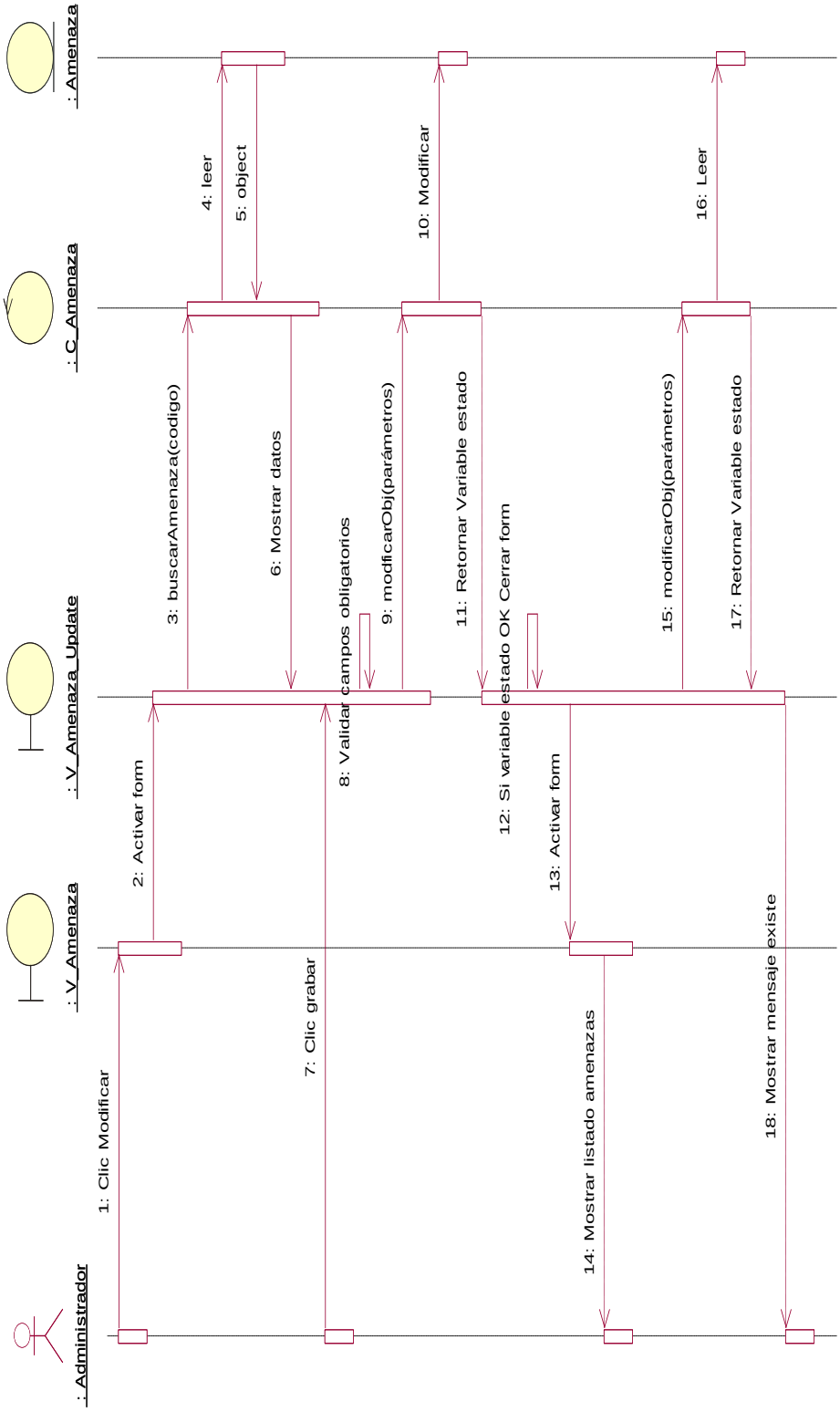


n. Amenazas

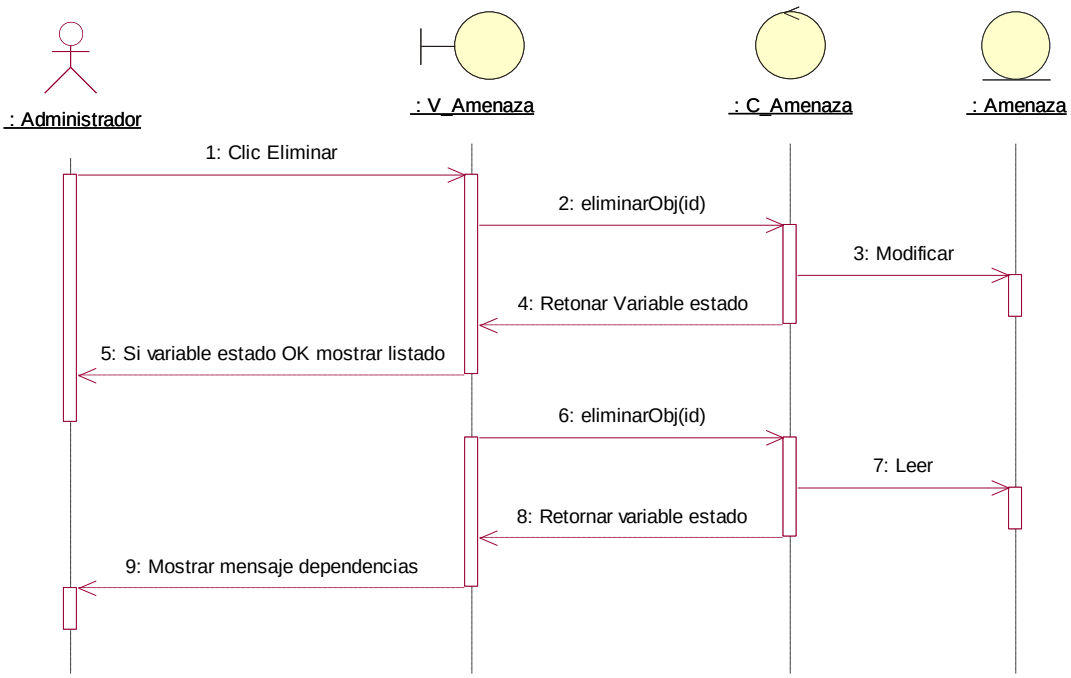
- **Registrar amenaza**



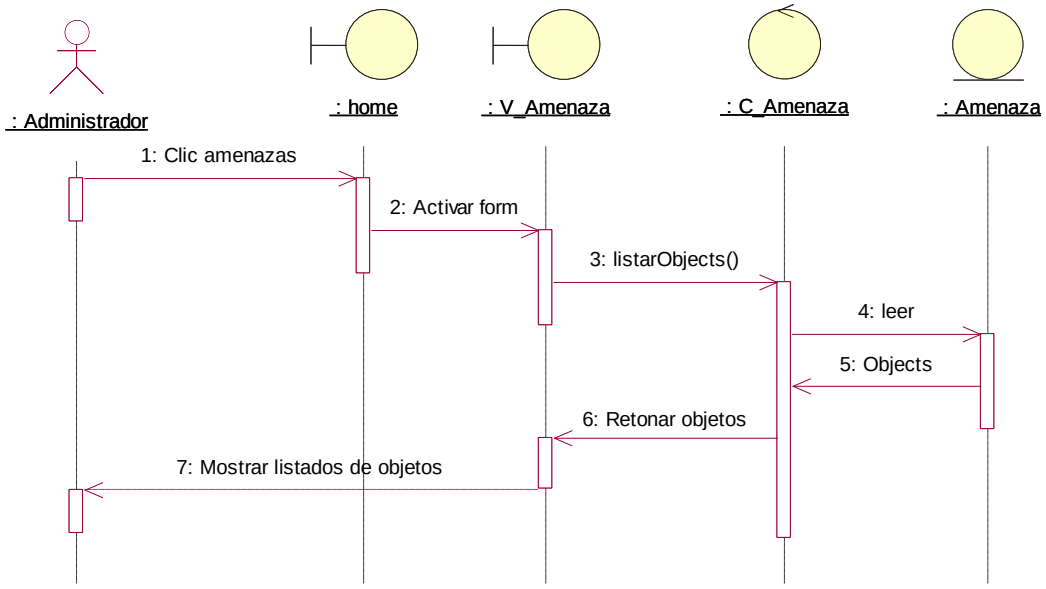
- **Modificar amenaza**



- **Eliminar amenaza**

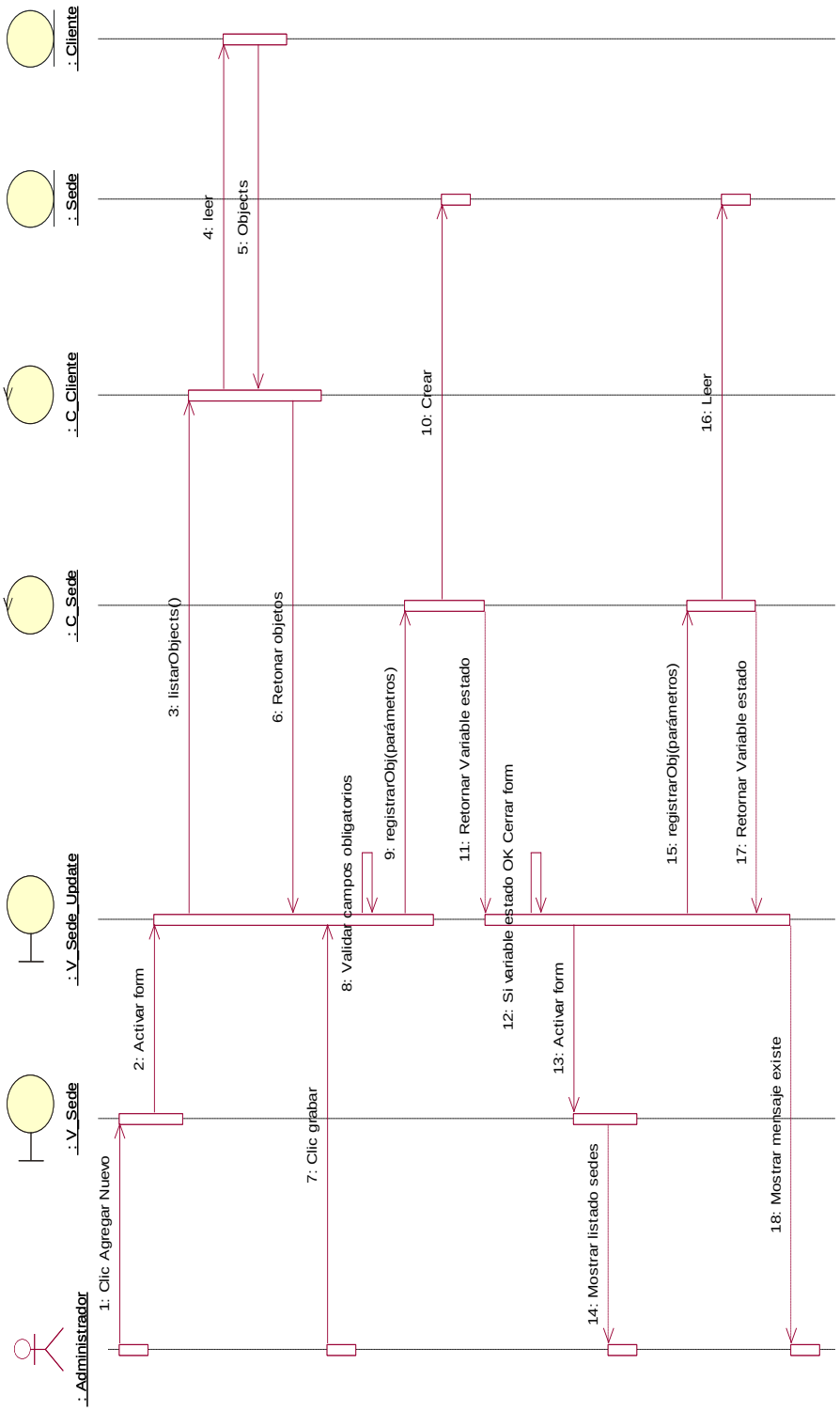


- **Listar amenazas**

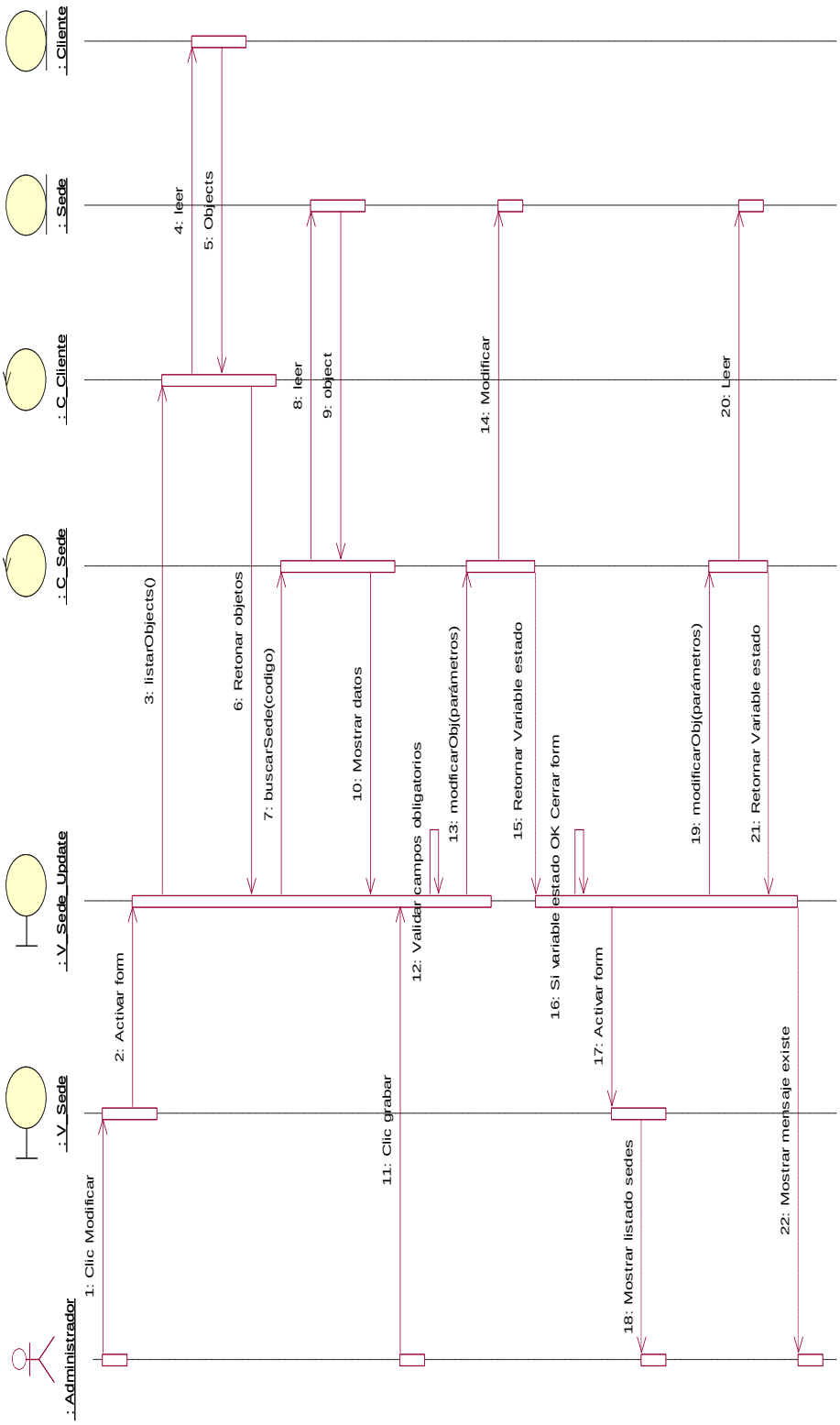


Módulo Auditoría

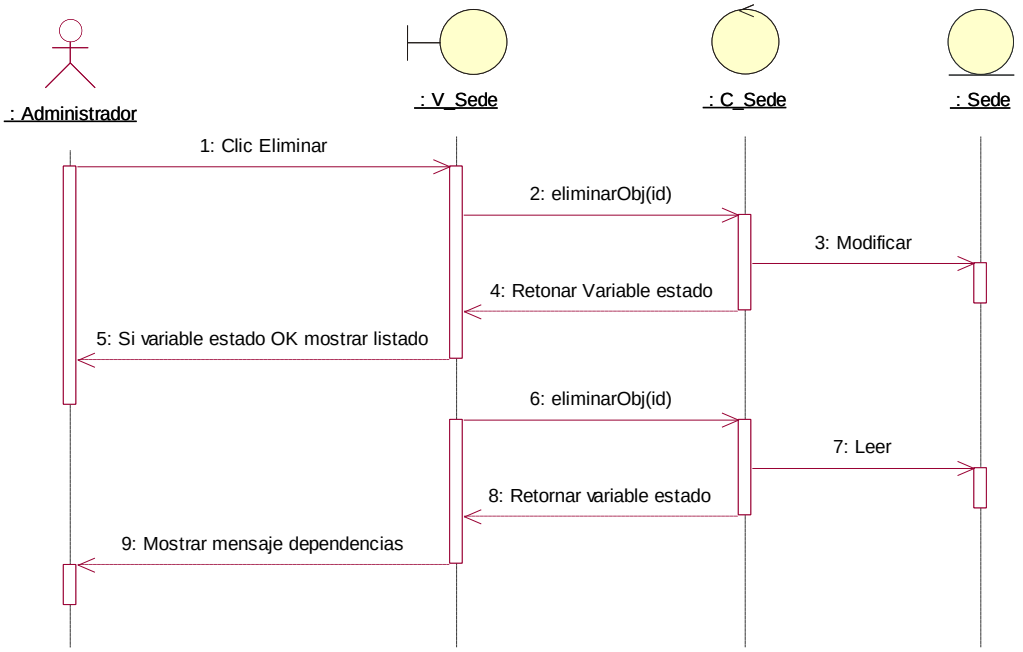
- **Registrar sedes**



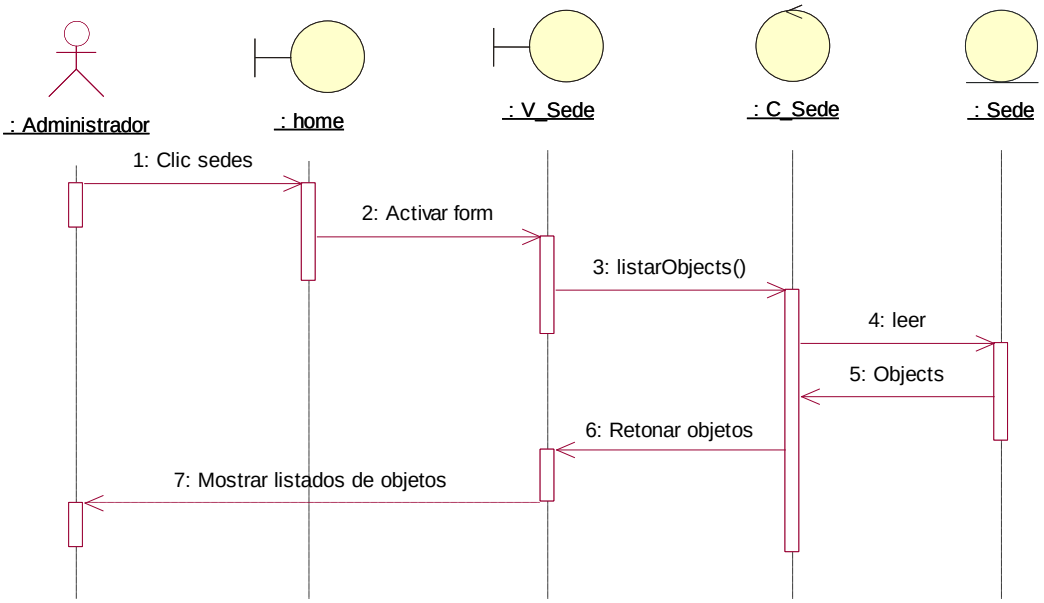
- **Modificar sede**



- **Eliminar sede**

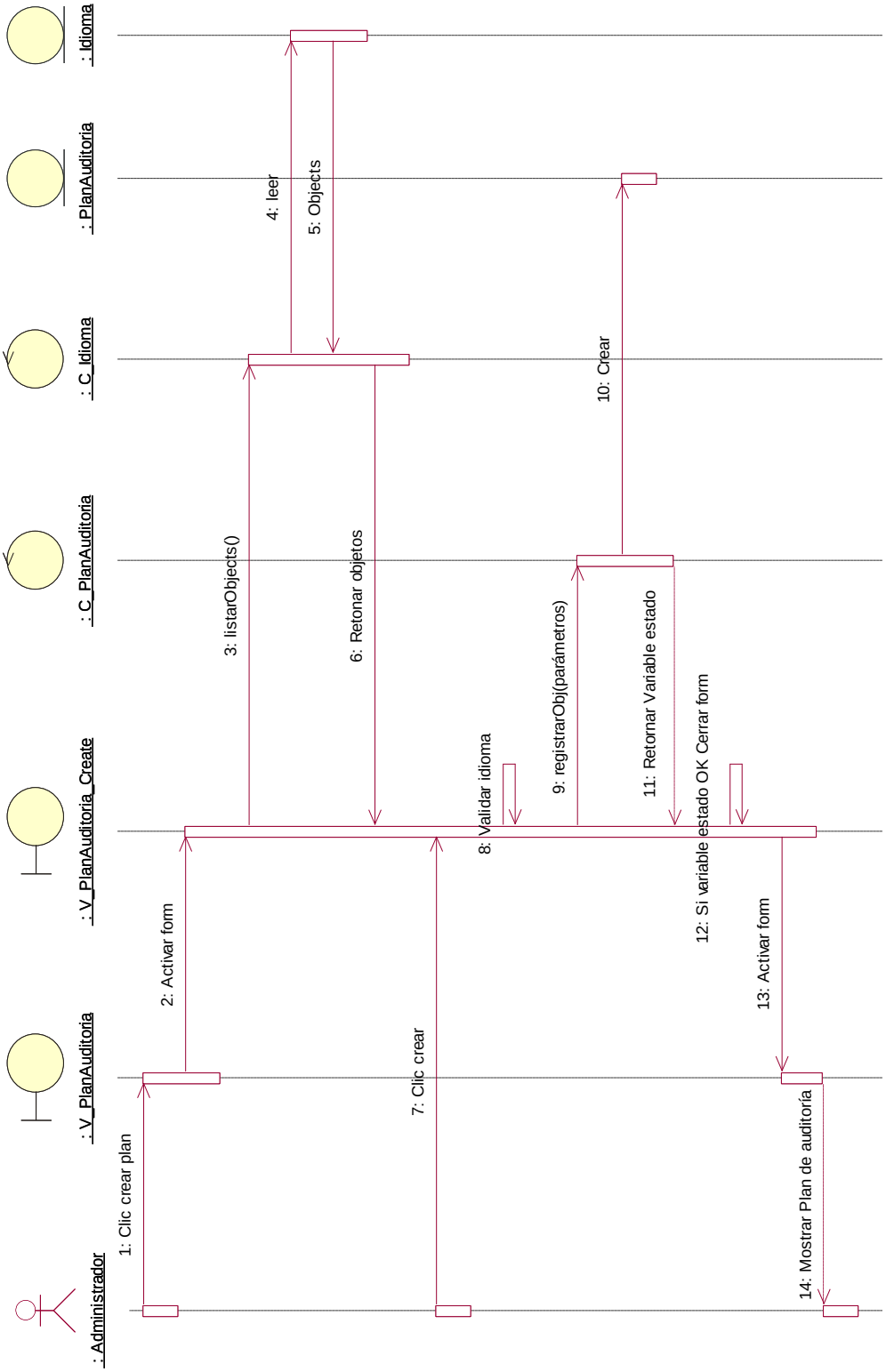


- **Listar sedes**

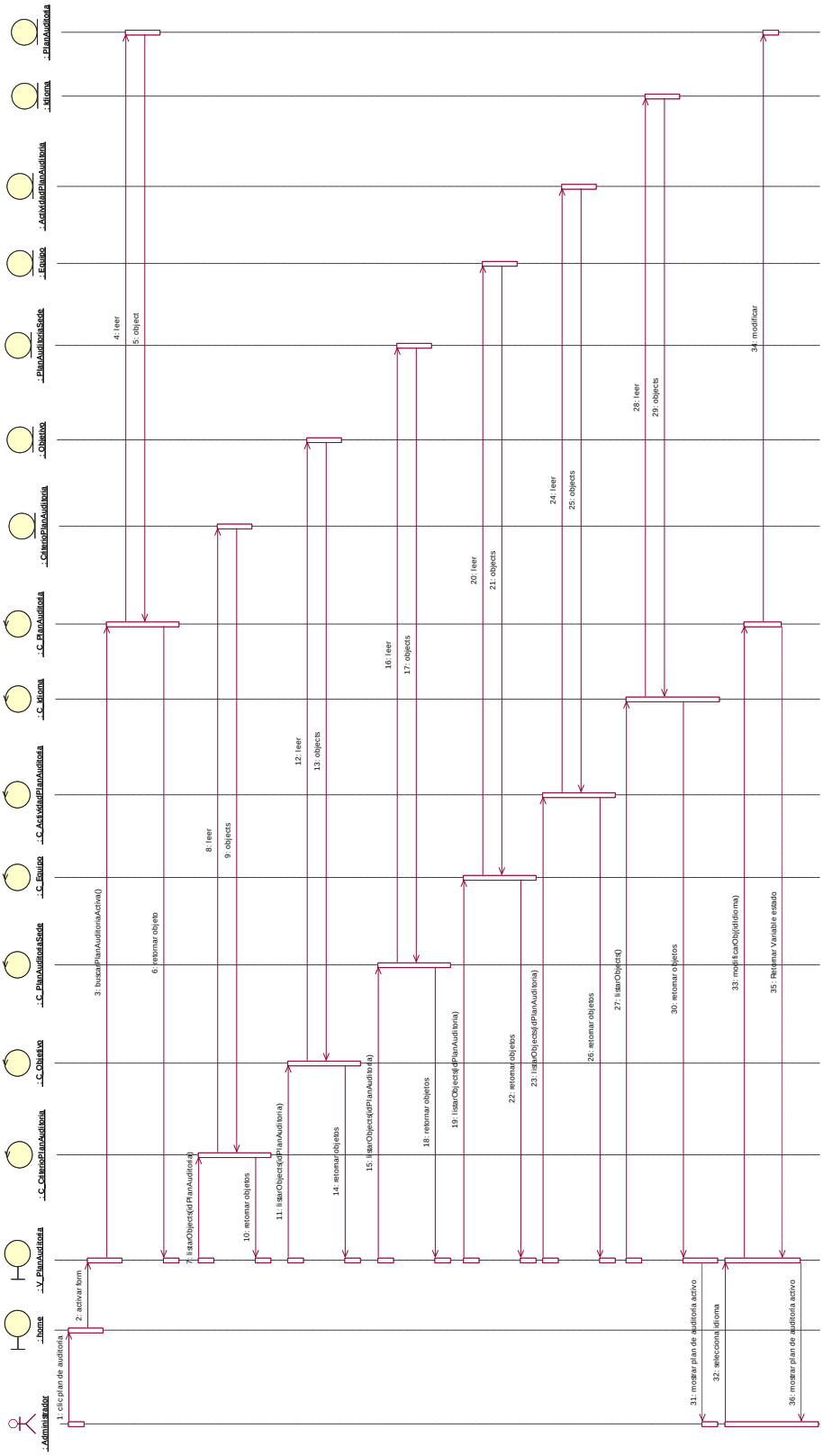


a. Plan auditoría

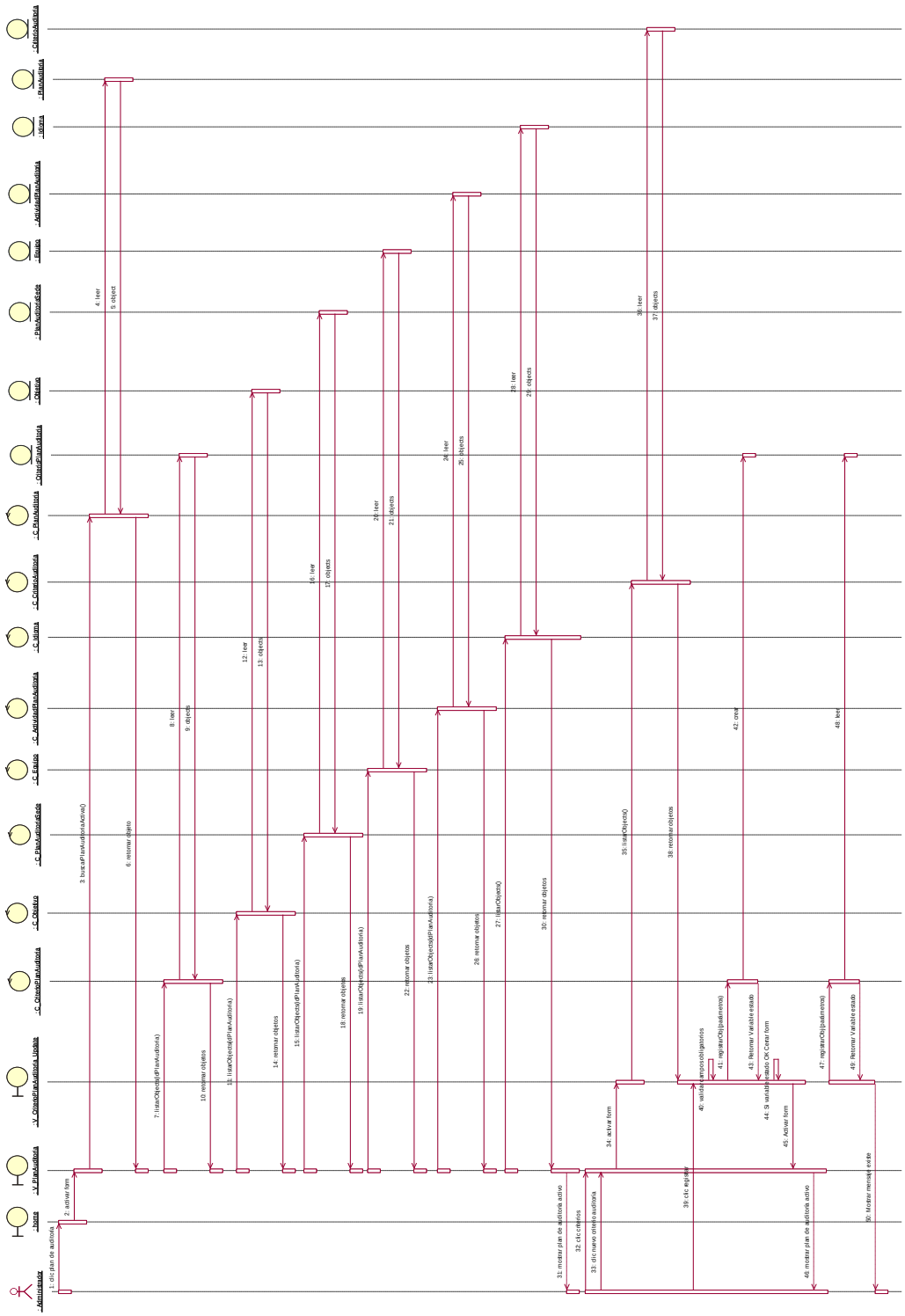
- Crear plan auditoría



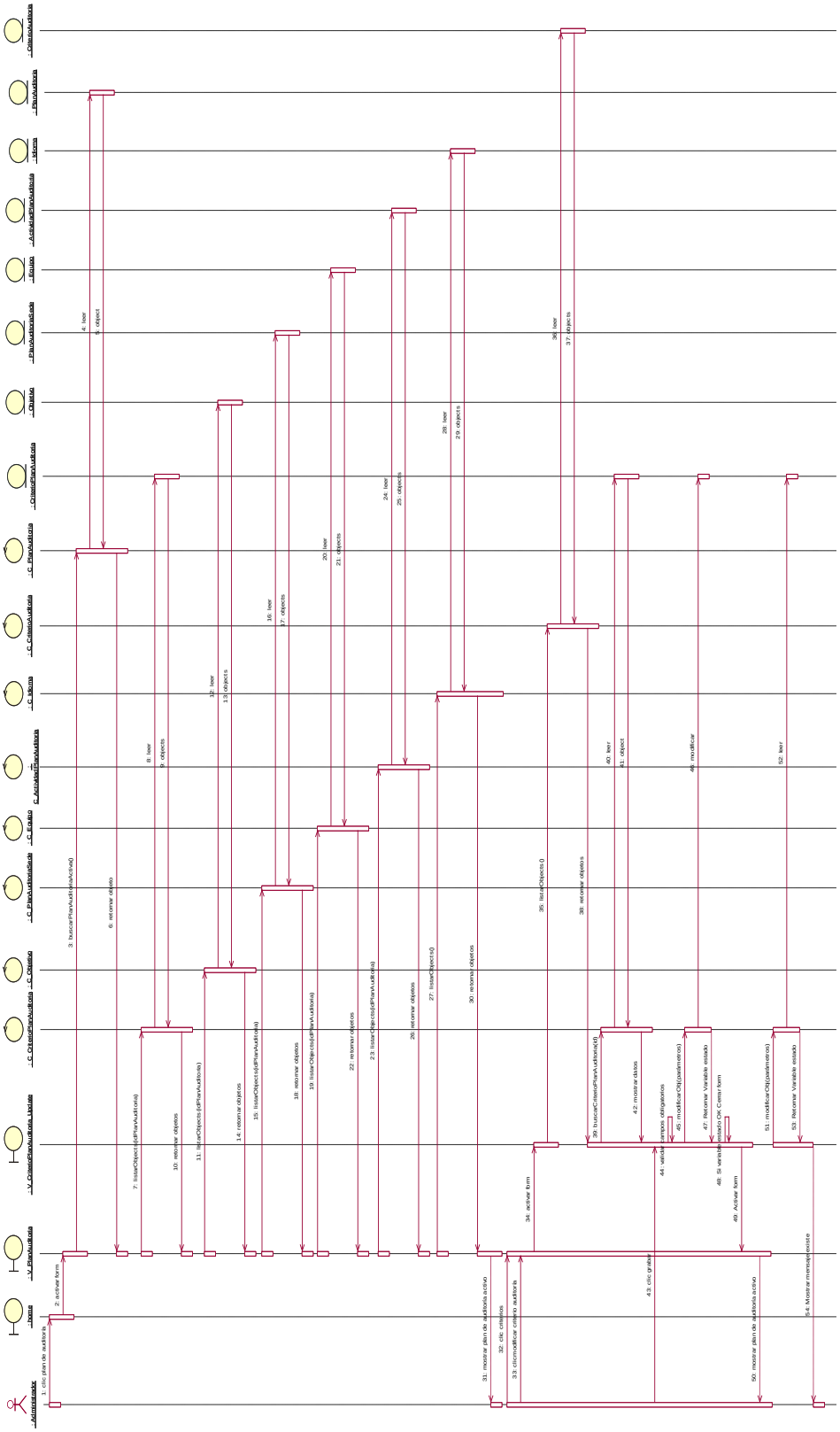
- **Modificar idioma plan auditoría**



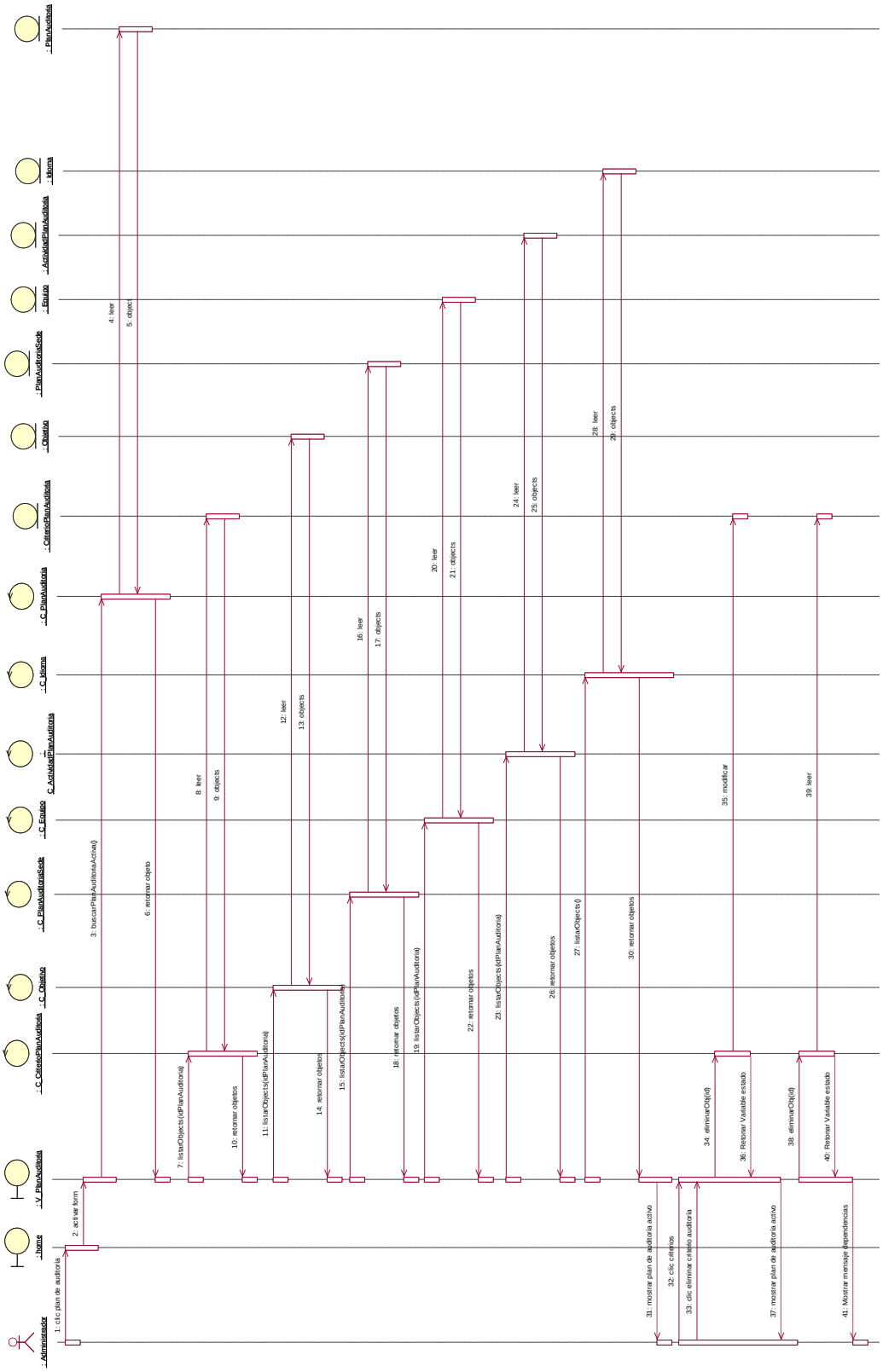
- **Registrar criterio - plan auditoría**



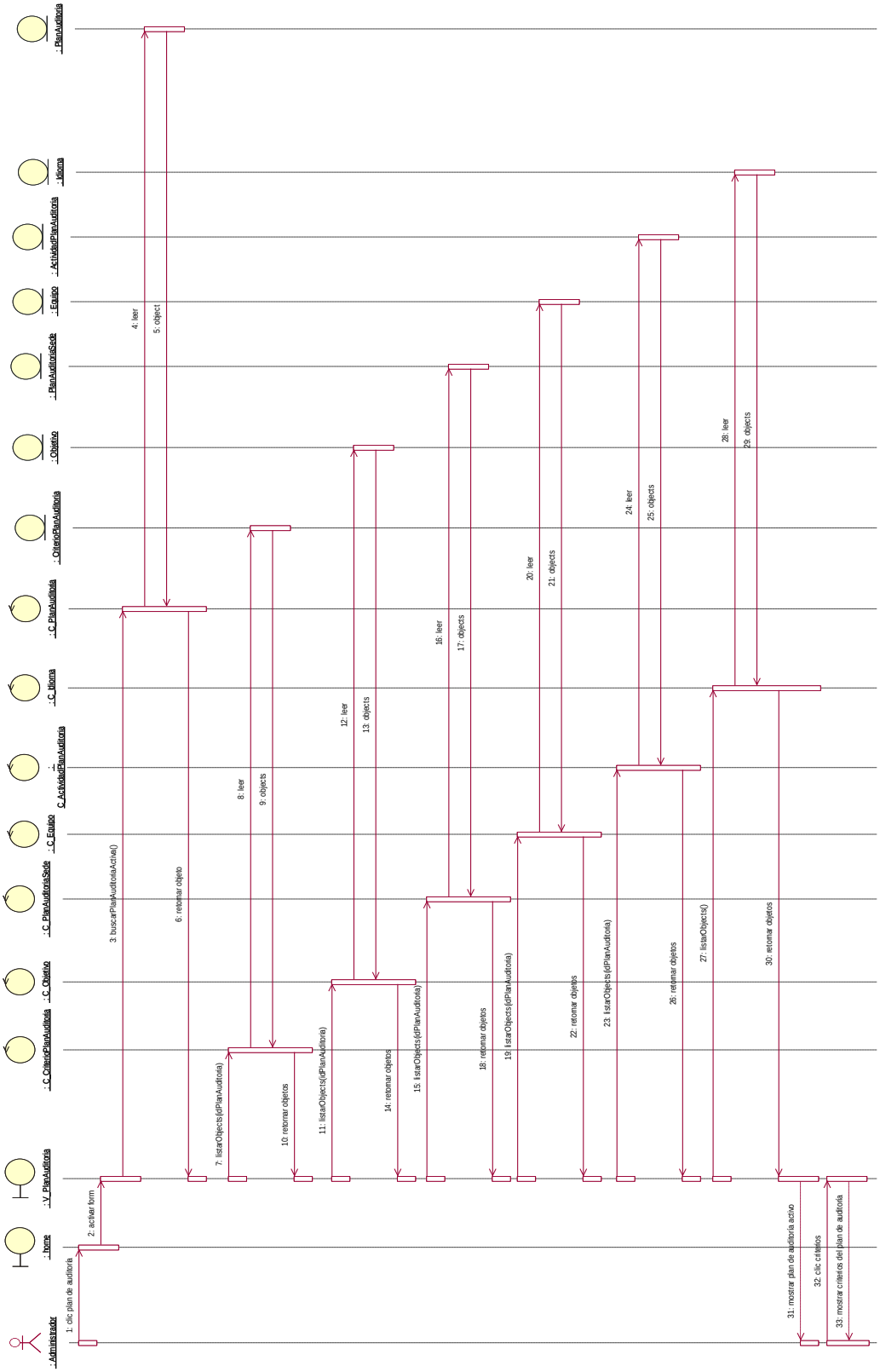
- **Modificar criterio – plan auditoría**



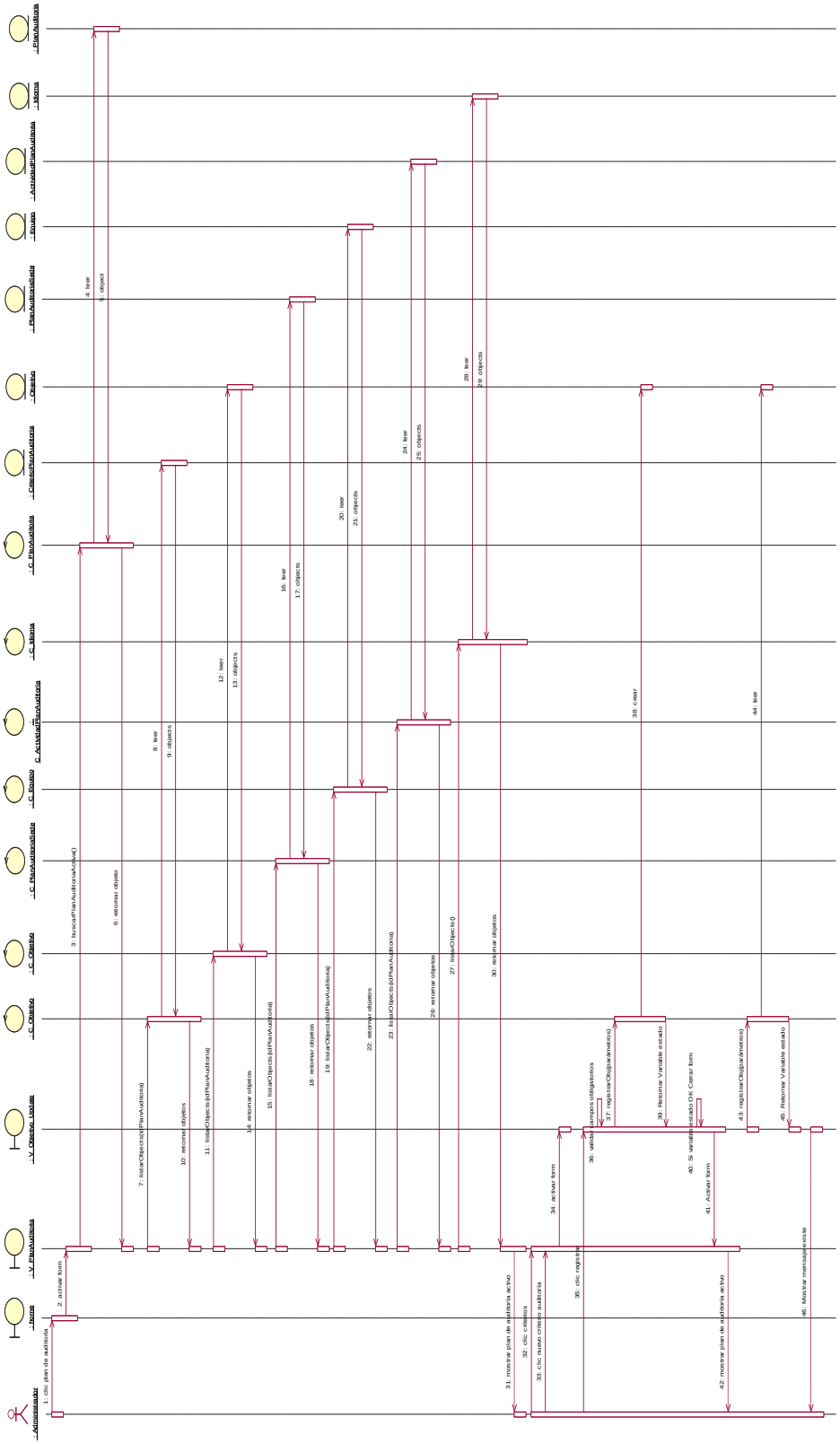
- **Eliminar criterio – plan auditoría**



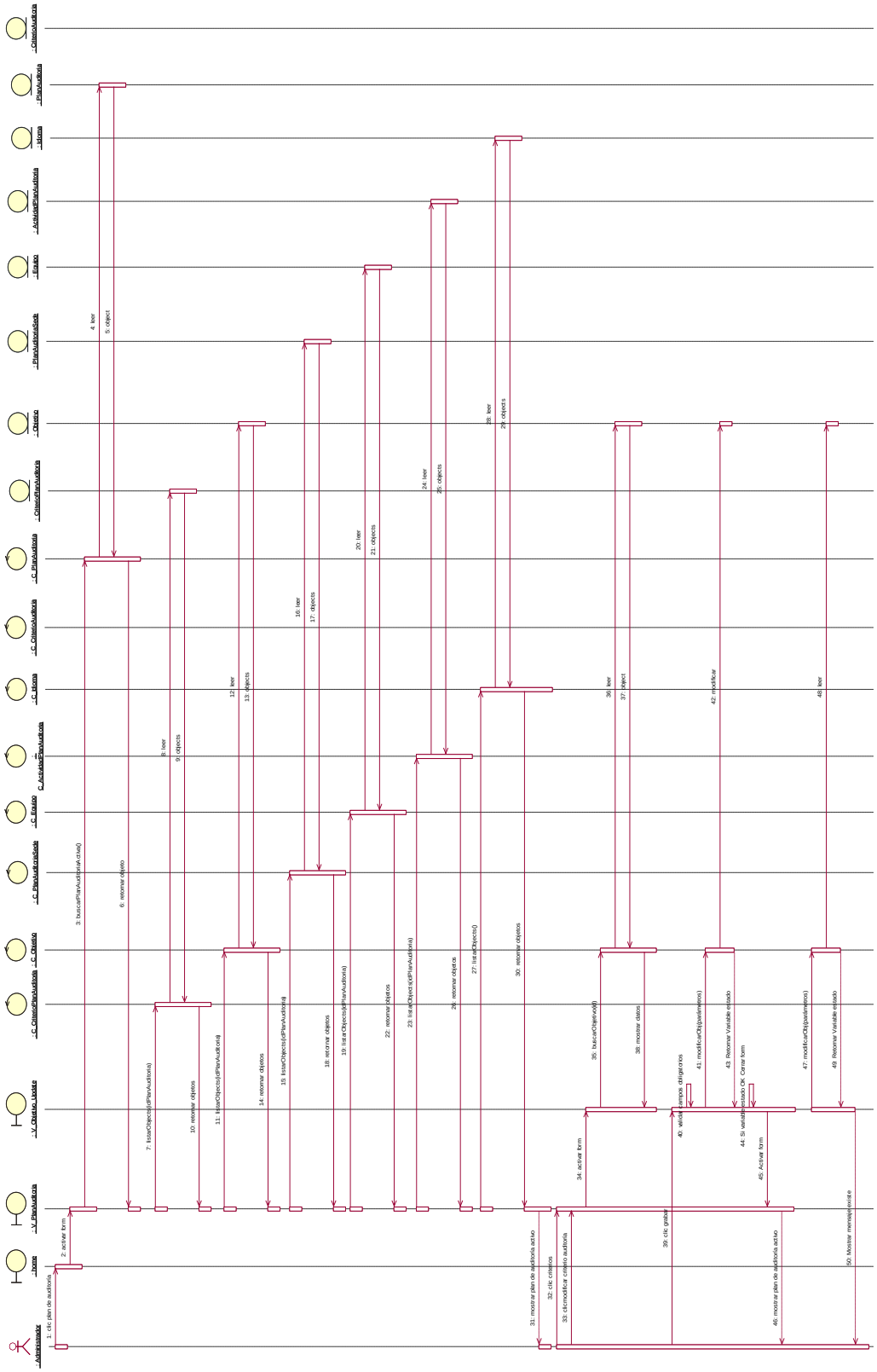
- **Listar criterios – plan auditoría**



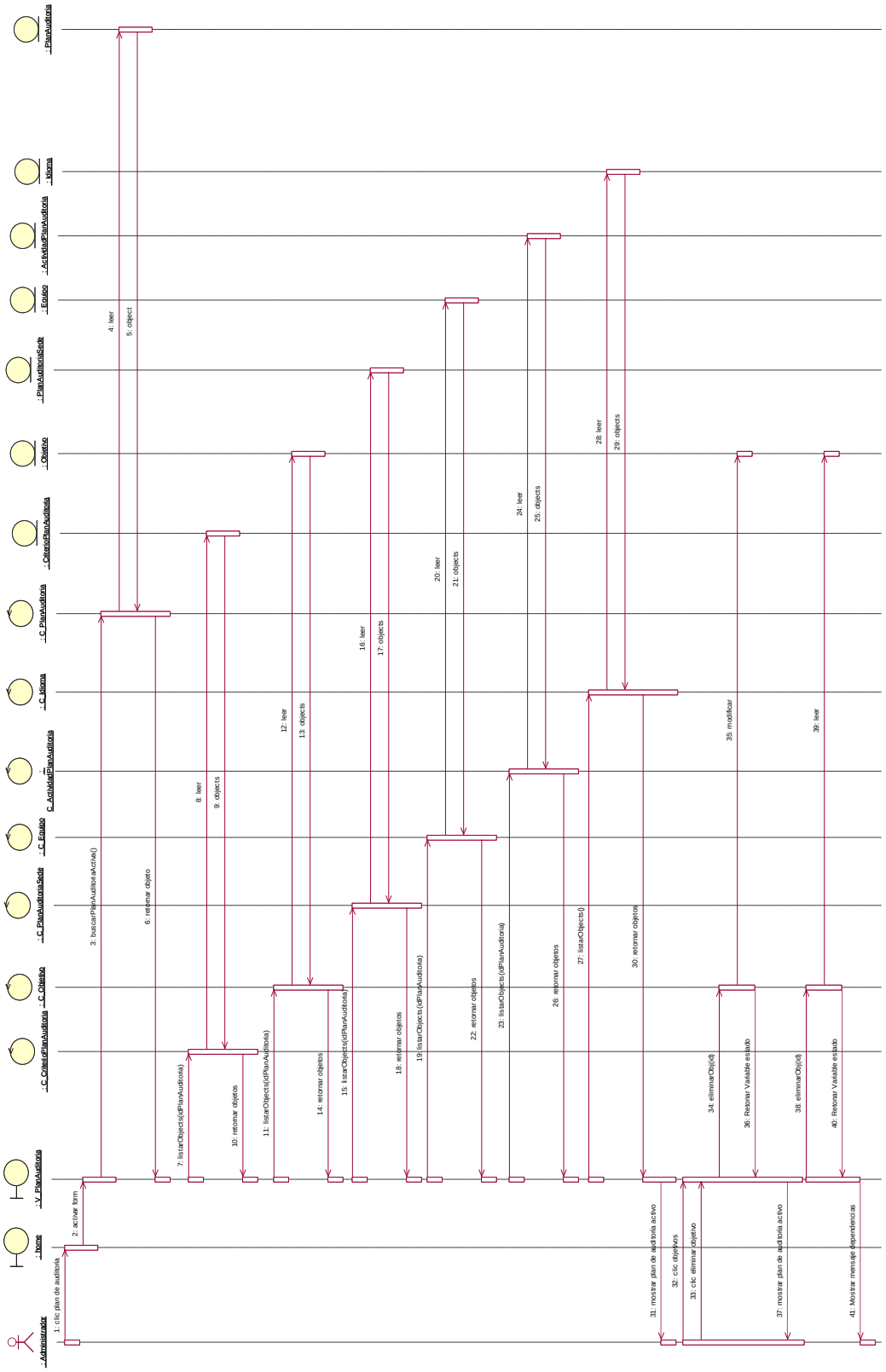
- **Registrar objetivo del plan auditoría**



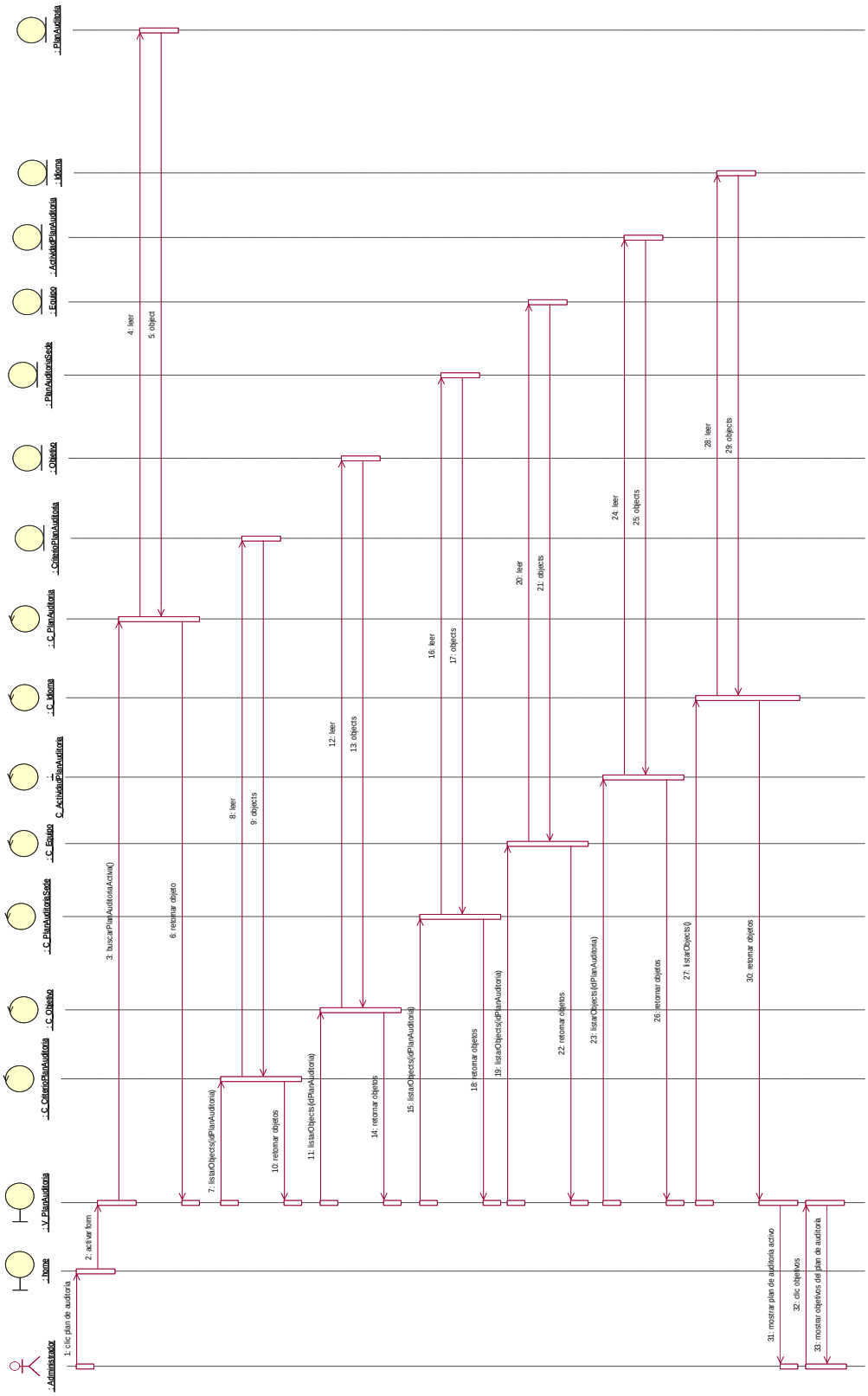
- **Modificar objetivo del plan auditoría**



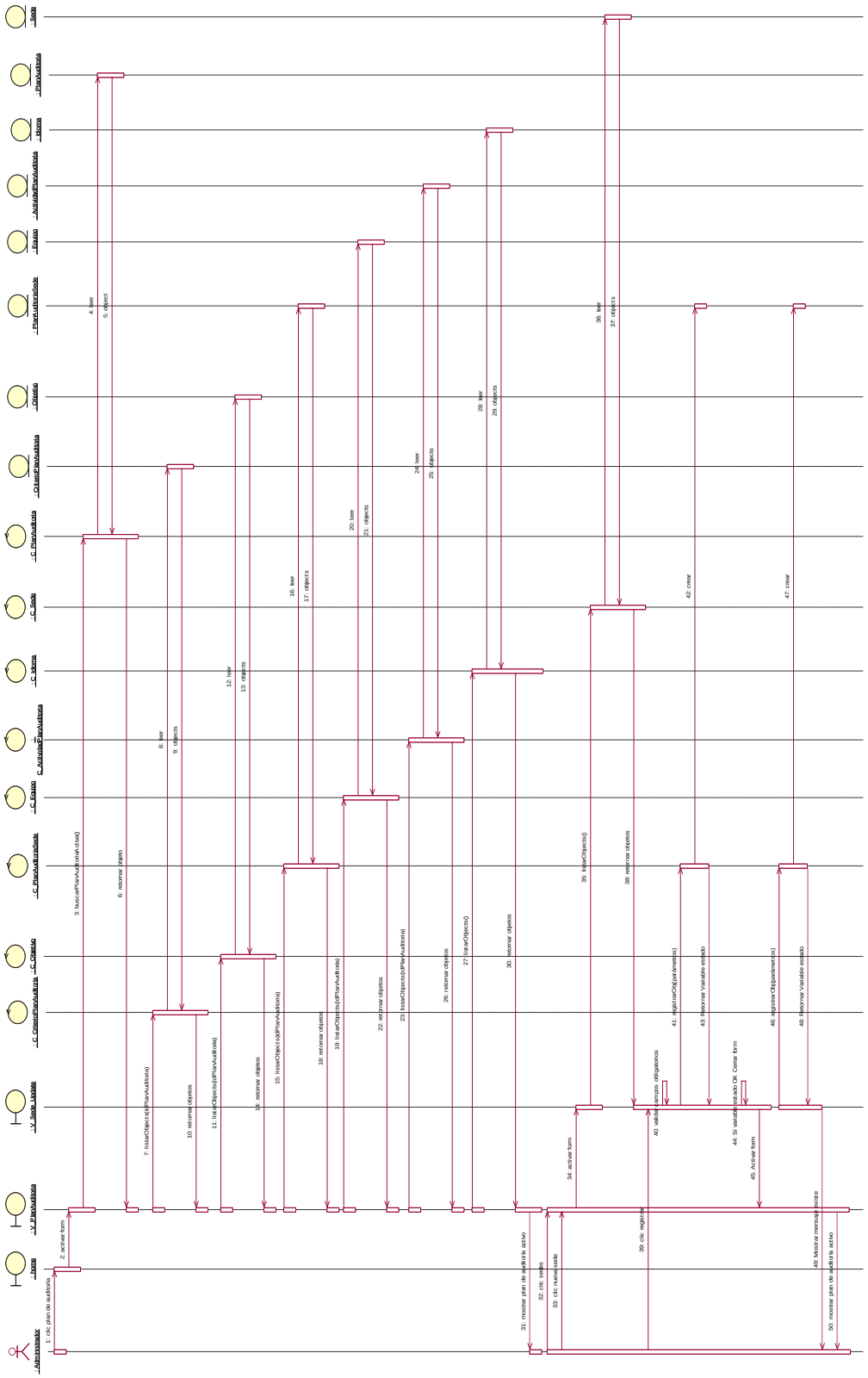
- **Eliminar objetivo del plan de auditoría**



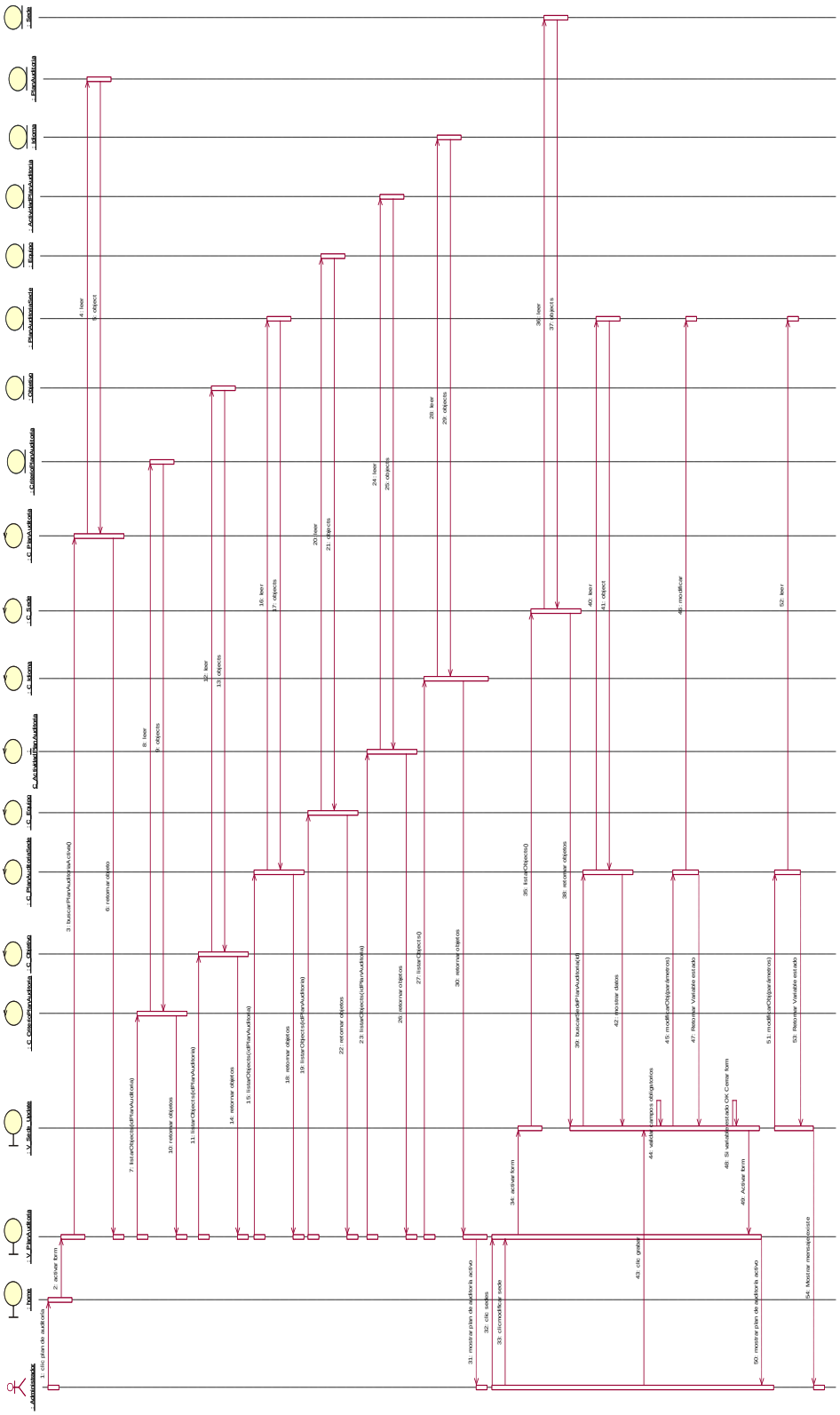
- **Listar objetivos del plan de auditoría**



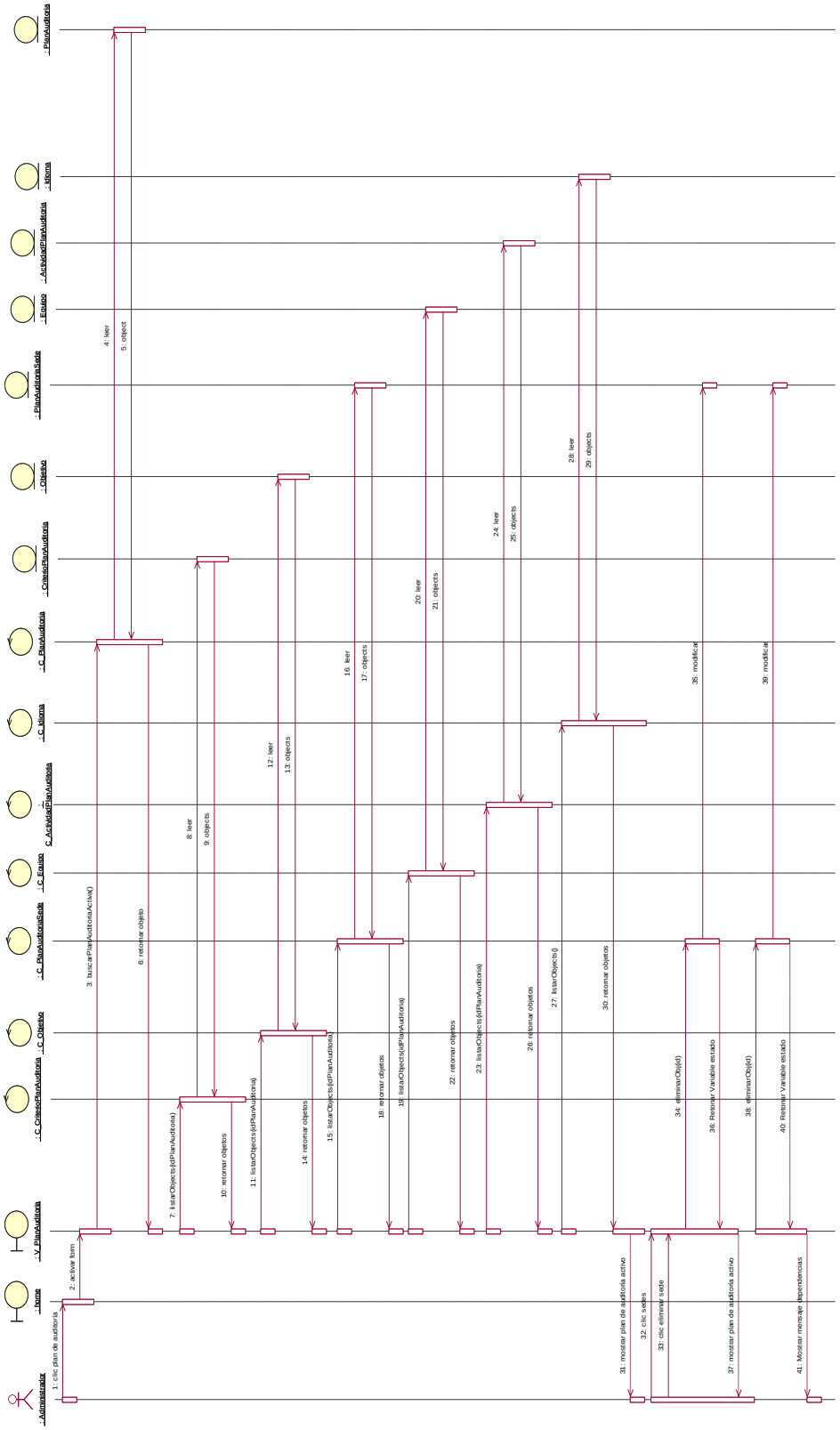
- **Registrar sede – plan auditoría**



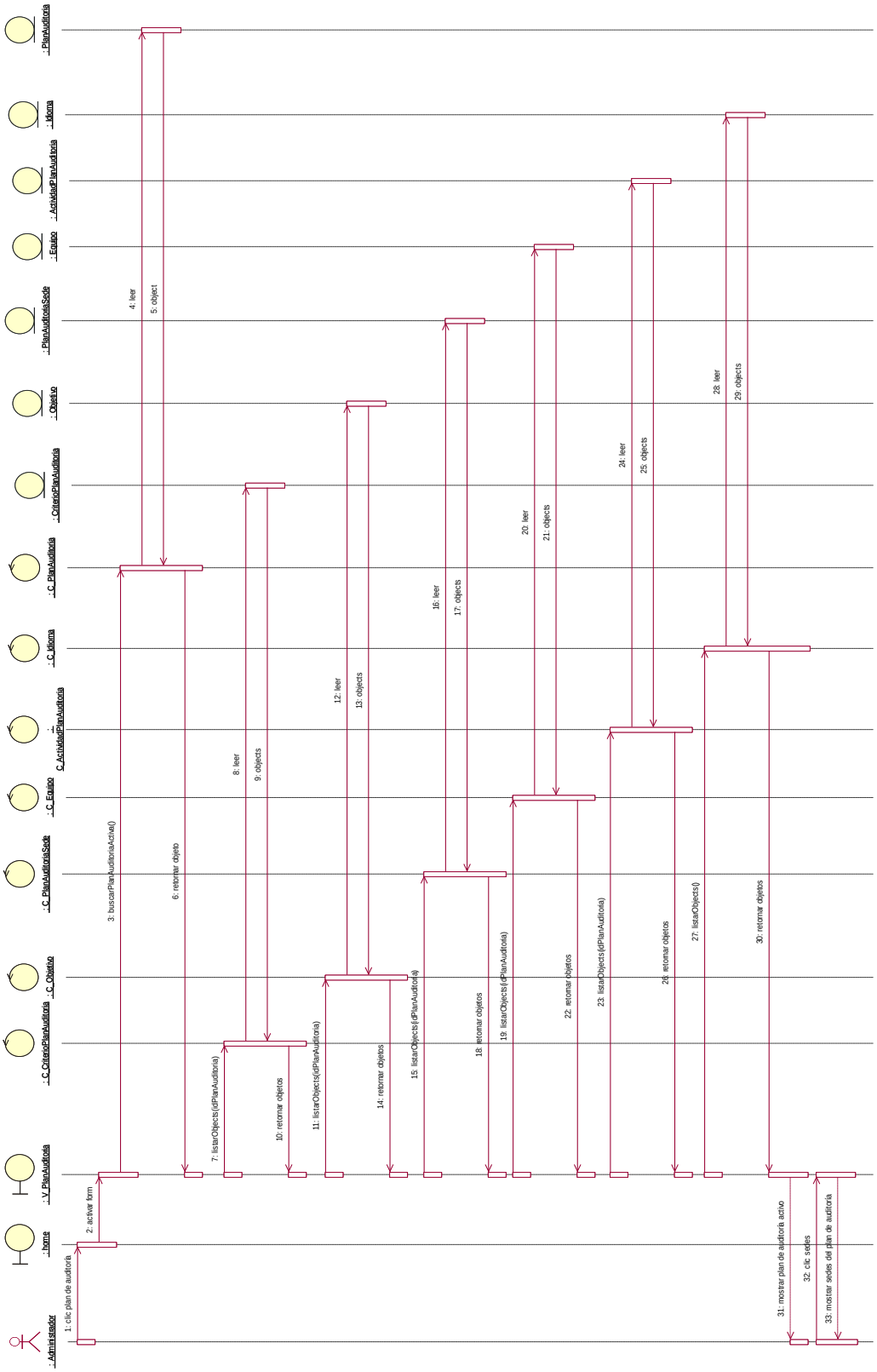
- **Modificar sede – plan auditoría**



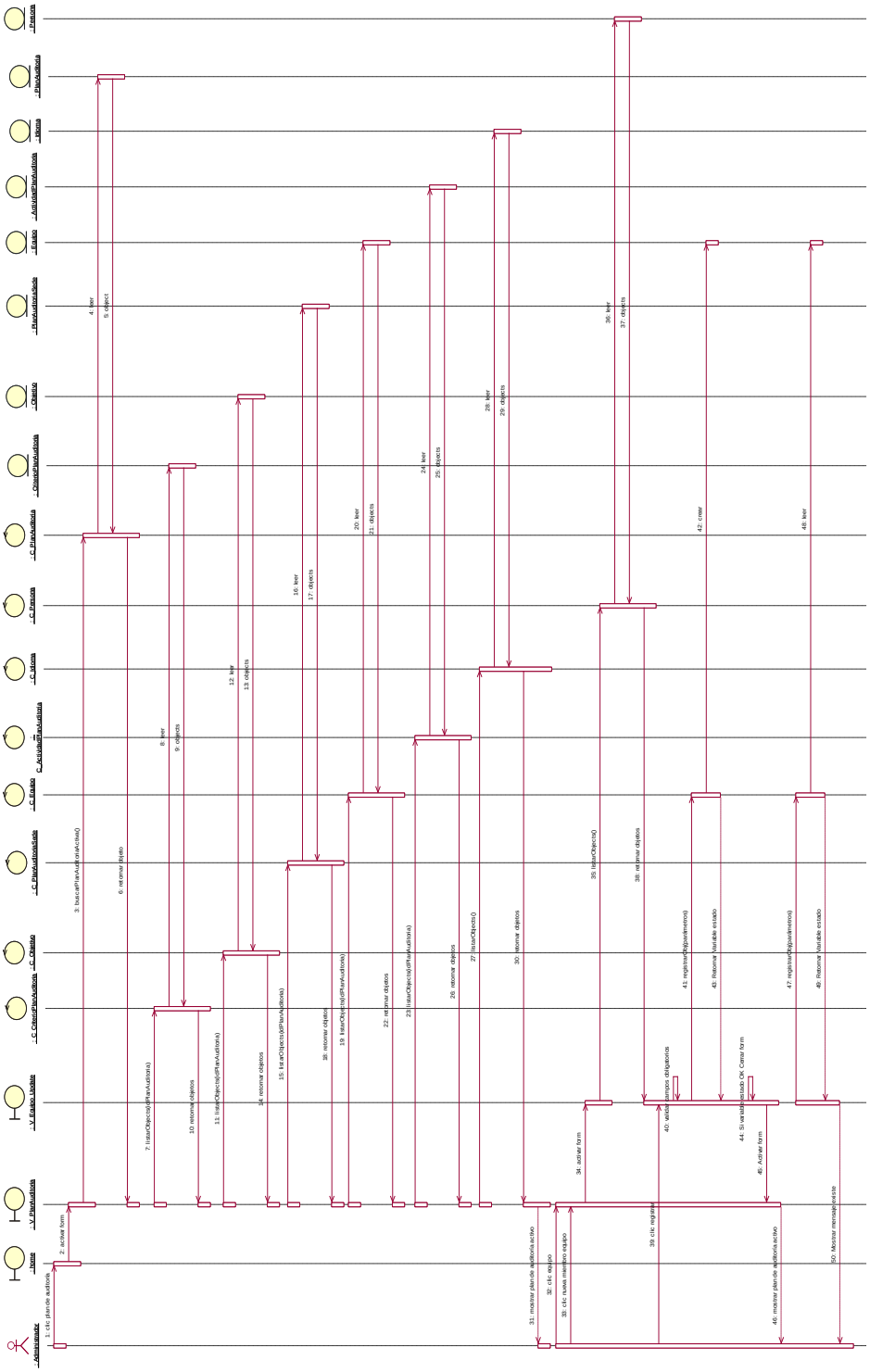
- **Eliminar sede – plan auditoría**



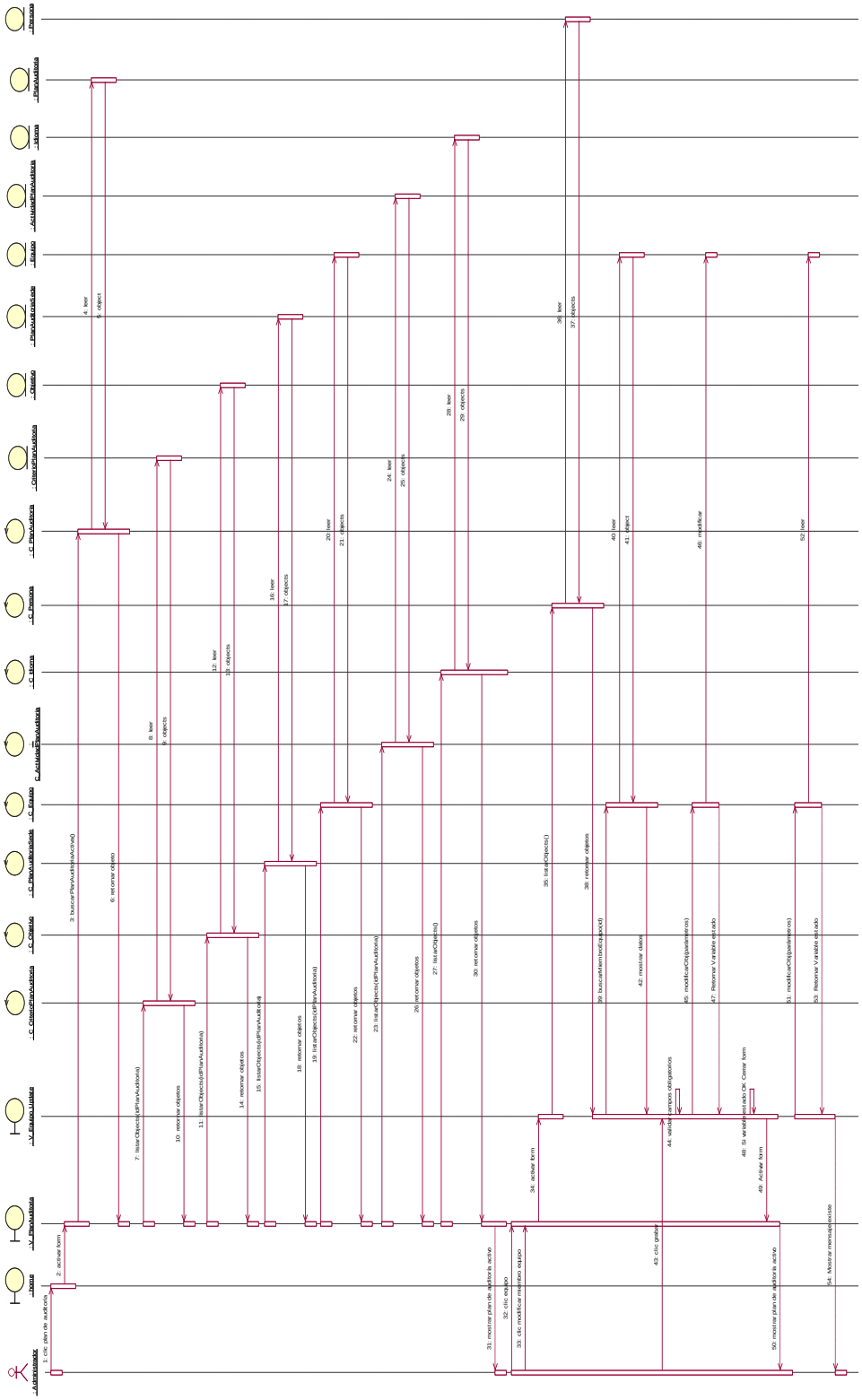
- **Listar sedes- plan auditoría**



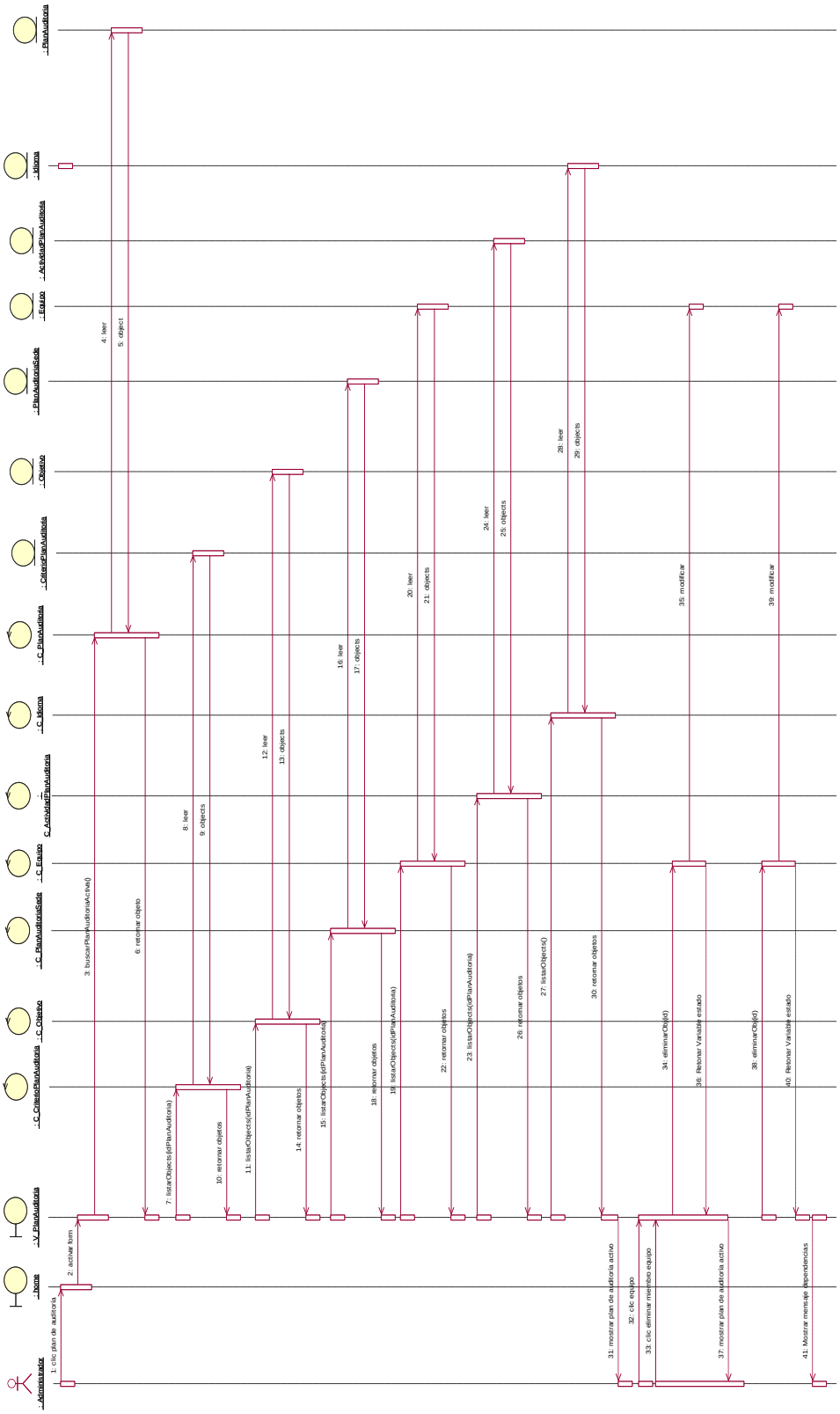
- **Registrar miembro equipo – plan auditoría**



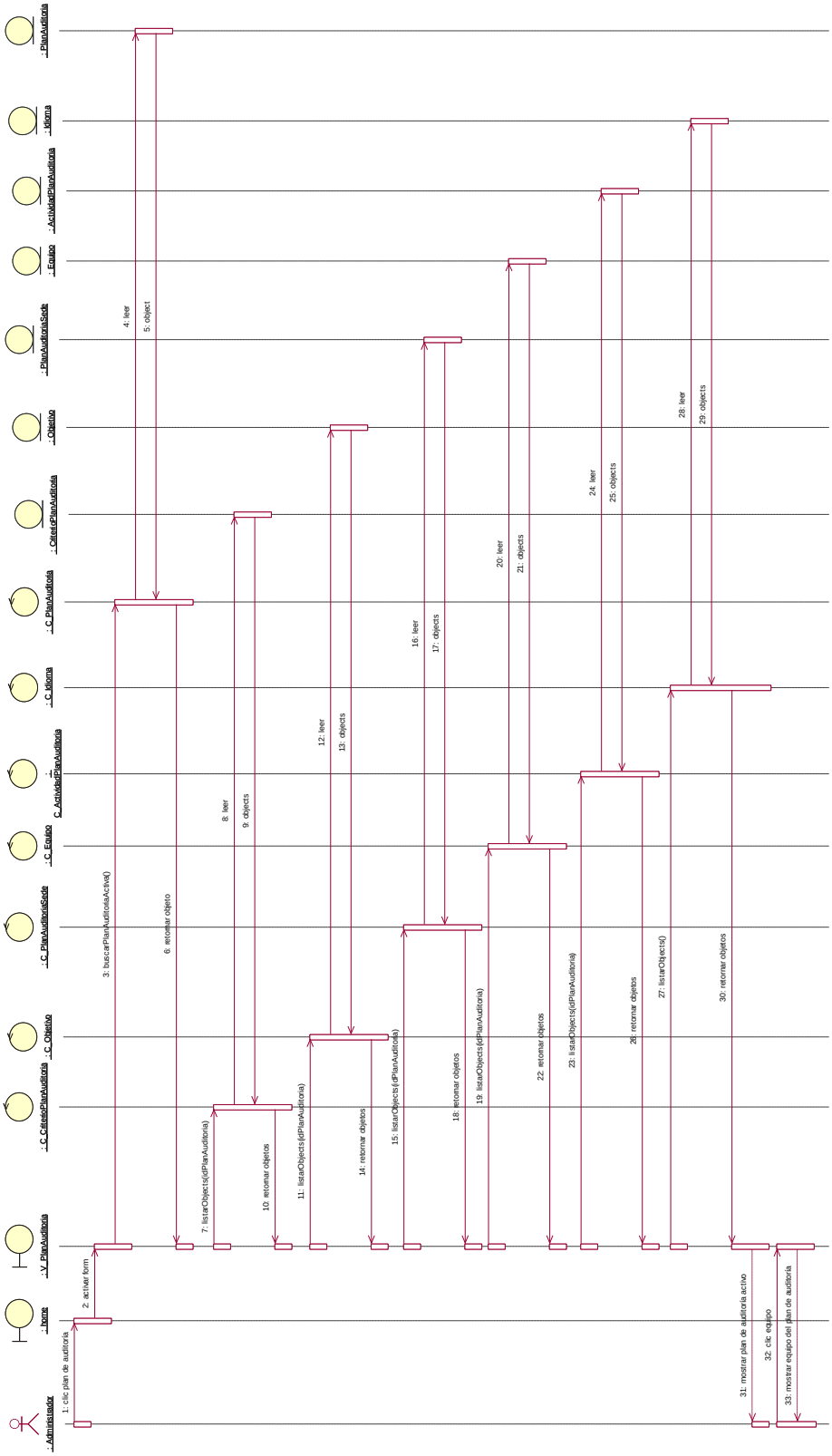
- **Modificar miembro equipo – plan auditoría**



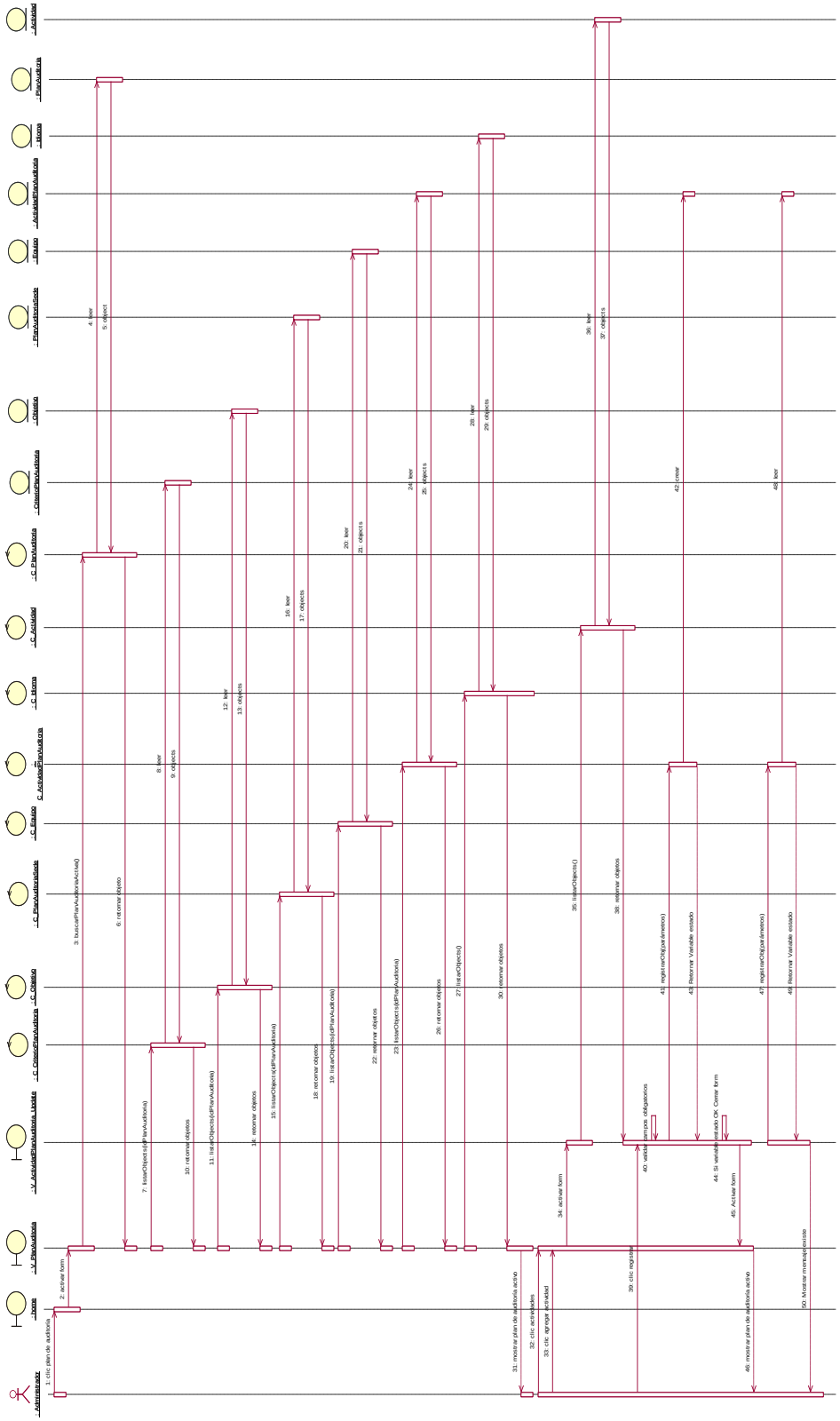
- **Eliminar miembro equipo – plan auditoría**



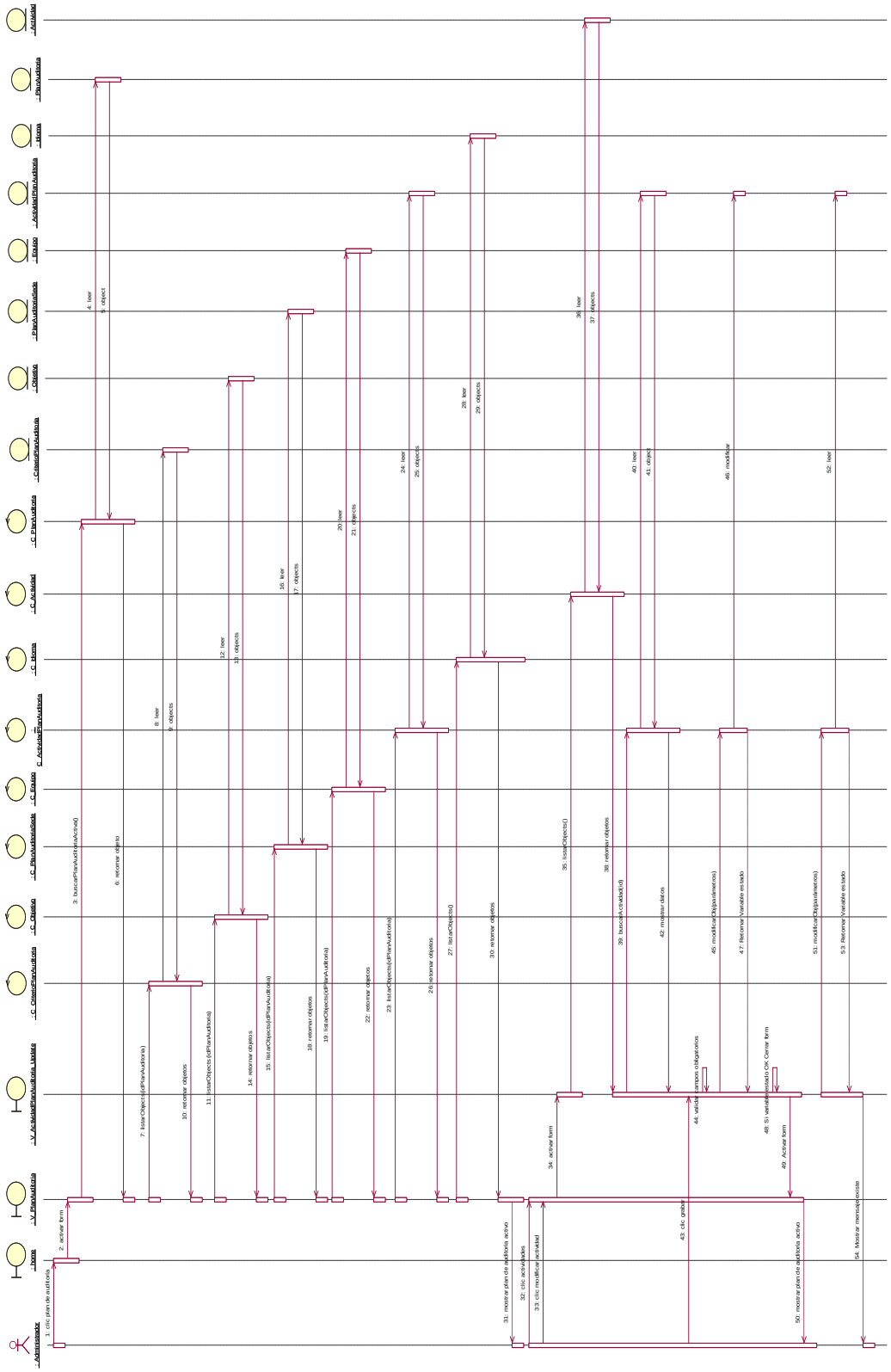
- **Listar equipo – plan auditoría**



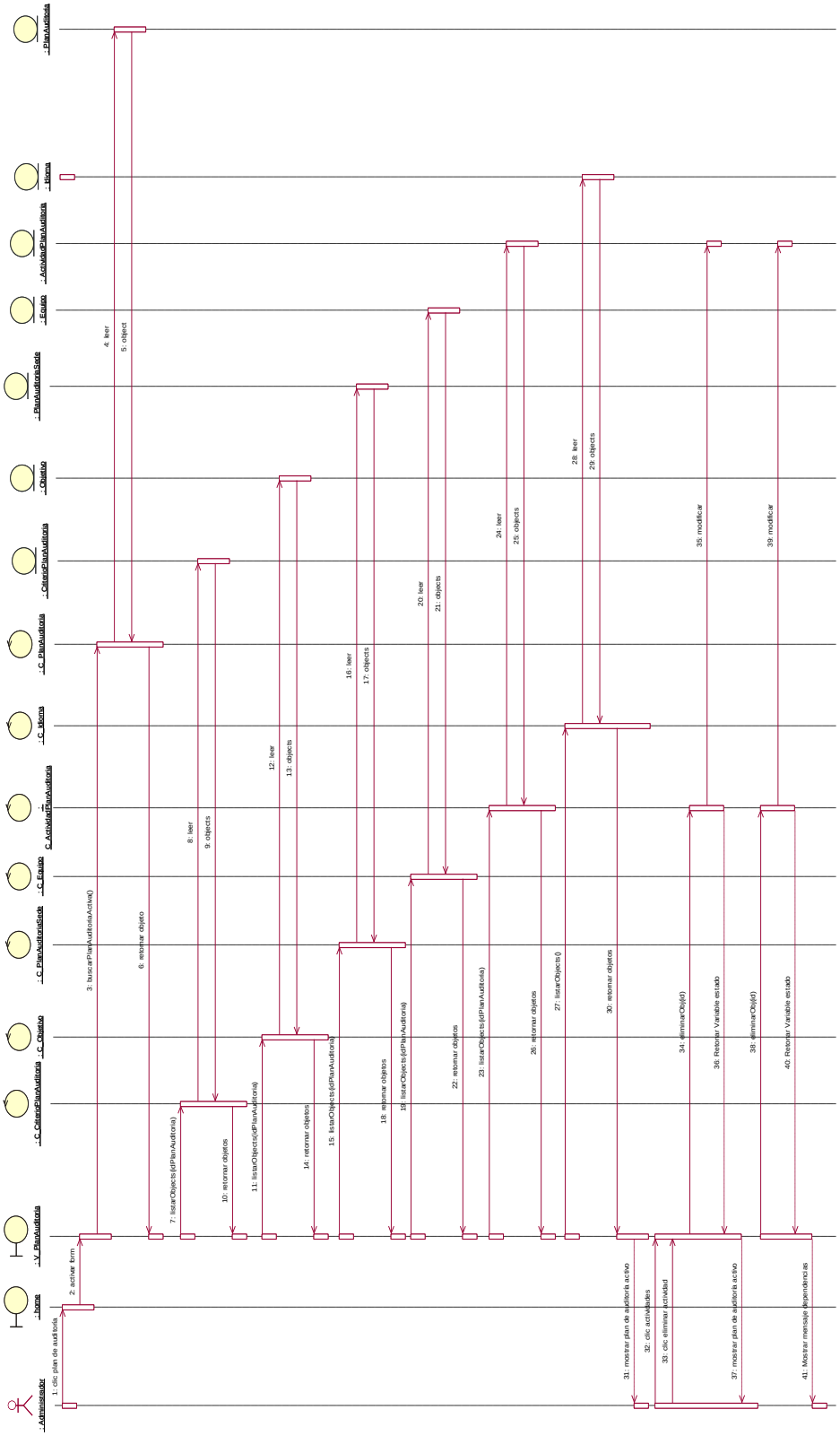
- **Registrar actividad – plan auditoría**



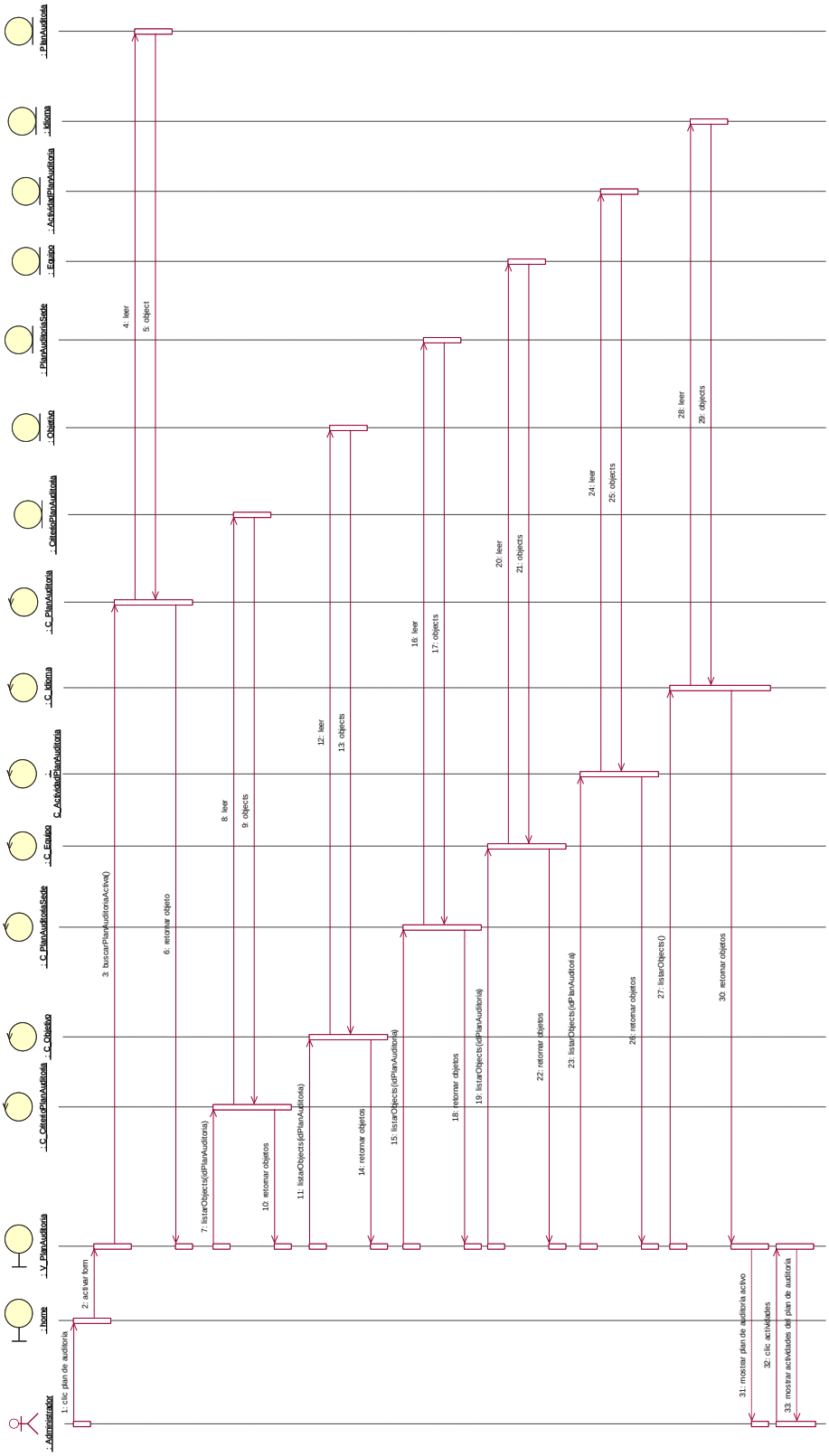
- **Modificar actividad – plan auditoría**



- **Listar actividades – plan auditoría**

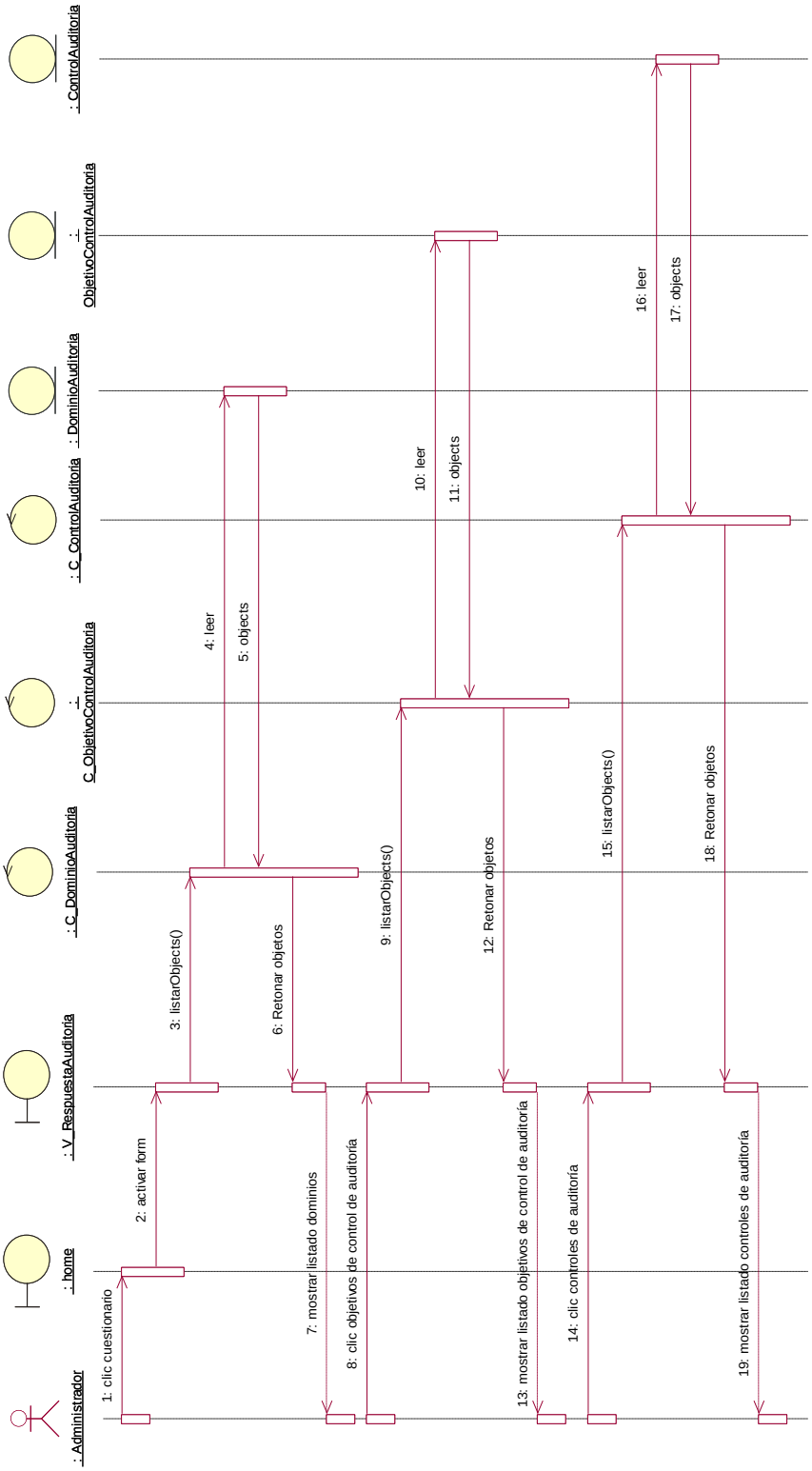


- **Finalizar plan auditoría**

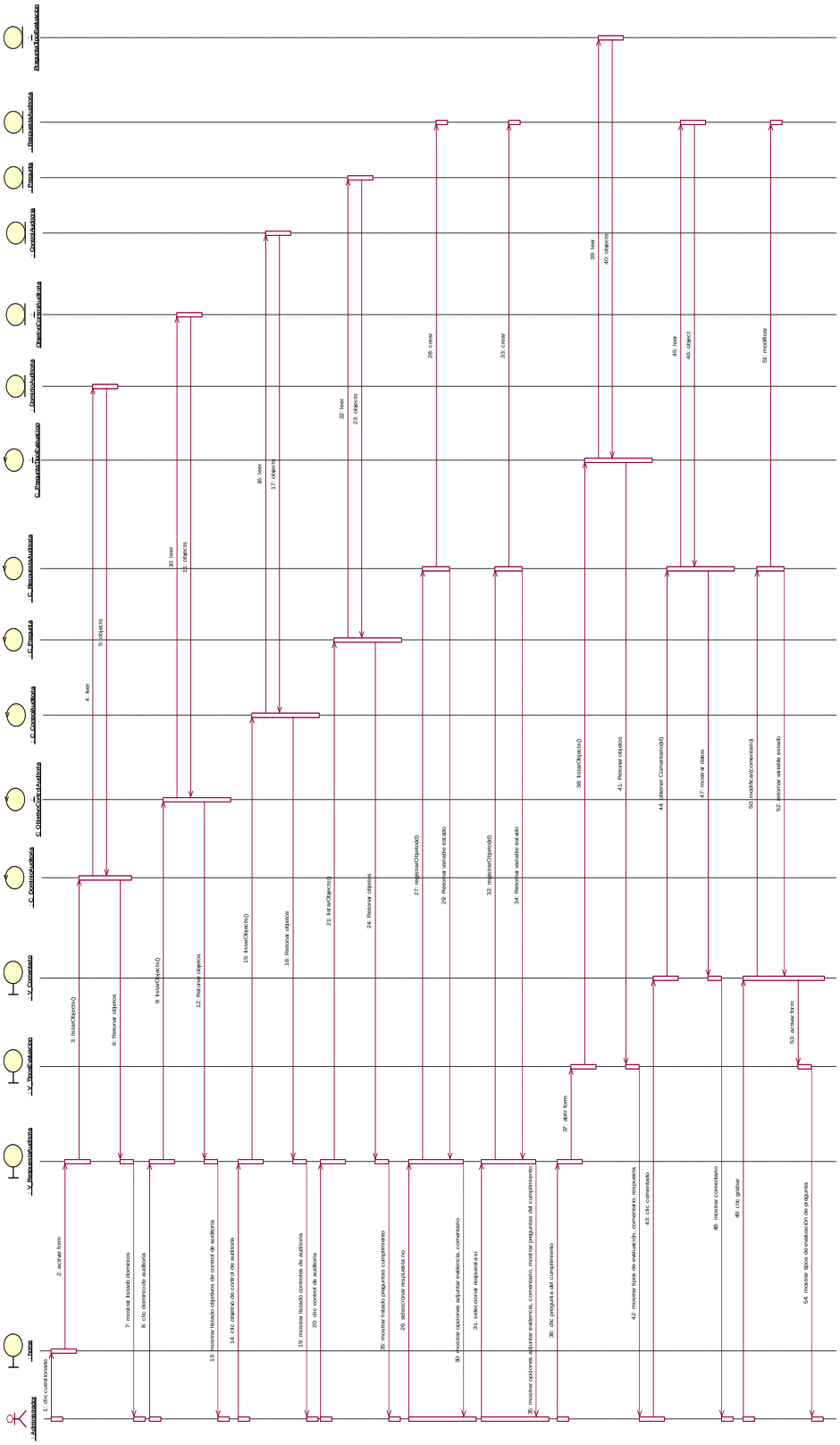


b. Cuestionario

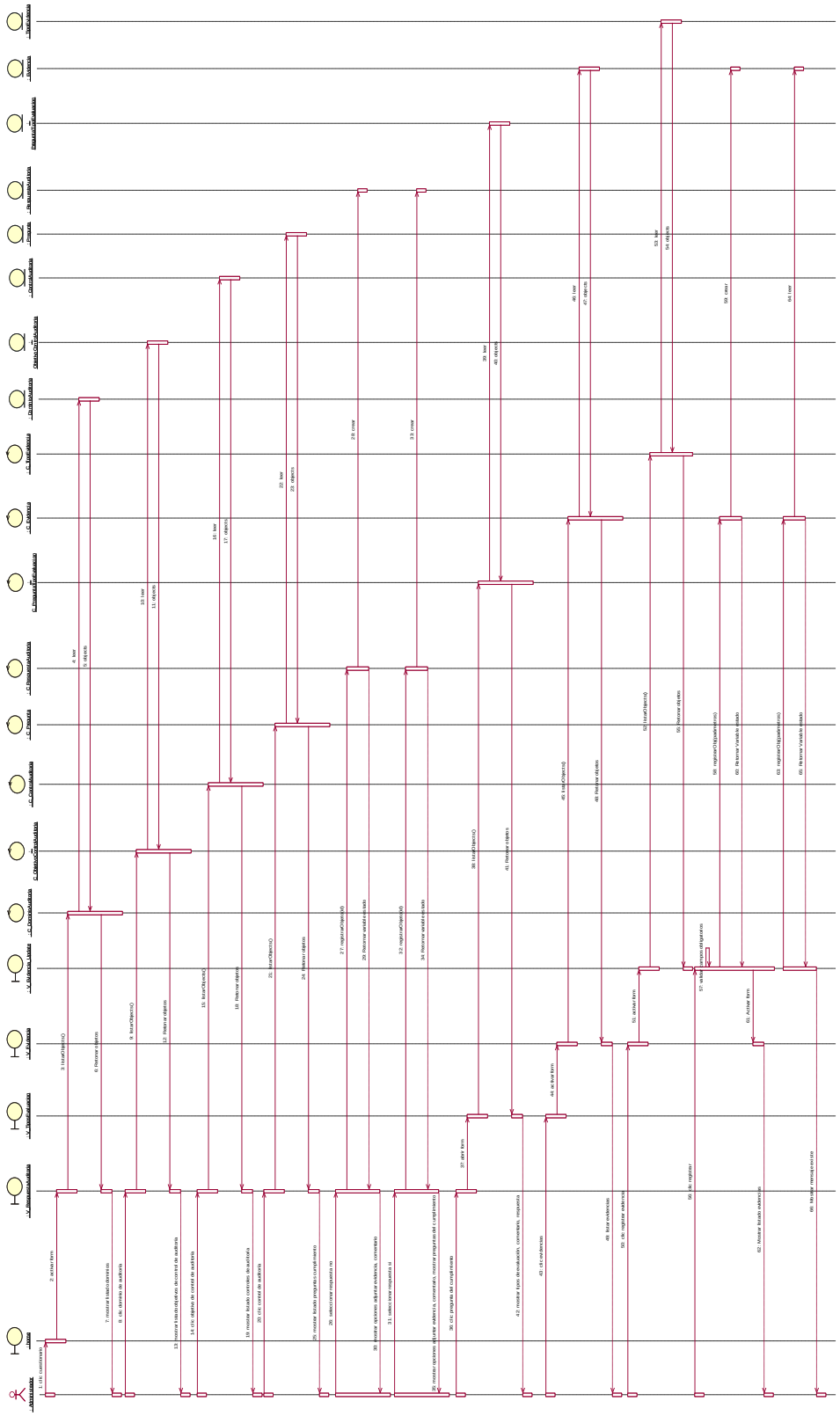
- Listar controles cuestionario



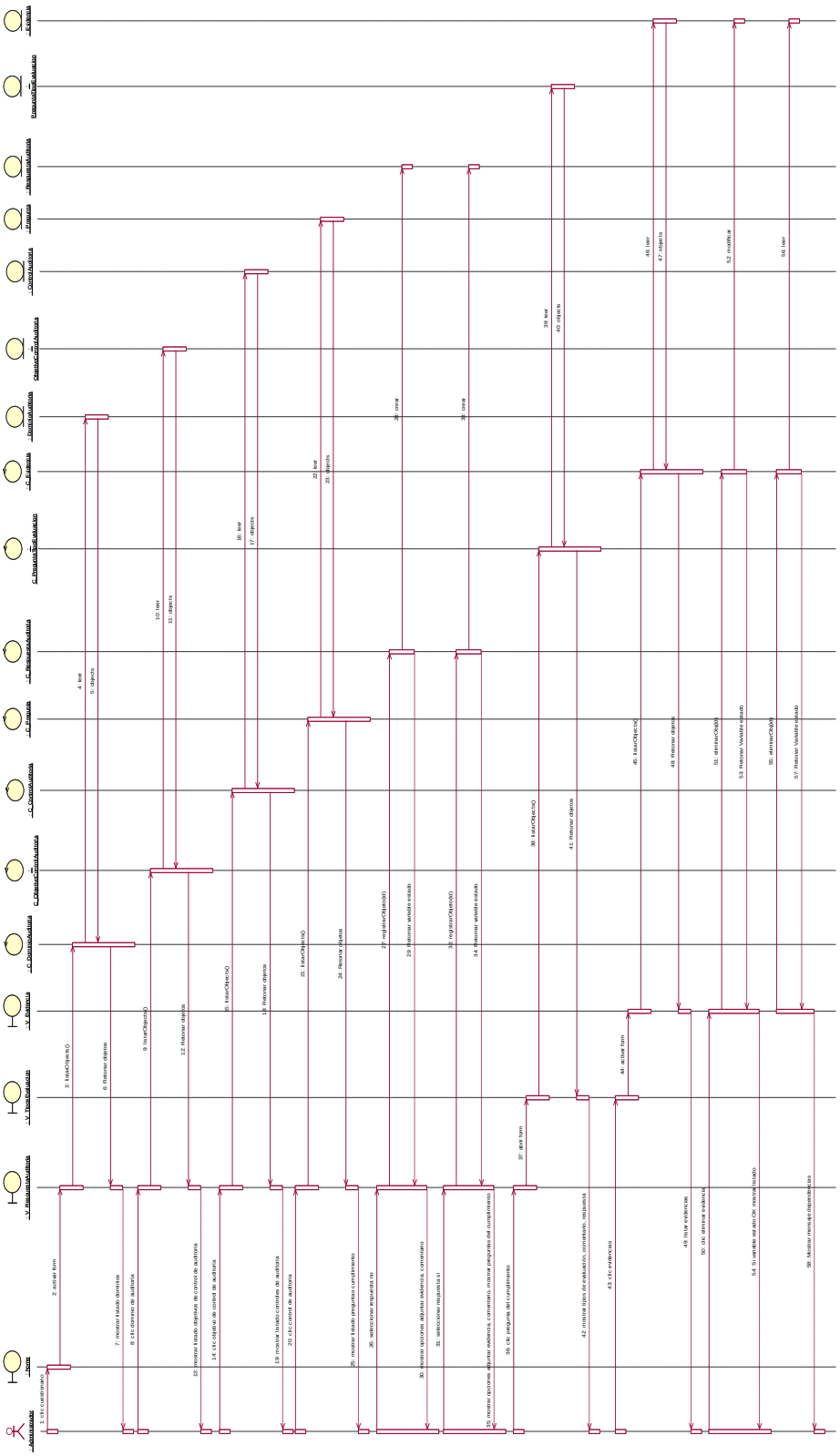
- **Completar cuestionario auditoría**



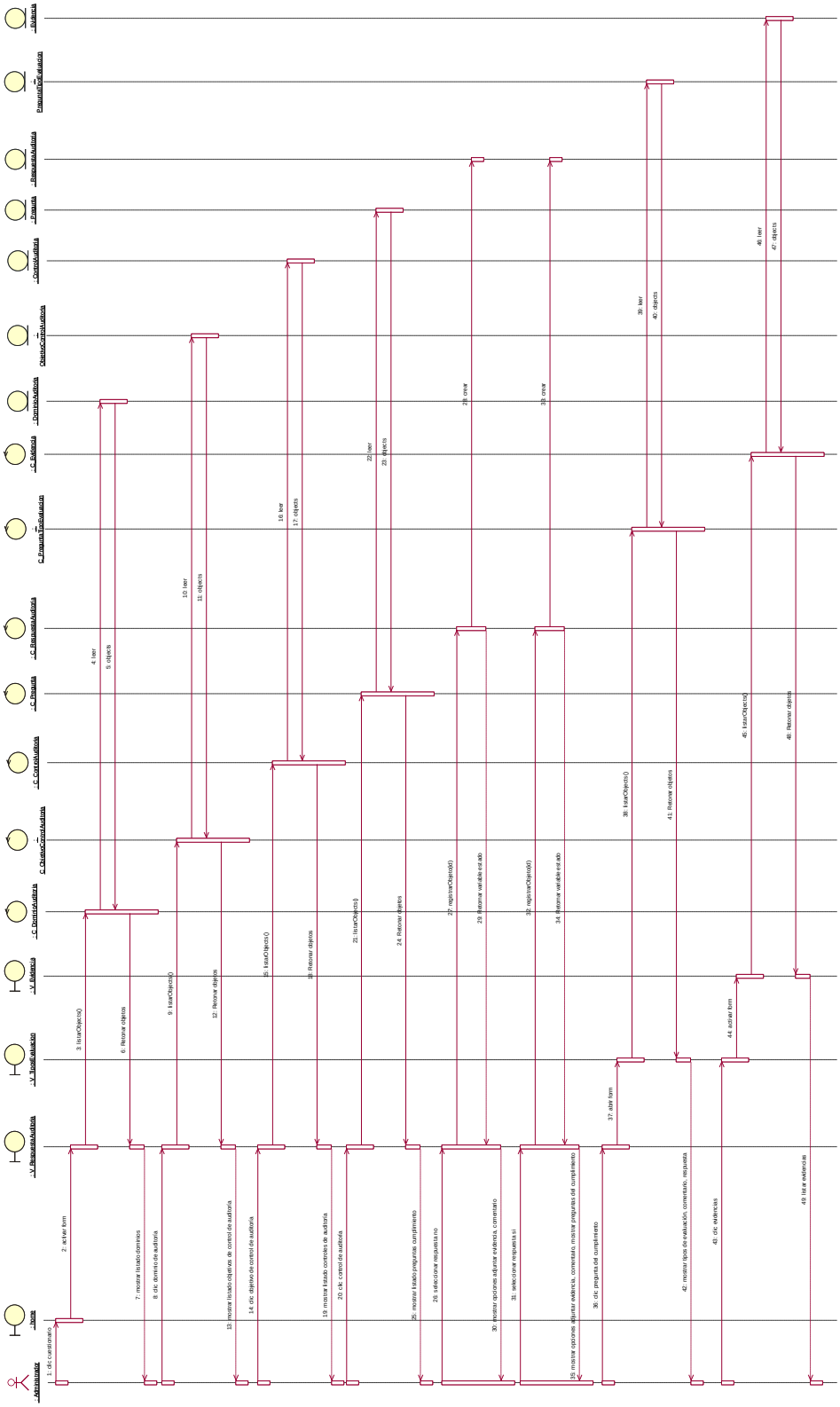
- **Adjuntar evidencia pregunta**



- **Eliminar evidencia pregunta**

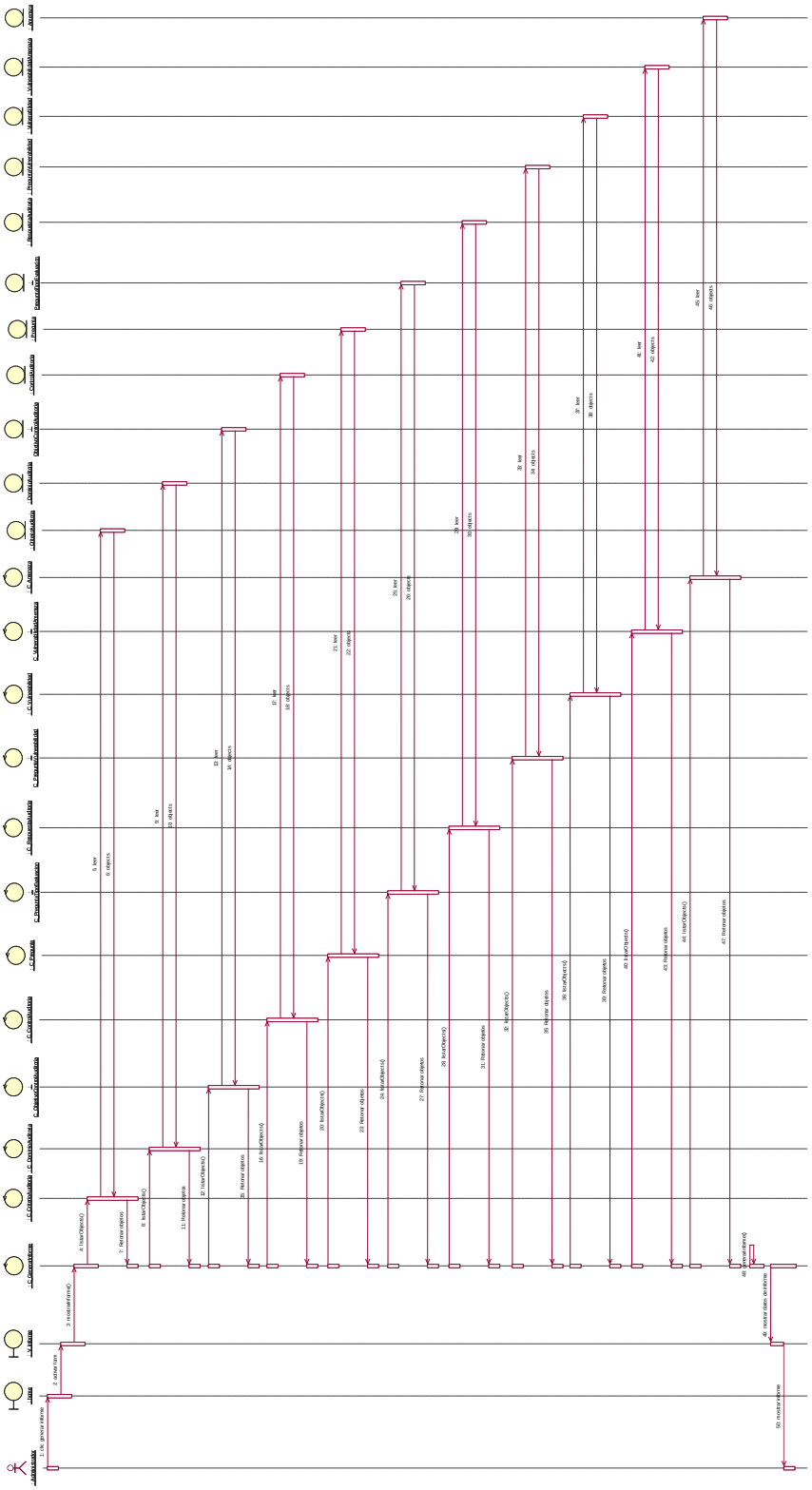


- **Listar evidencias pregunta**

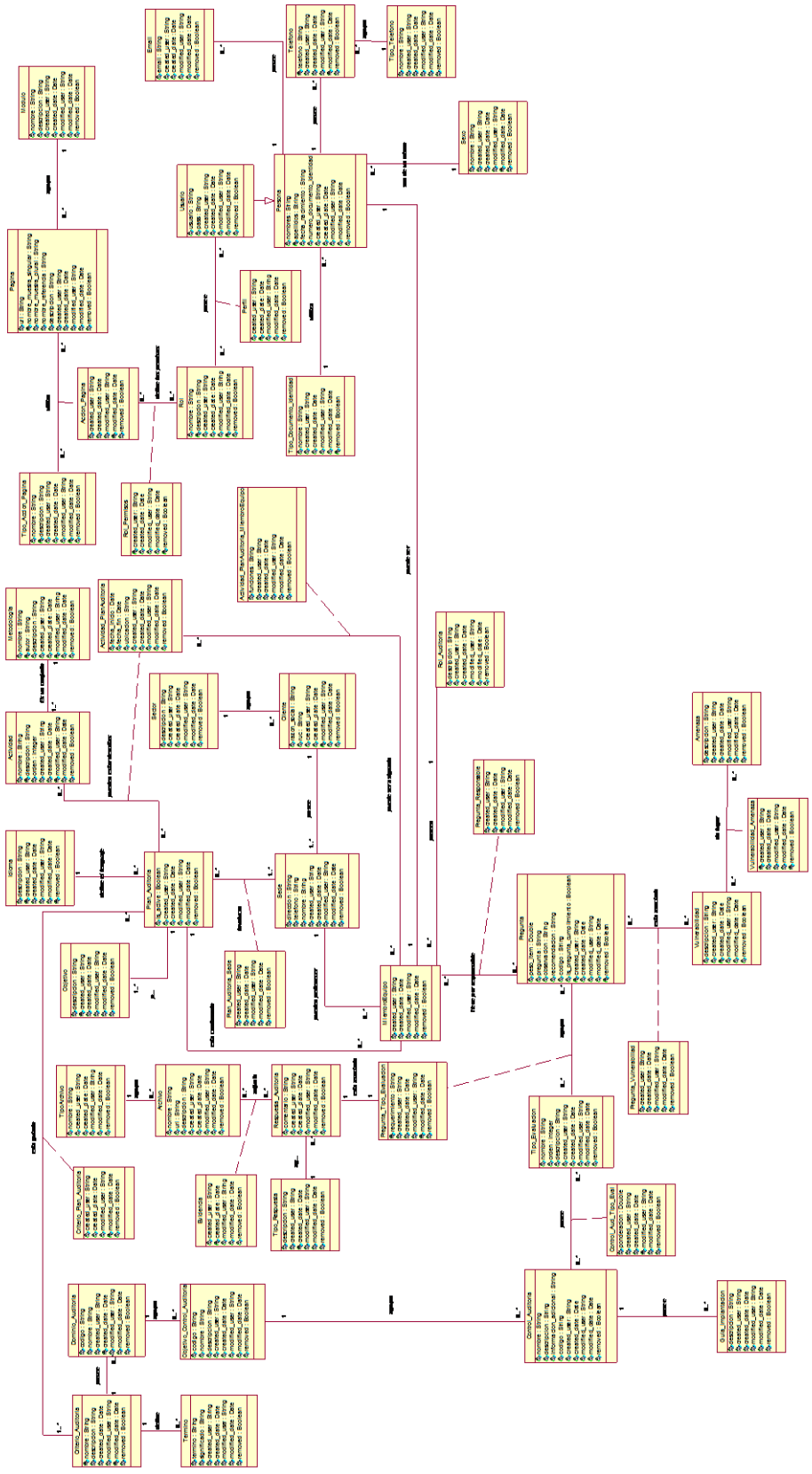


c. Informe auditoría

- **Generar informe de Auditoría**



4.3.3 Diagrama de clases

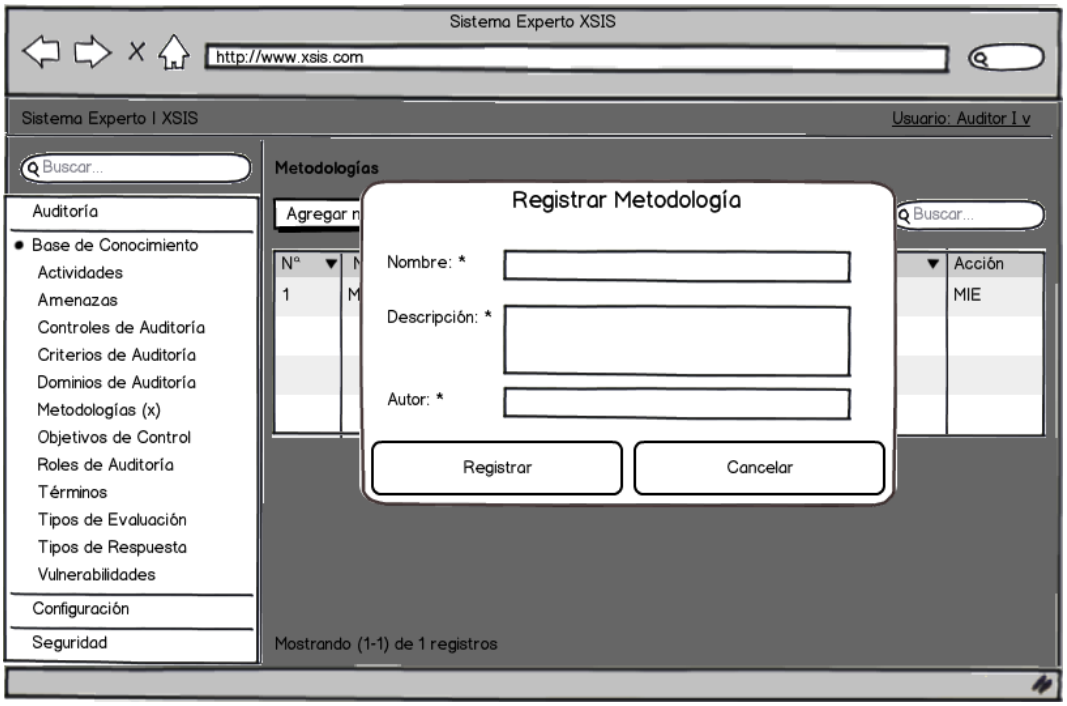


4.3.4 Prototipos

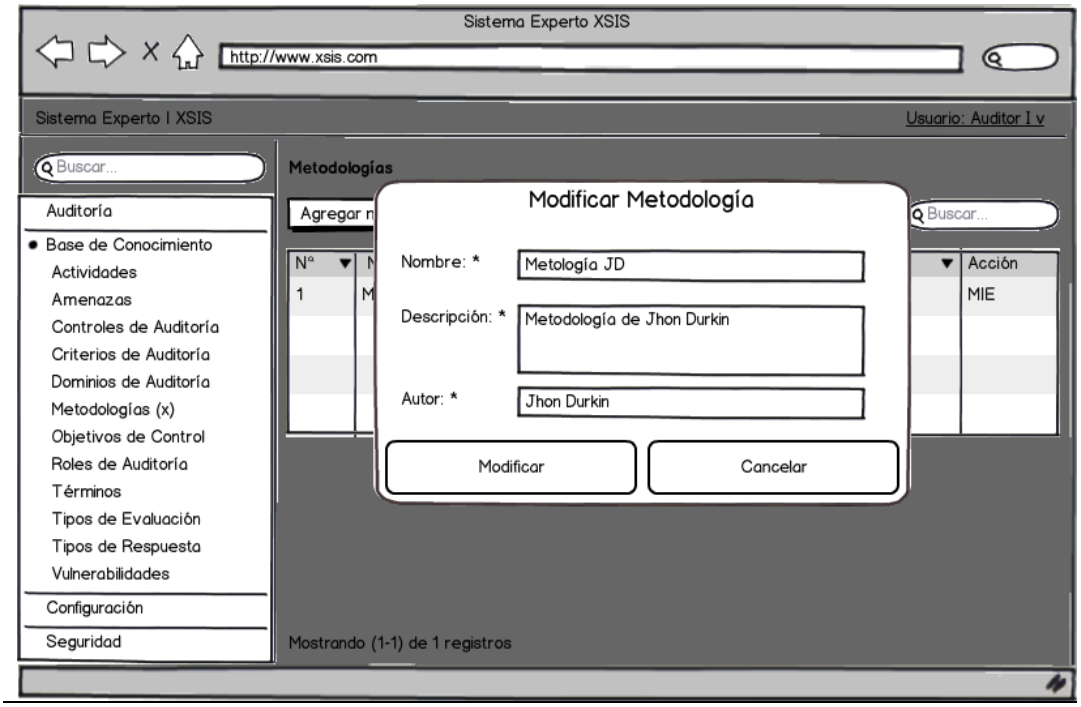
Módulo de Base de Conocimiento

a. Metodología

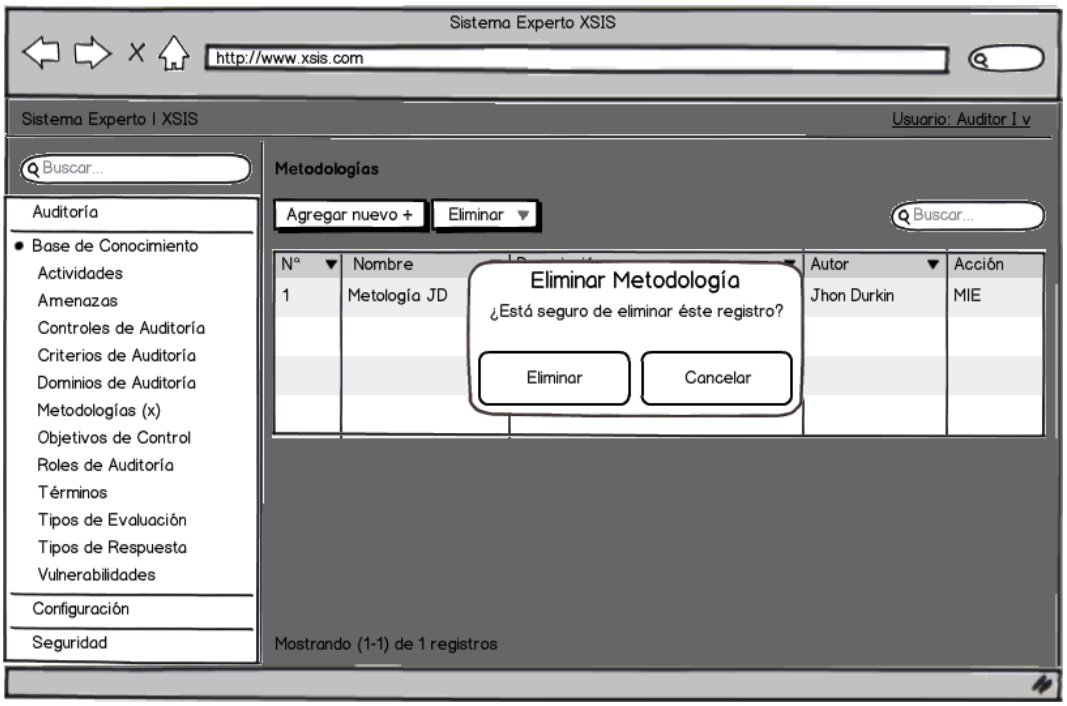
- **Registrar metodología**



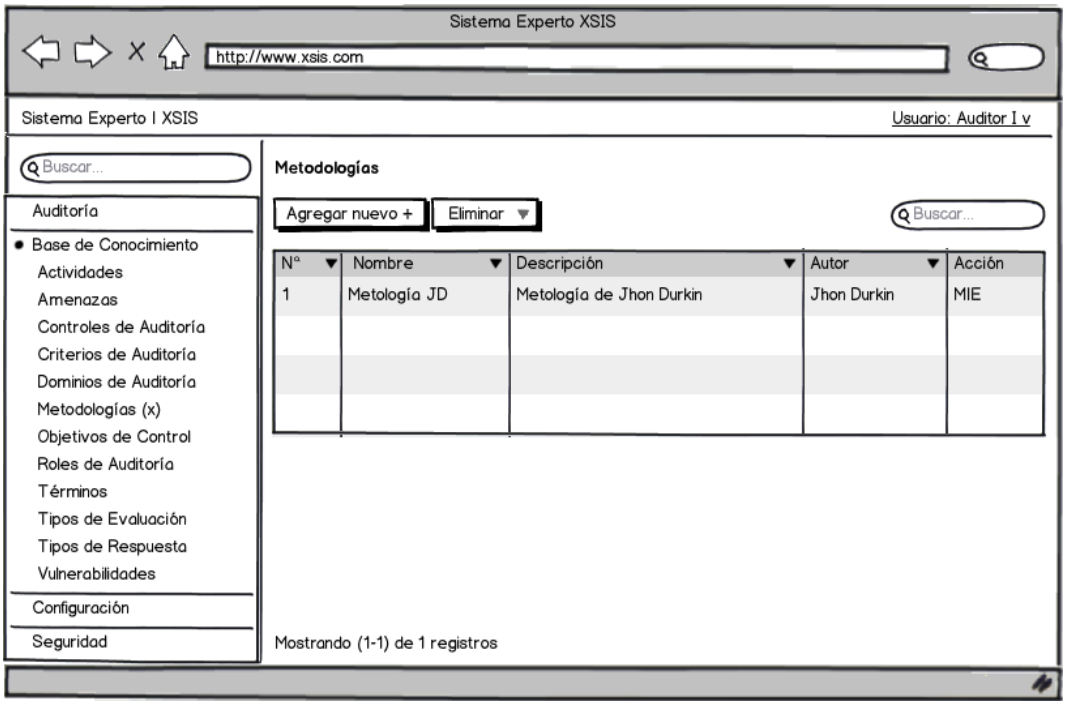
- **Modificar metodología**



- **Eliminar metodología**

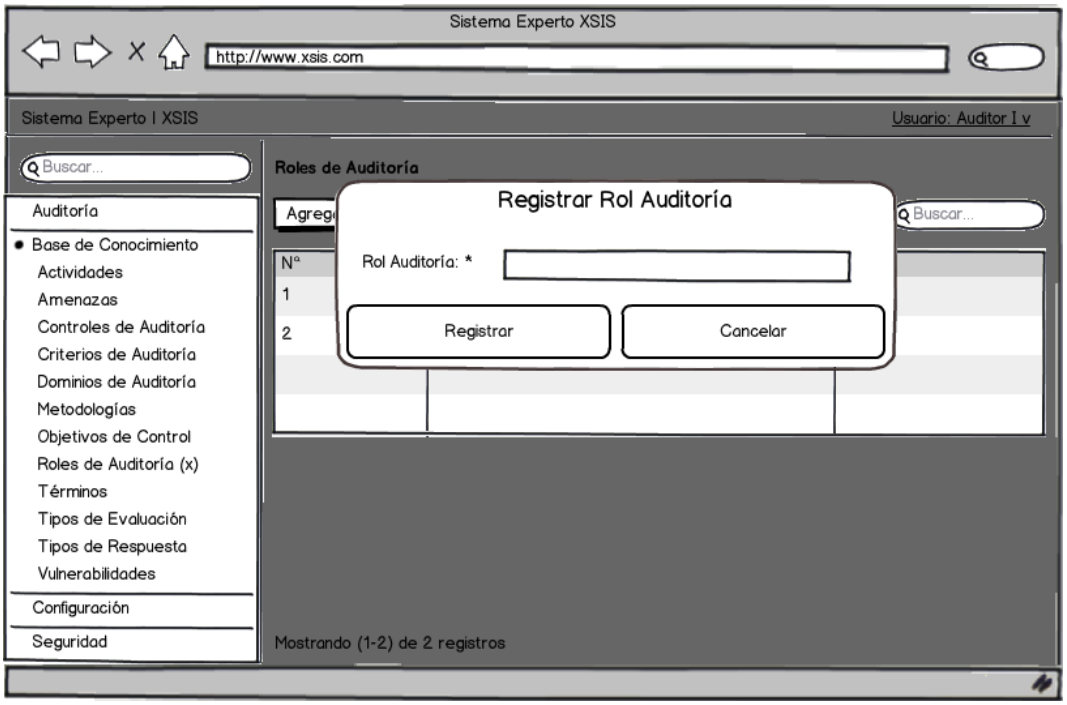


- **Listar metodologías**

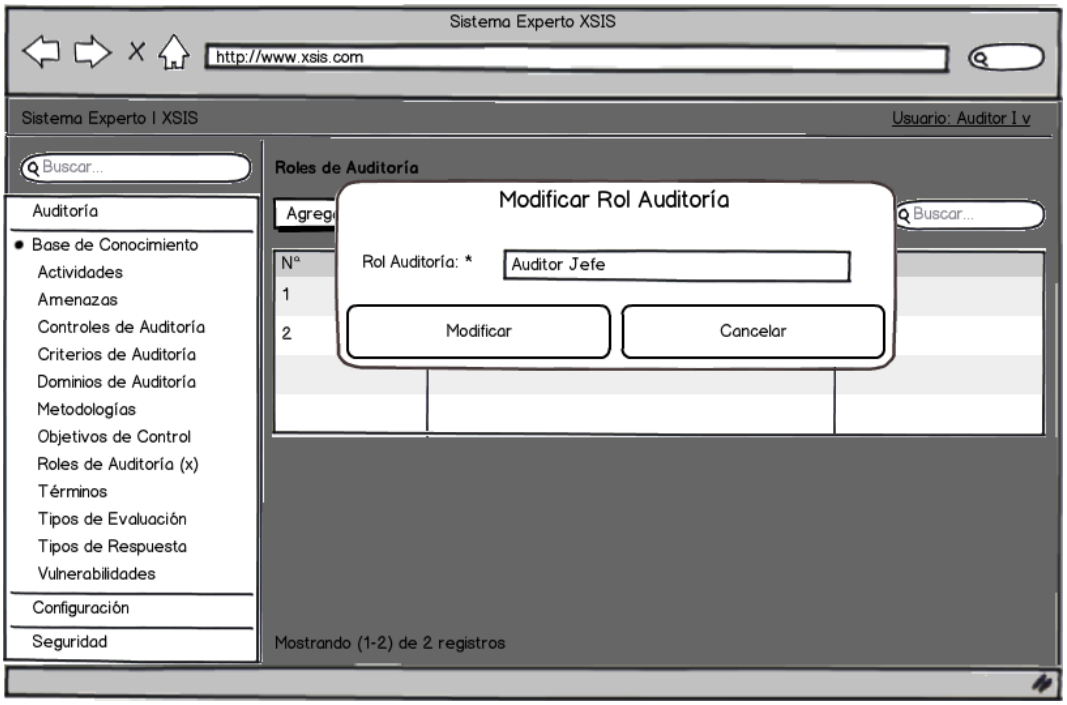


b. Roles auditoría

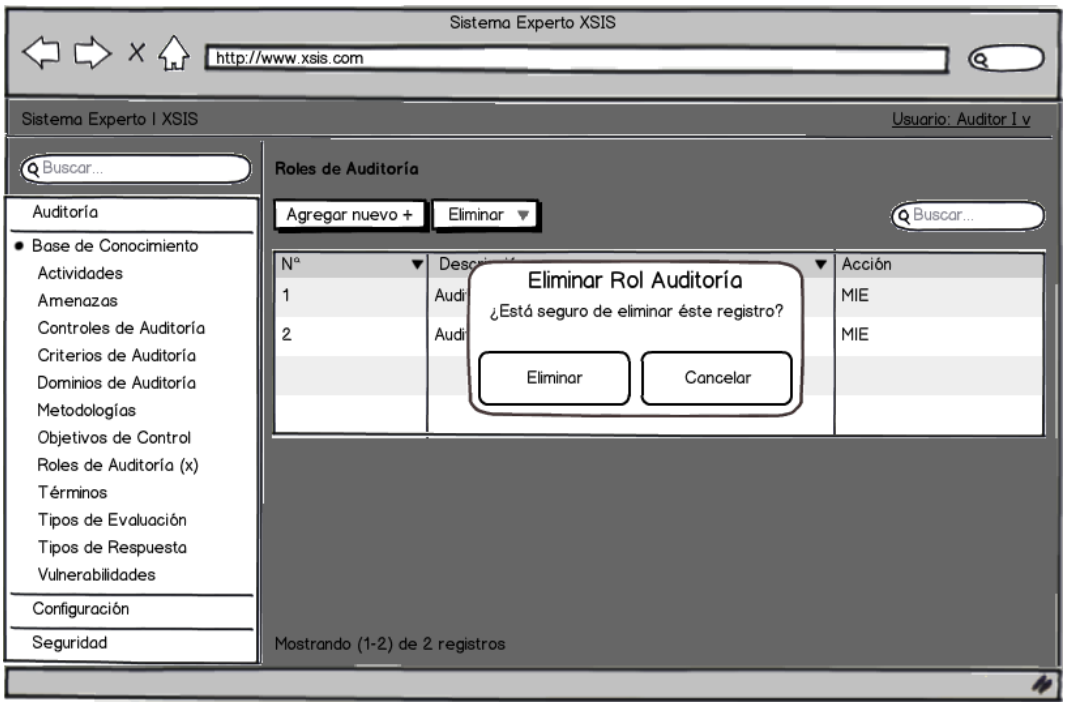
- **Registrar rol auditoría**



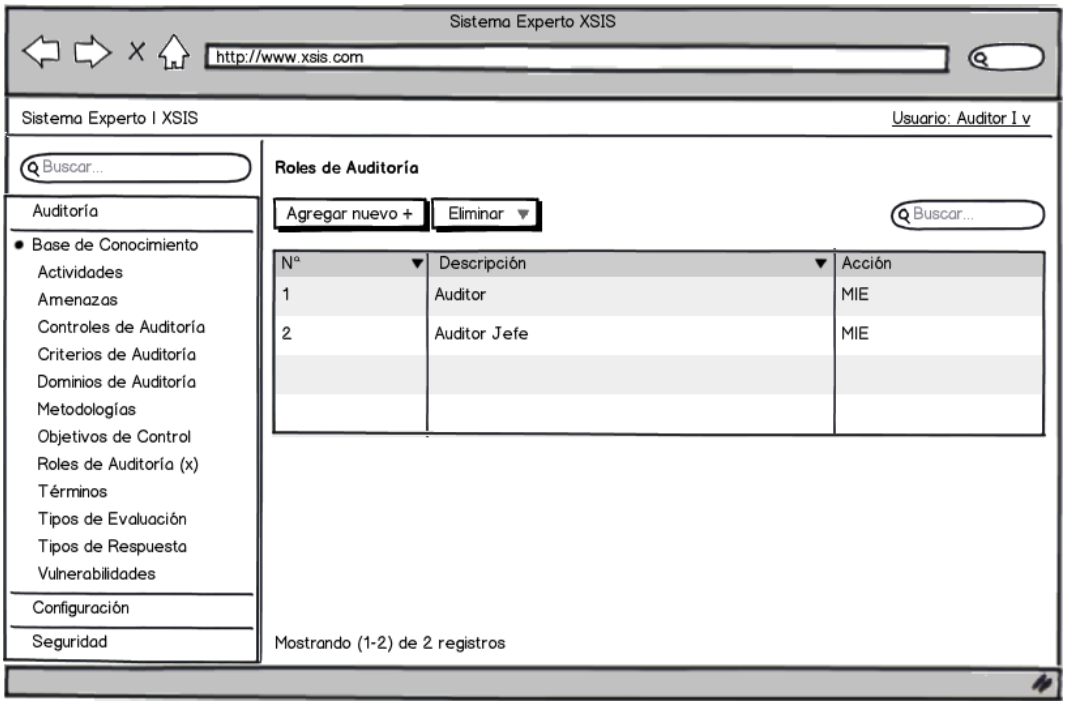
- **Modificar rol auditoría**



- **Eliminar rol auditoría**

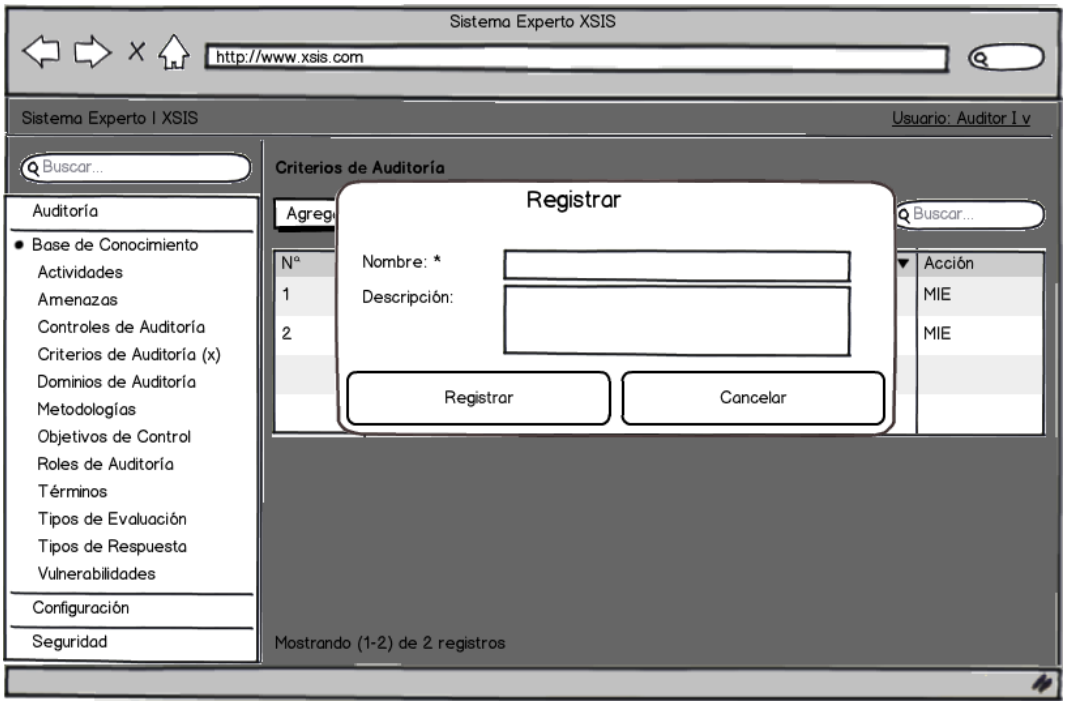


- **Listar roles auditoría**

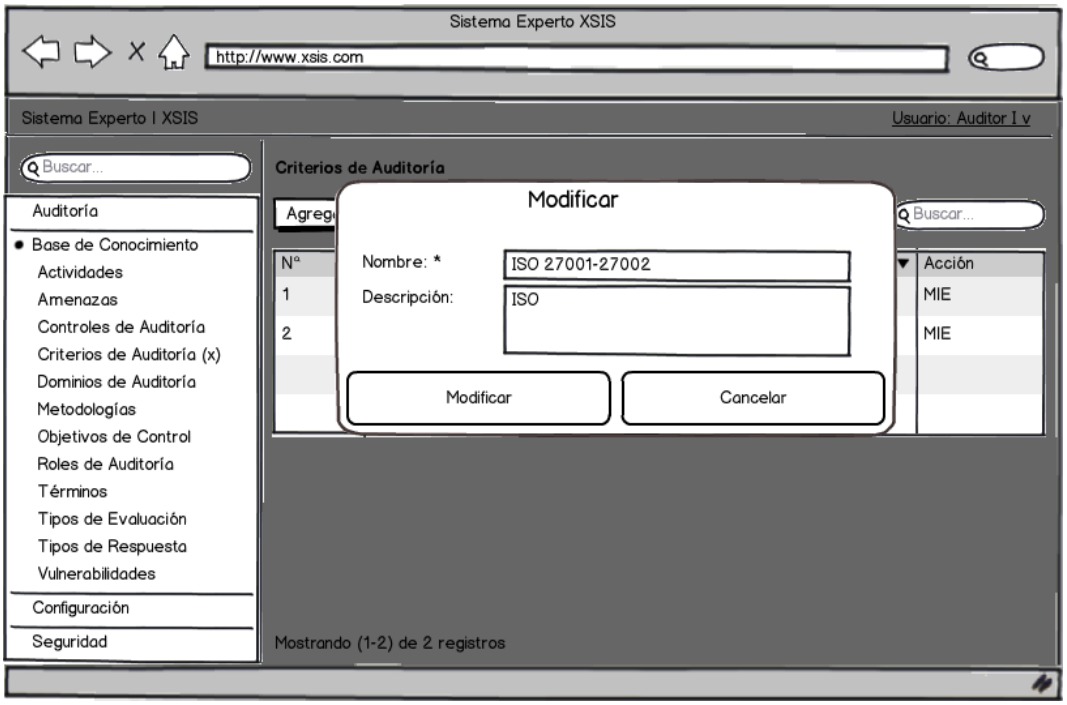


c. Criterios

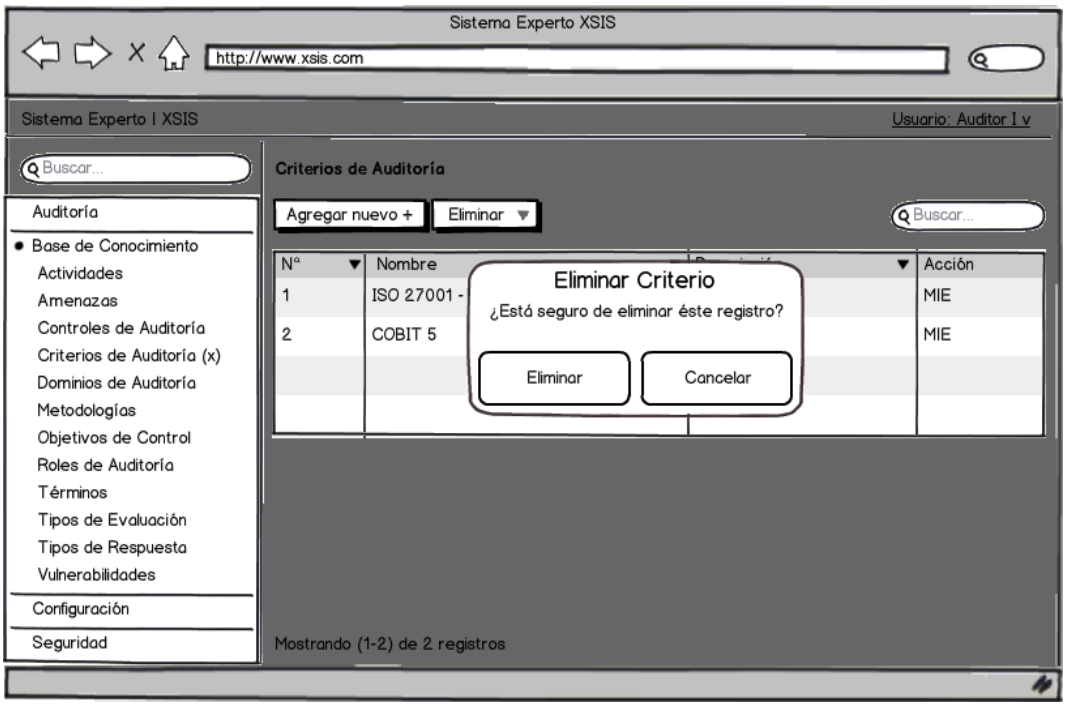
- **Registrar criterio**



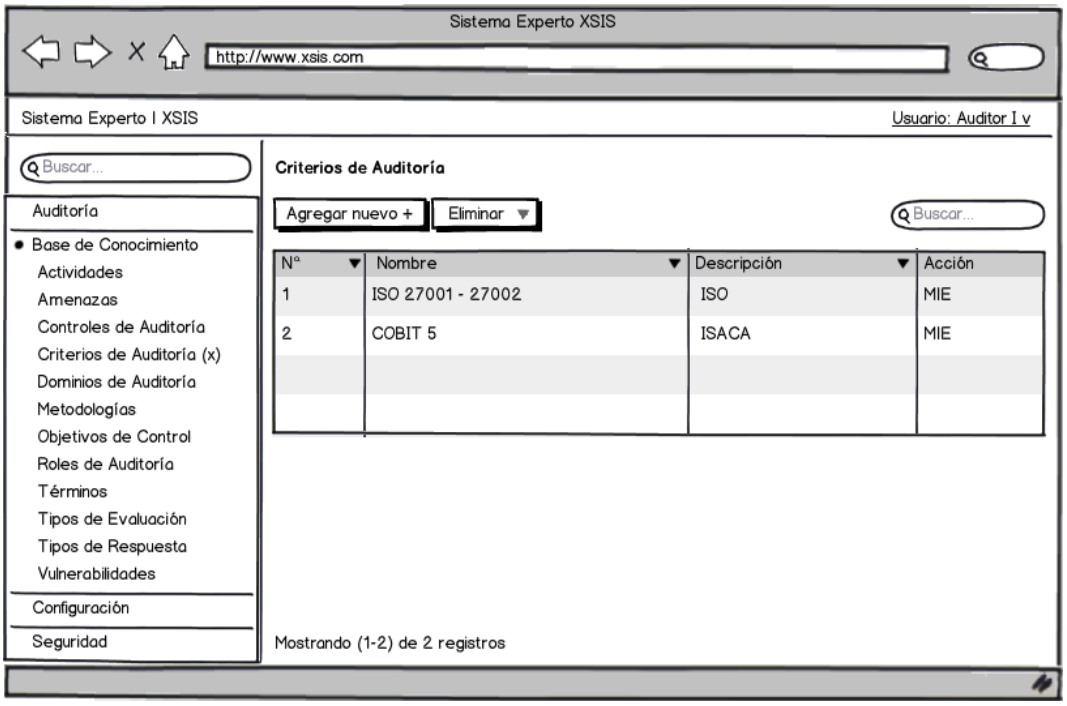
- **Modificar criterio**



- **Eliminar criterio**

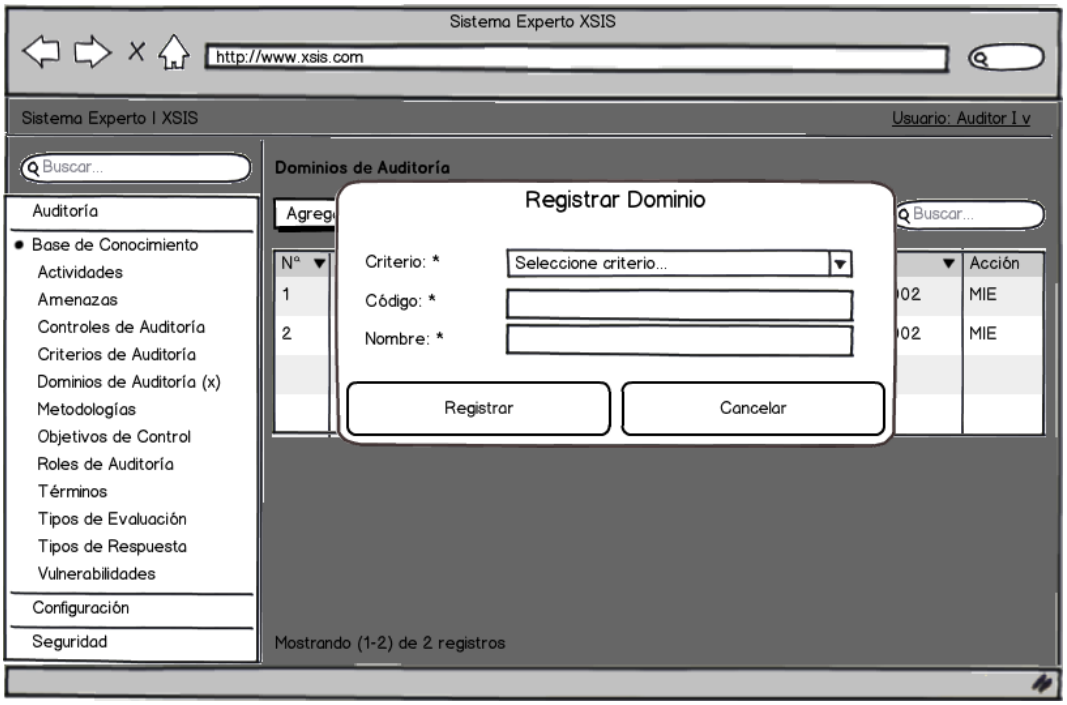


- **Listar criterios**

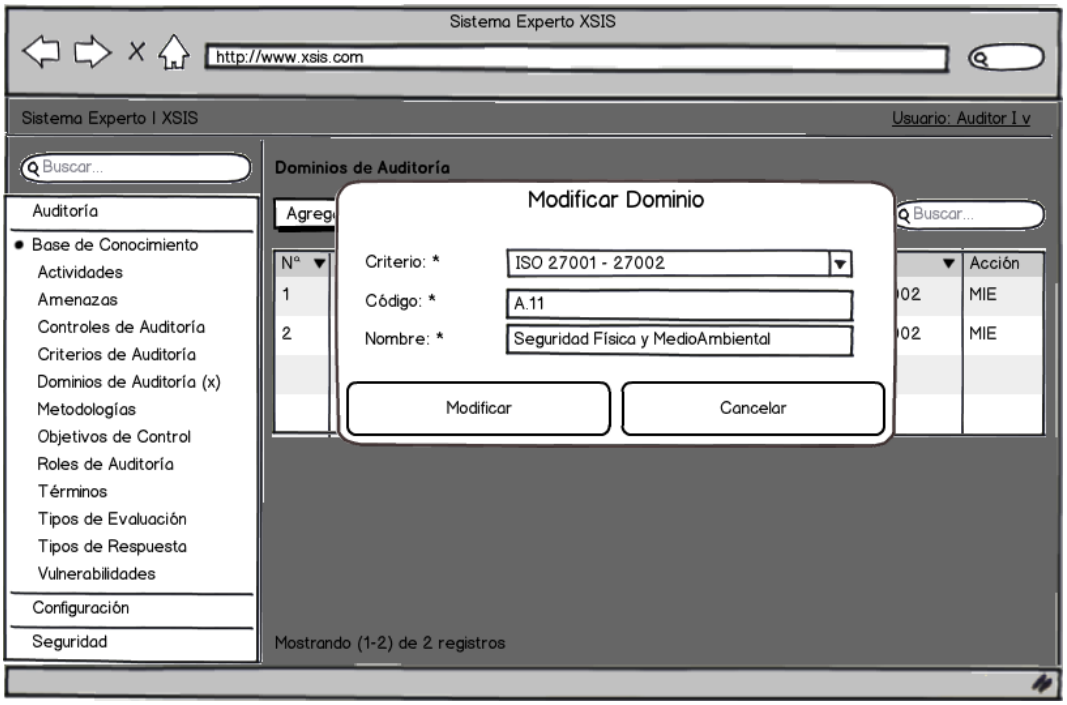


d. Dominios

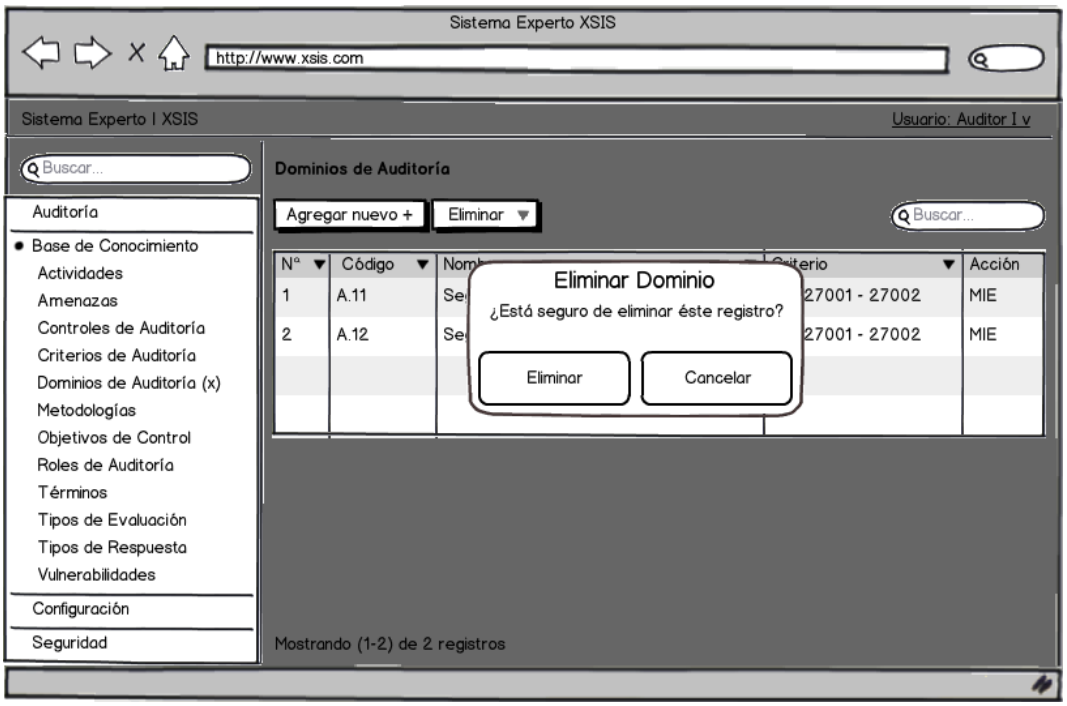
- **Registrar dominio**



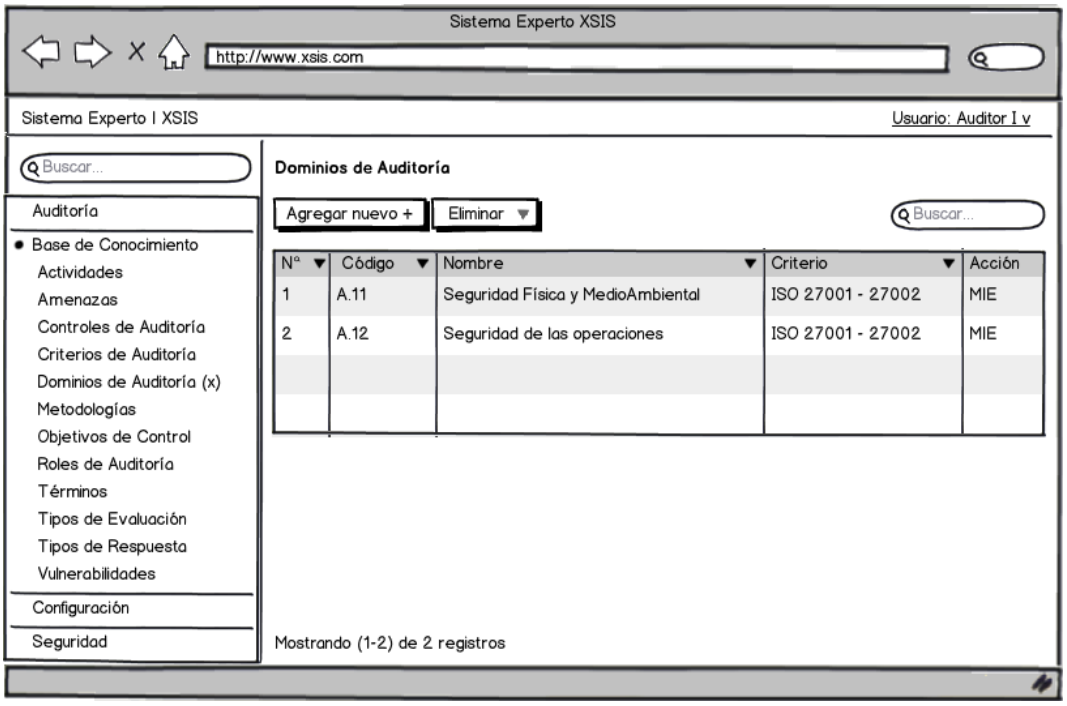
- **Modificar dominio**



- **Eliminar dominio**

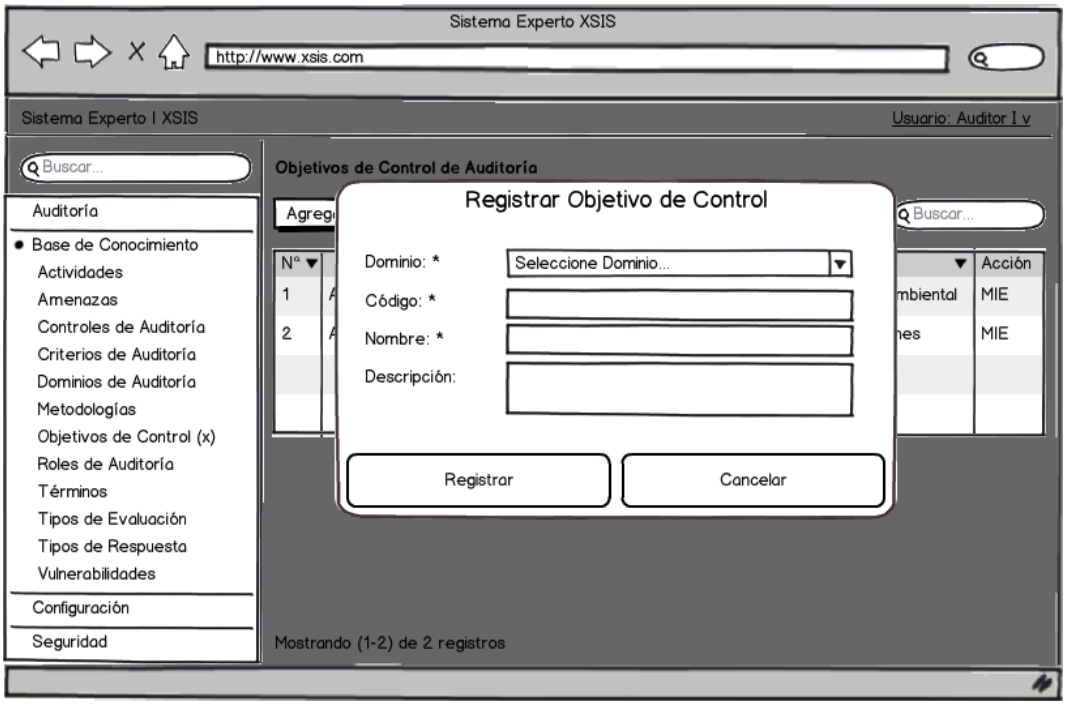


- **Listar dominios**

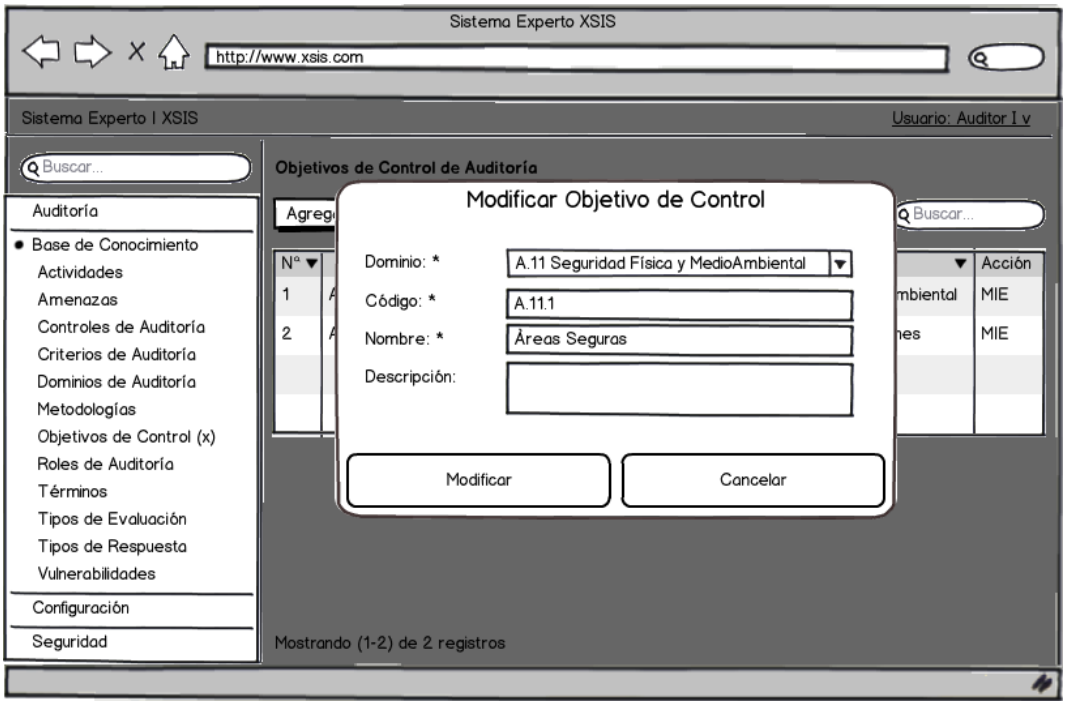


e. Objetivos de control de auditoría

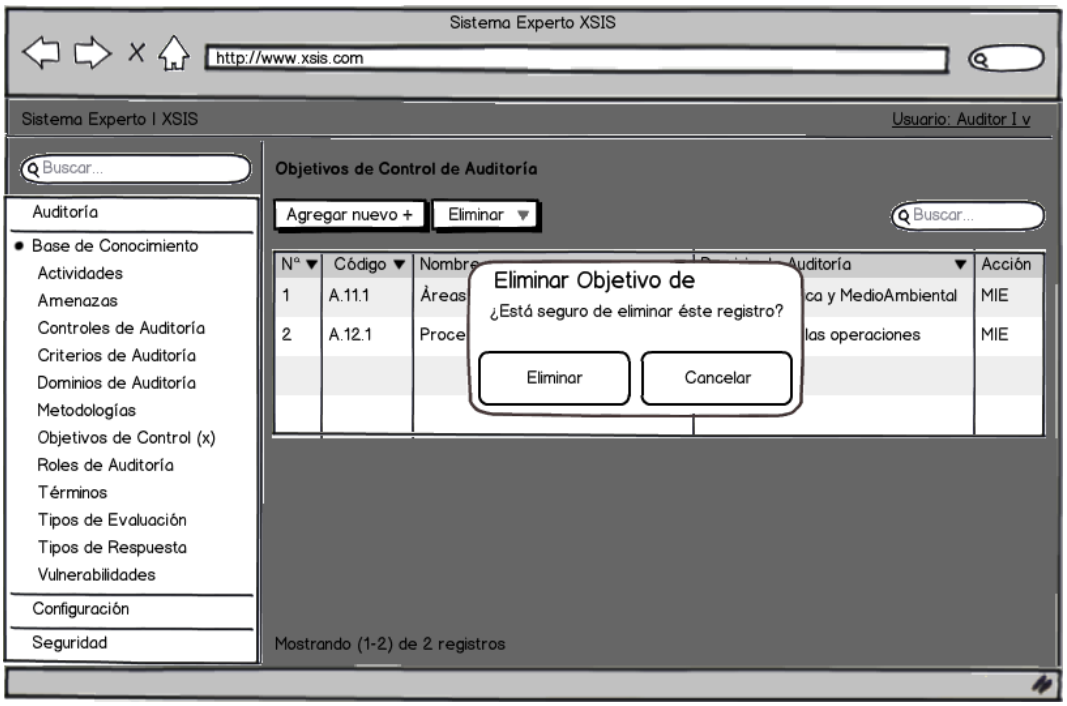
- **Registrar objetivo de control**



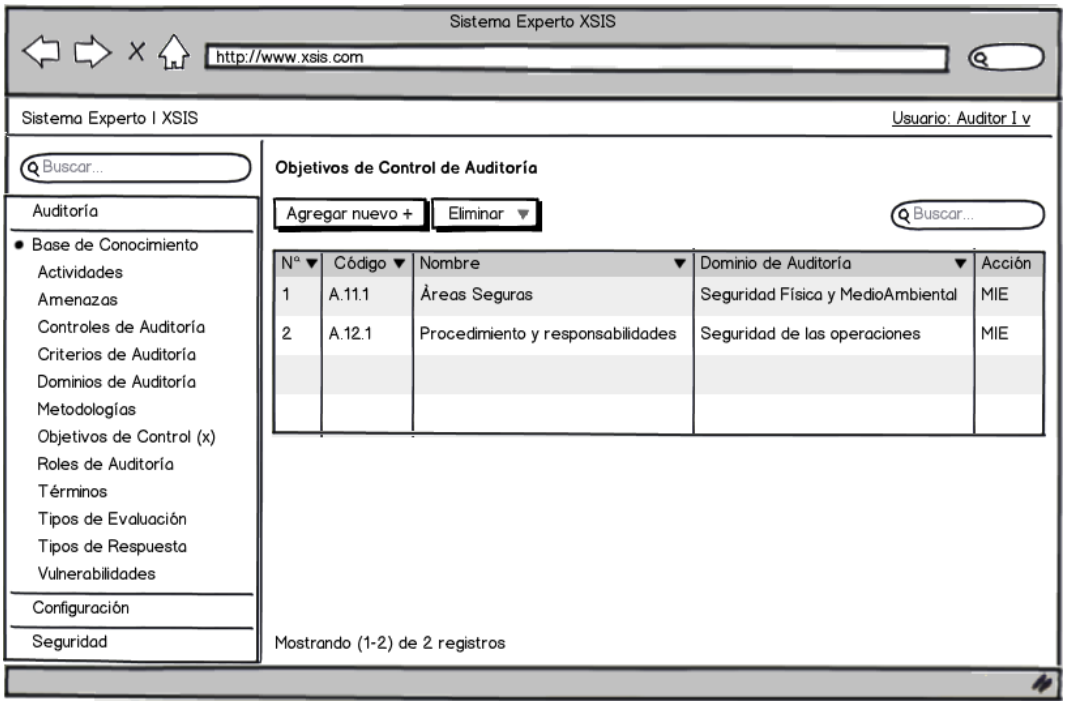
- **Modificar objetivo de control**



- **Eliminar objetivo de control**

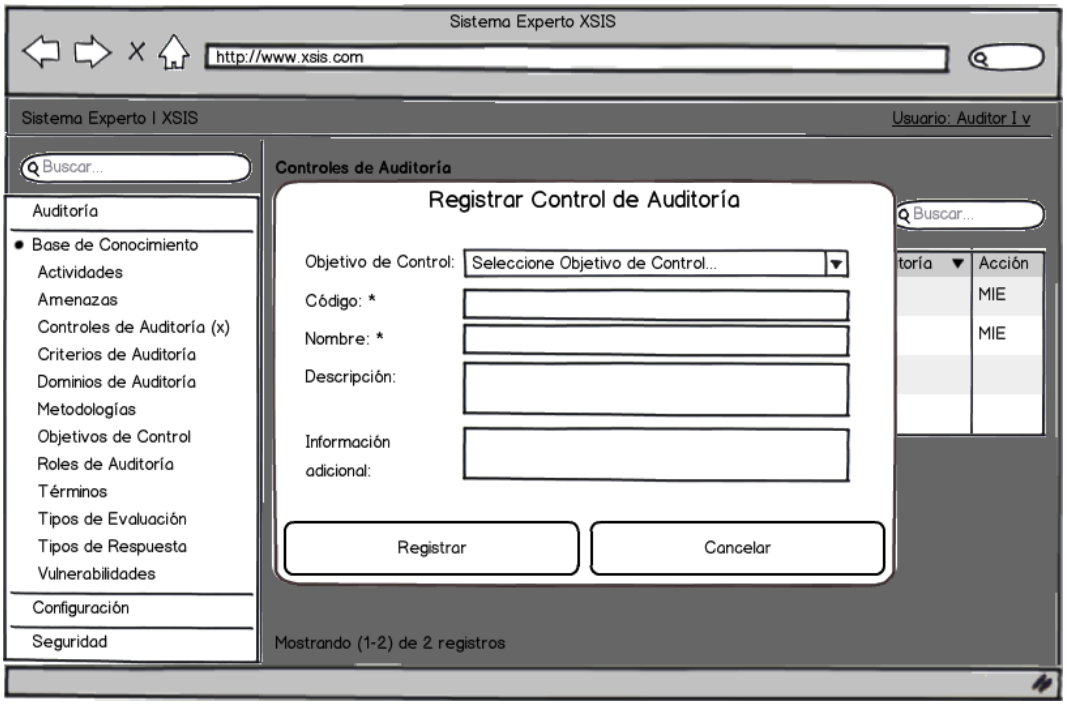


- **Listar objetivos de control**

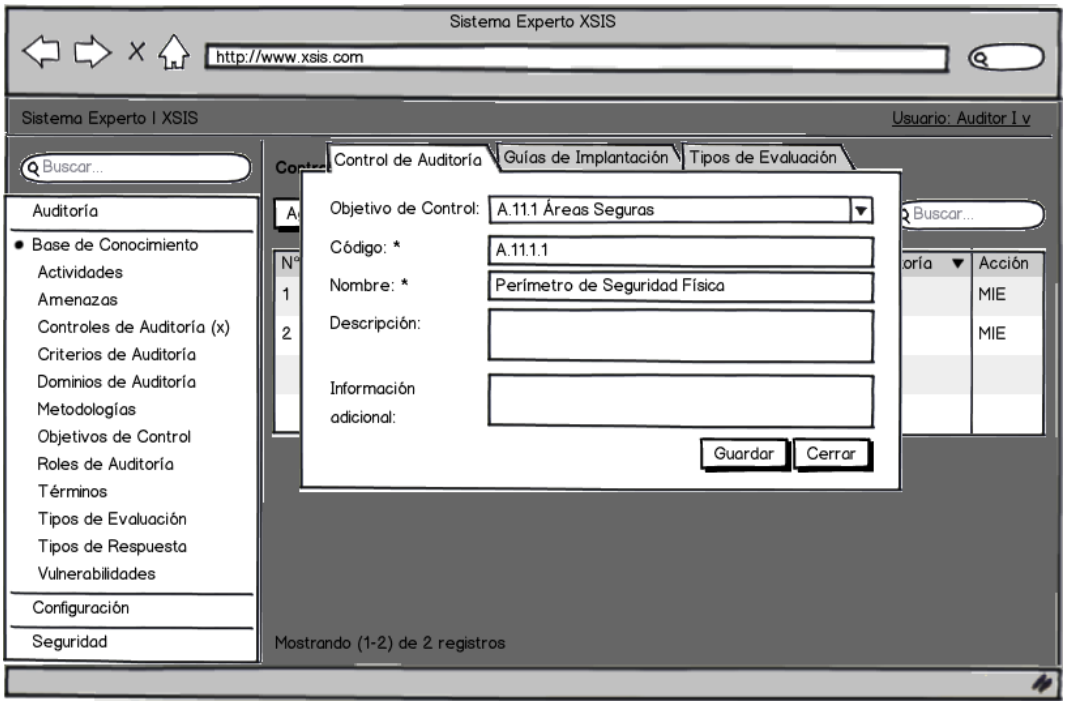


f. Control de Auditoría

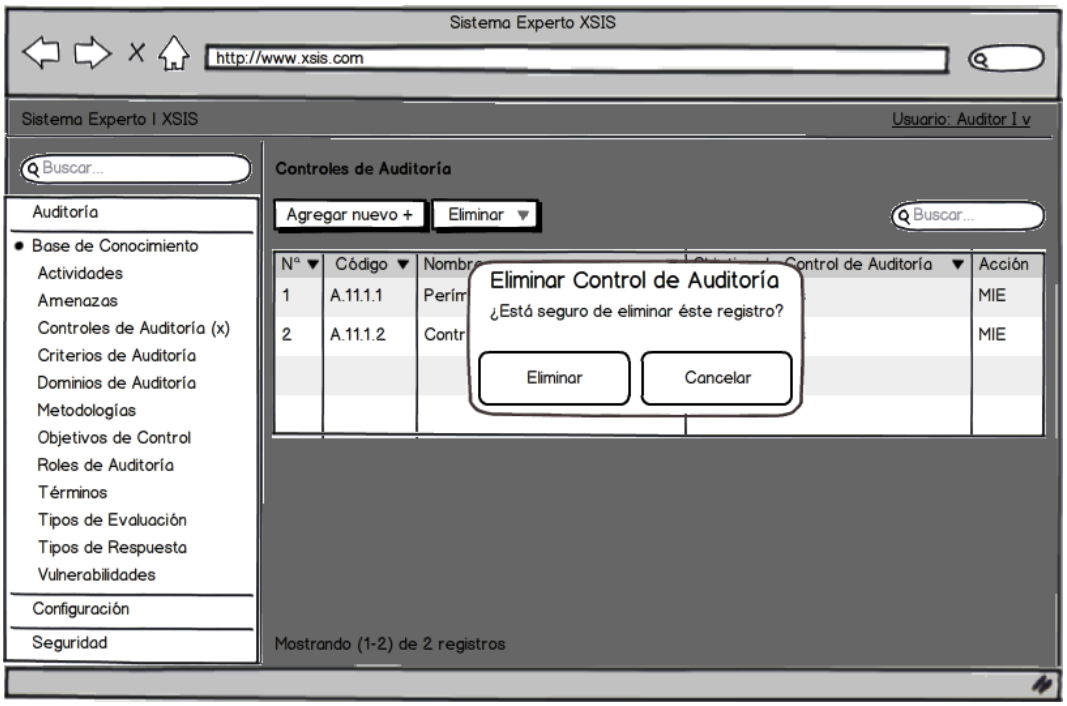
- **Registrar Control Auditoría**



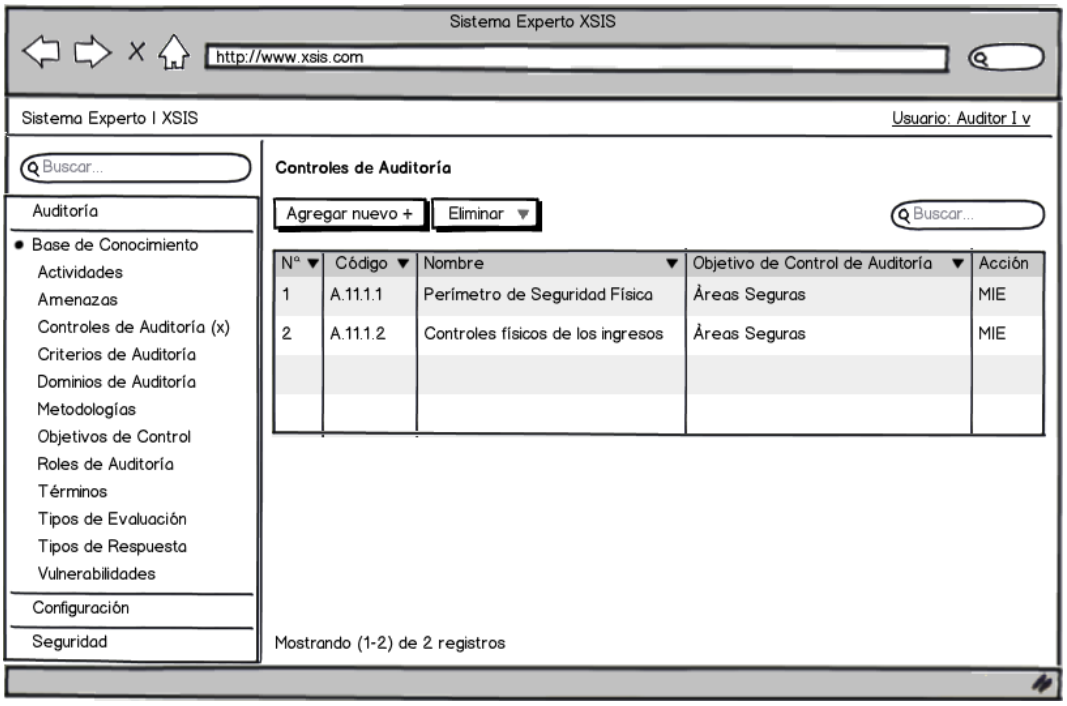
- **Modificar Control de Auditoría**



- **Eliminar Control de Auditoría**

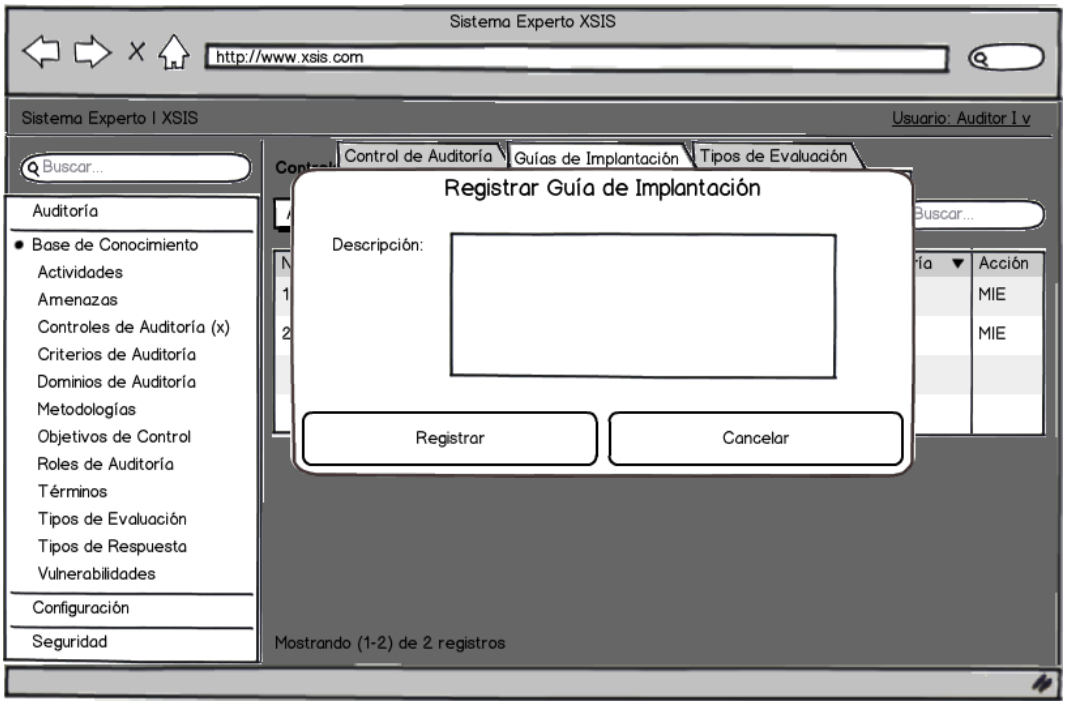


- **Listar controles de Auditoría**

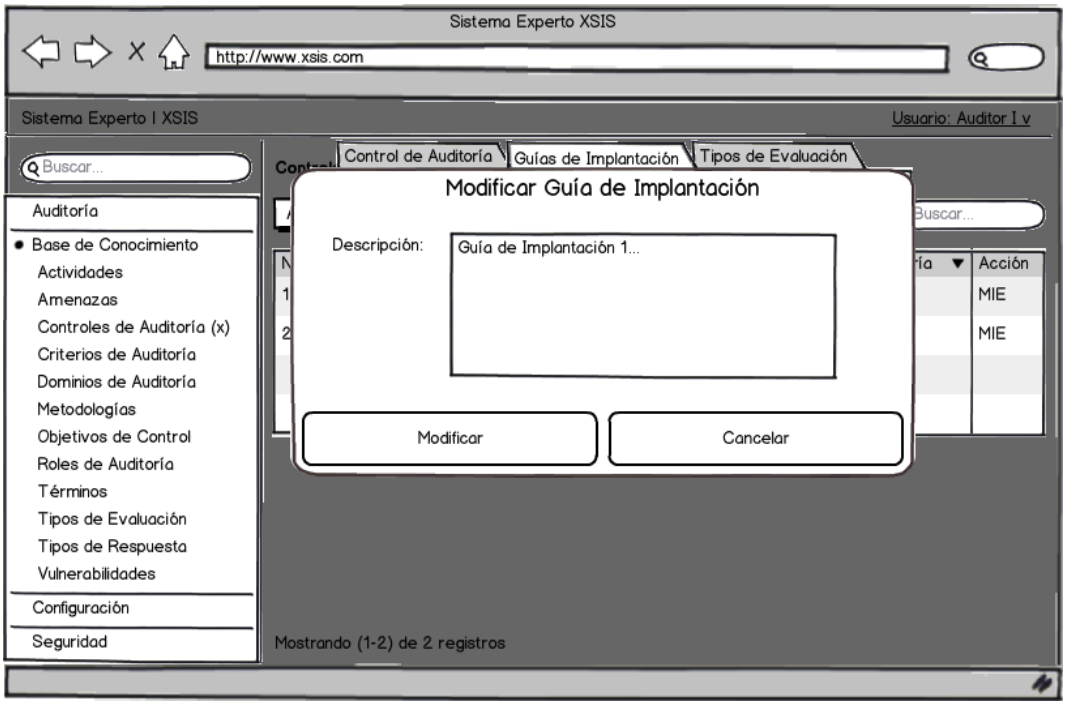


g. Guía de Implantación

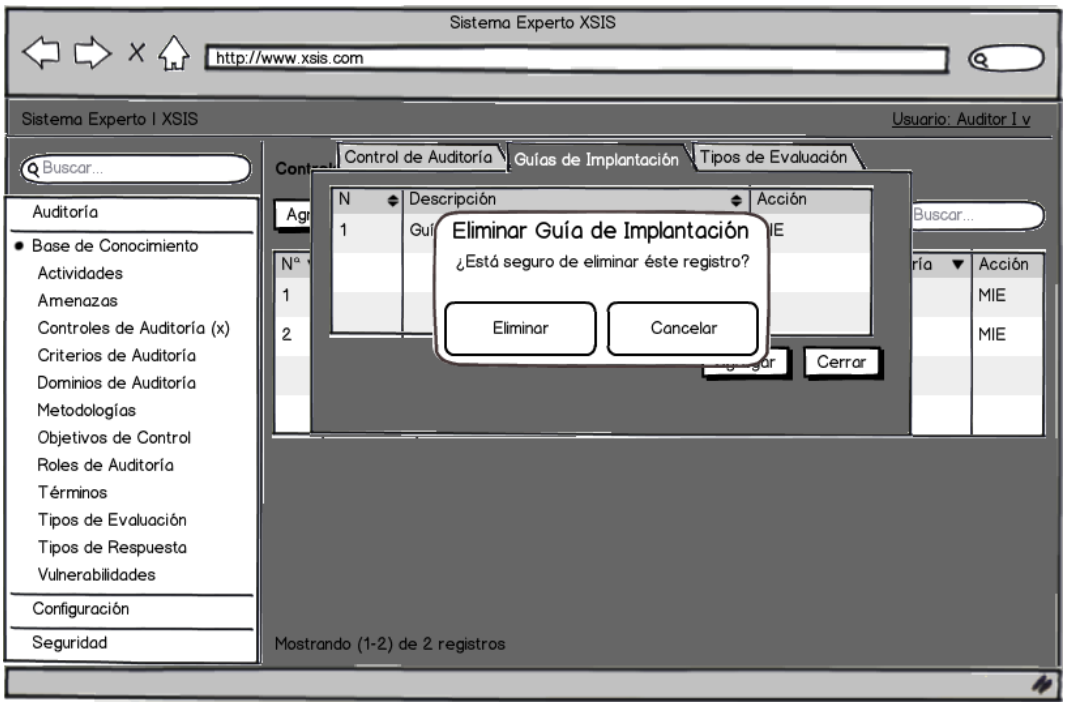
- **Registrar guía de implantación**



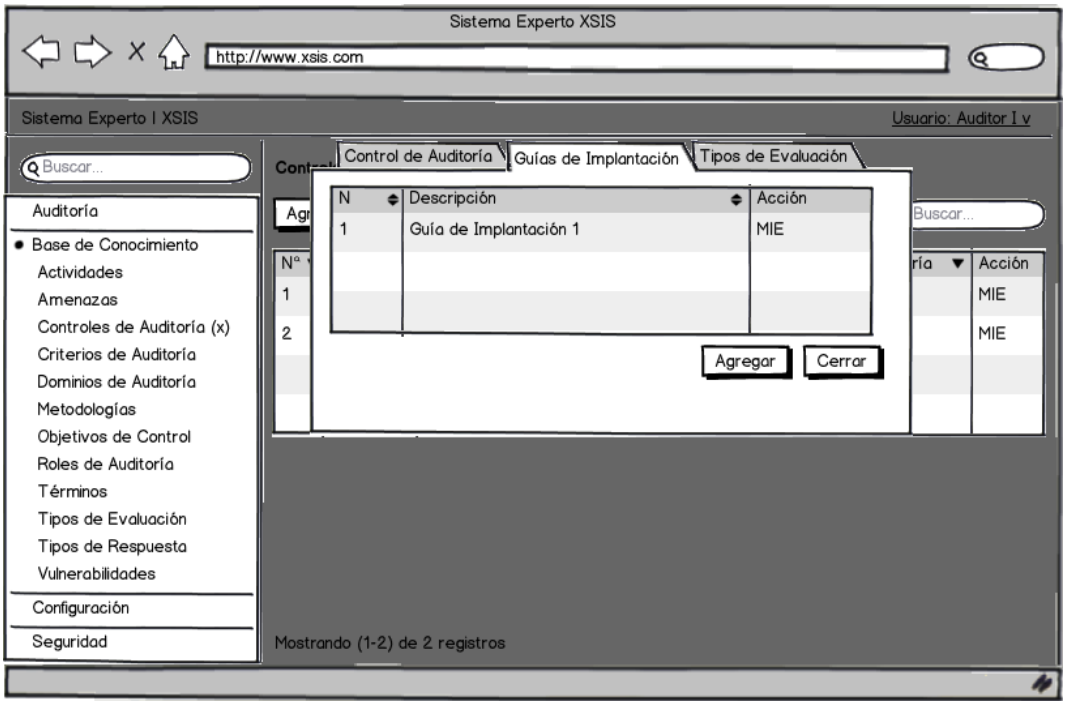
- **Modificar guía de implantación**



- **Eliminar guía de implantación**

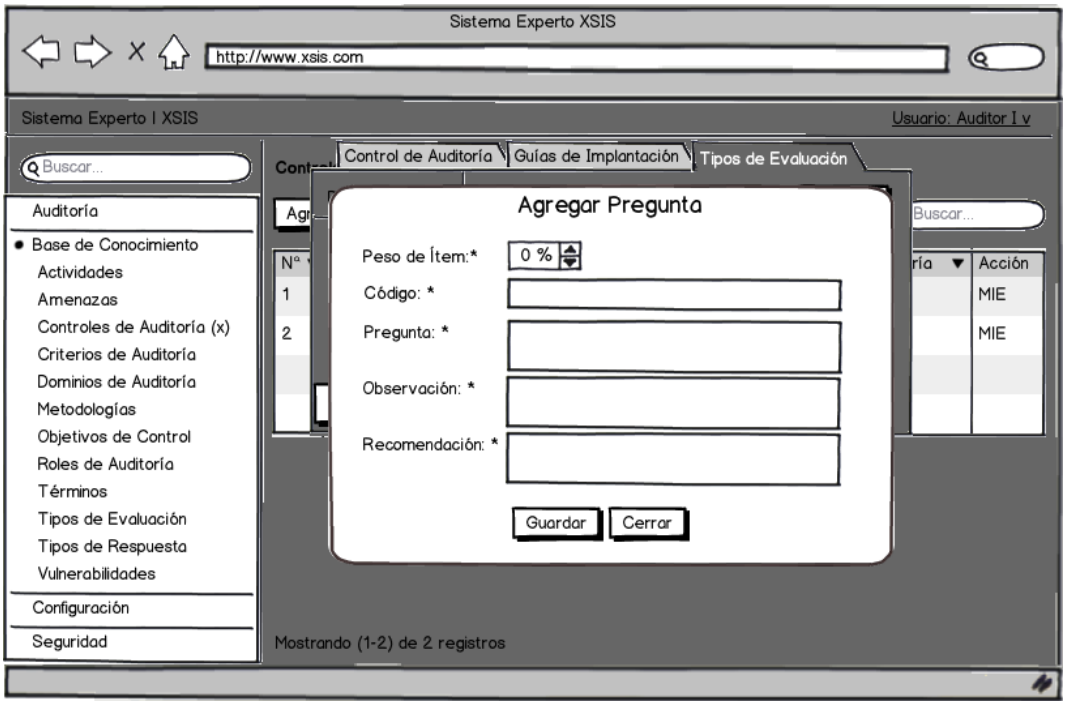


- **Listar guías de implantación**



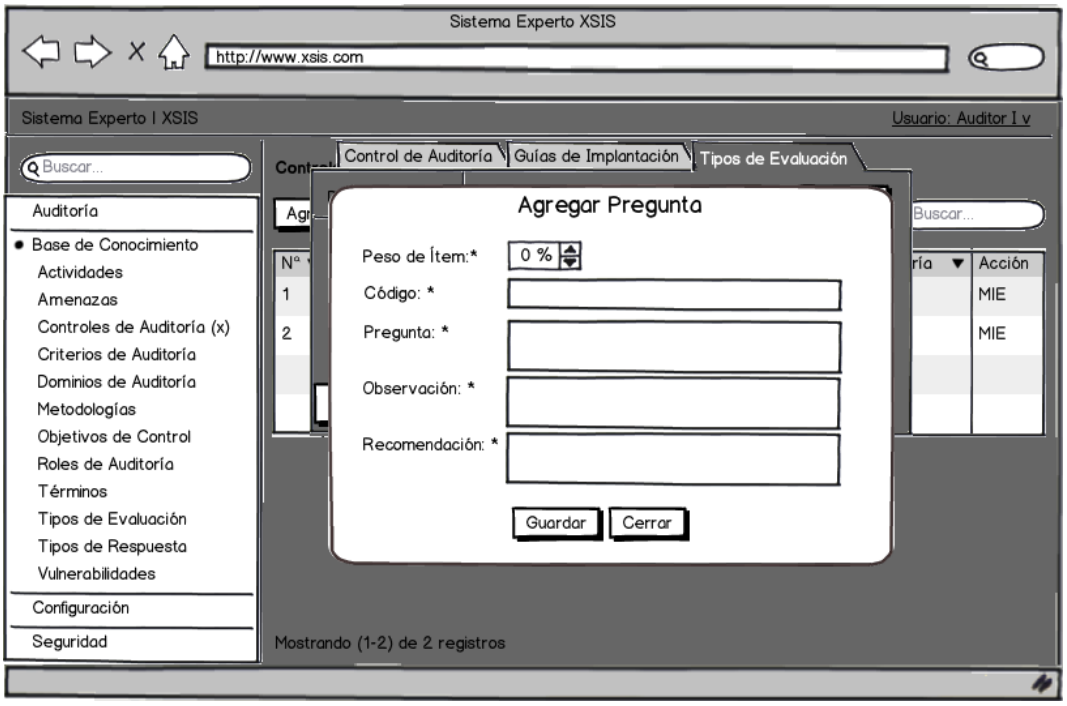
h. Pregunta – Tipo Evaluación

- **Agregar tipo de evaluación – pregunta**

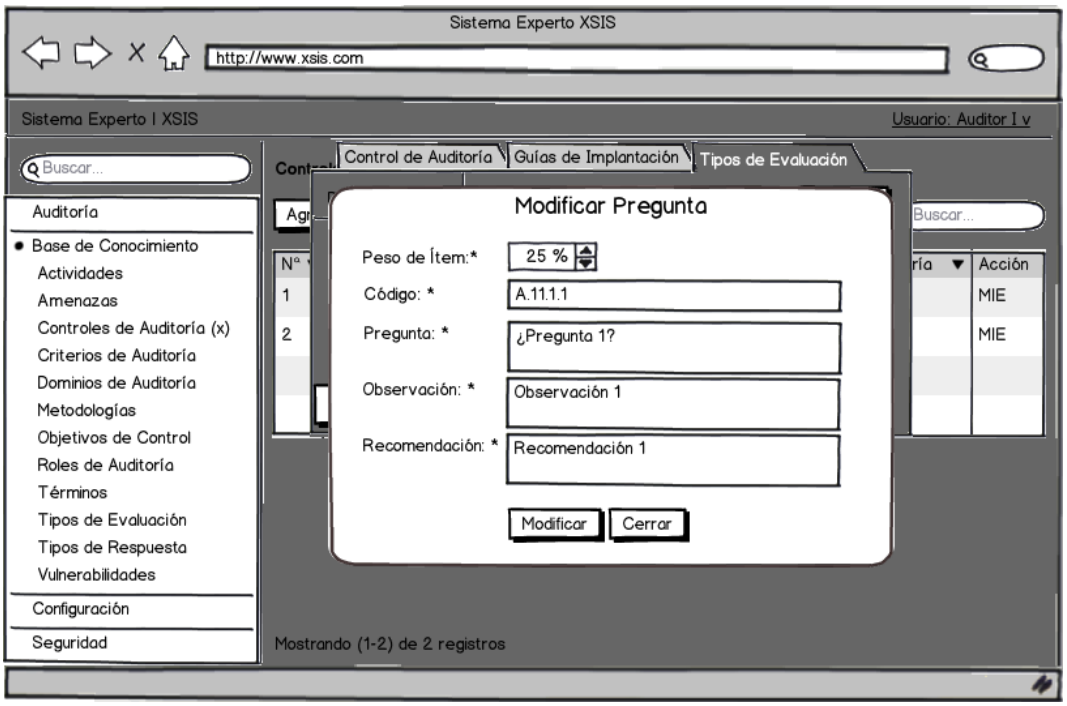


i. Pregunta – control auditoría

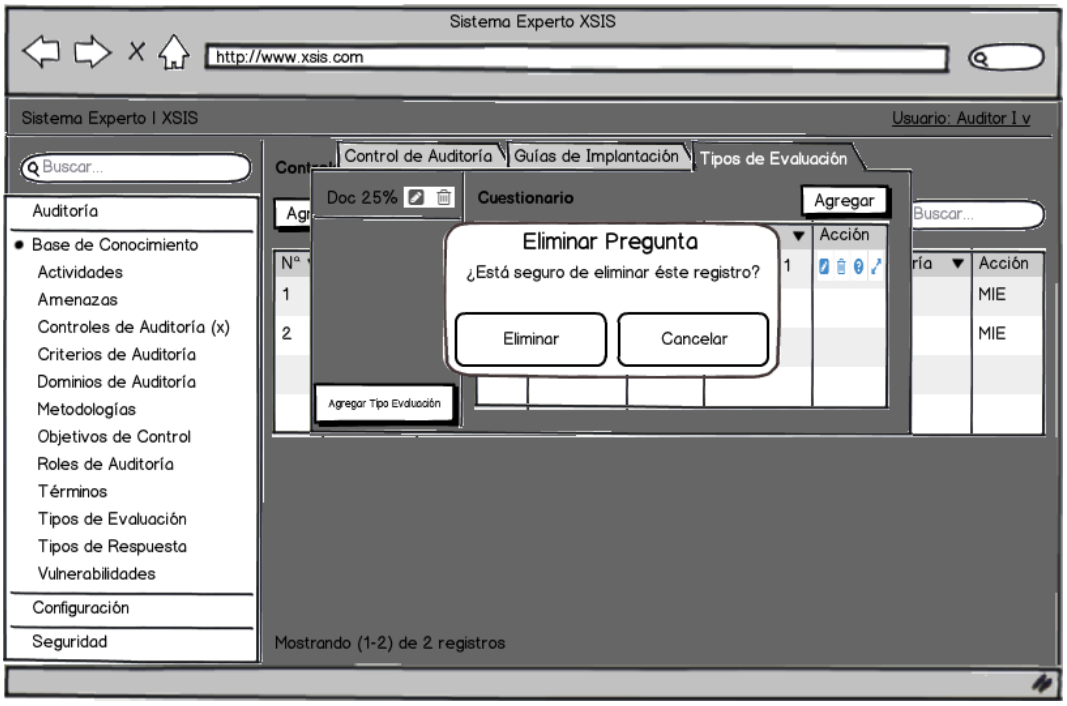
- **Registrar pregunta control auditoría**



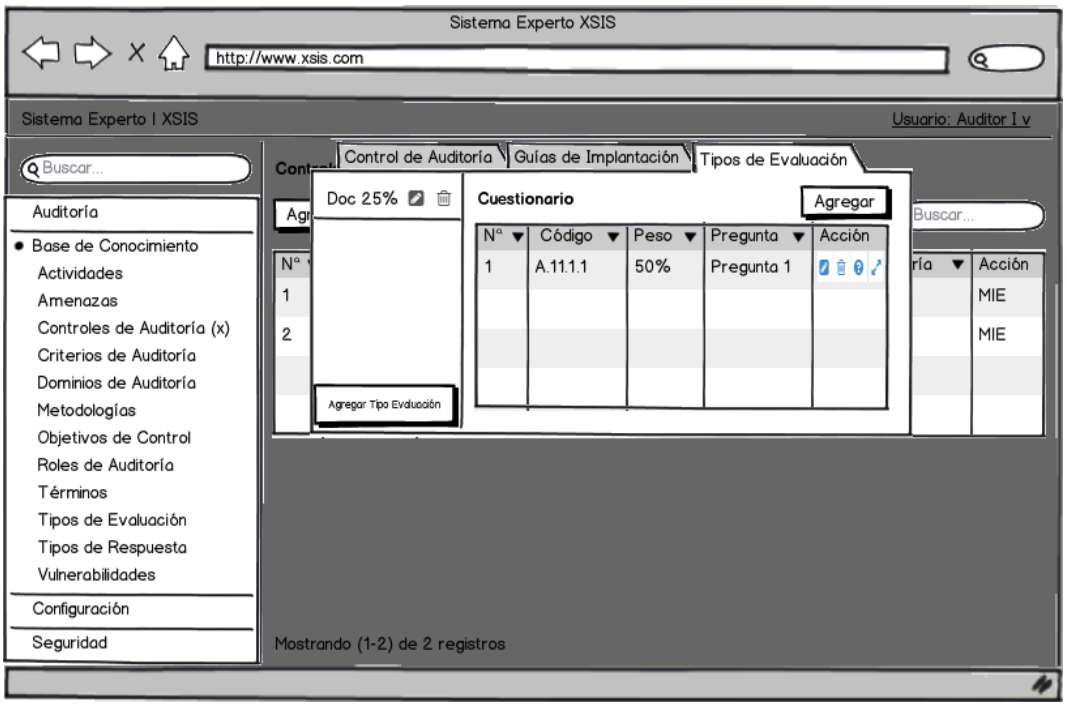
- **Modificar pregunta control auditoría**



- **Eliminar pregunta control auditoría**

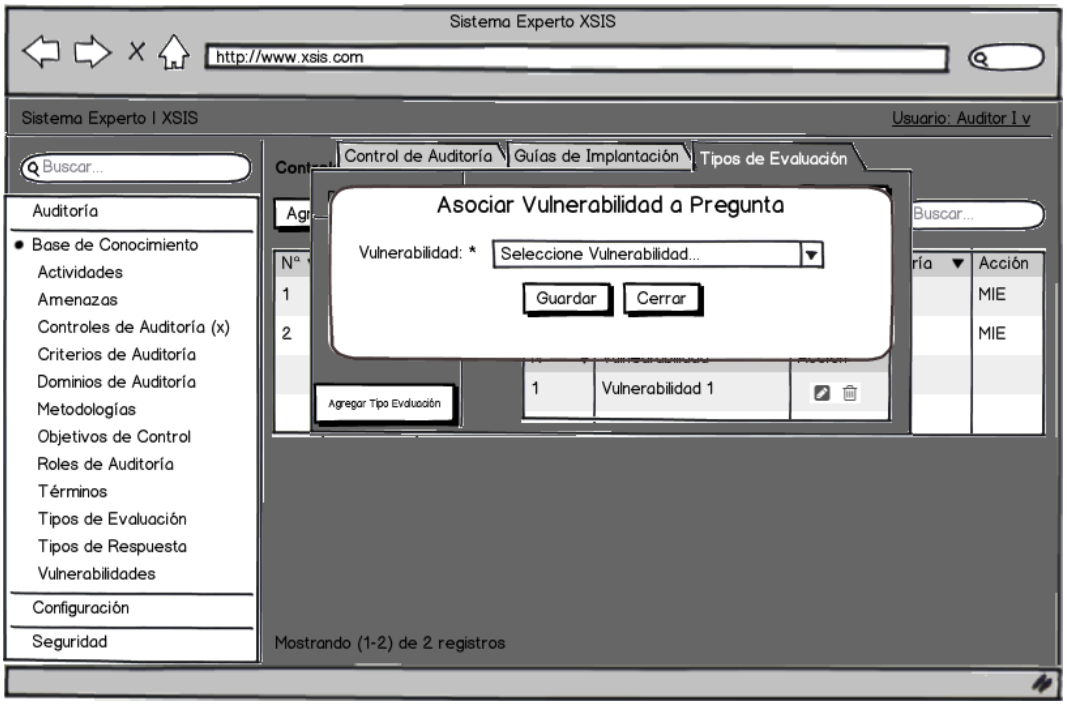


- **Listar preguntas control auditoría**

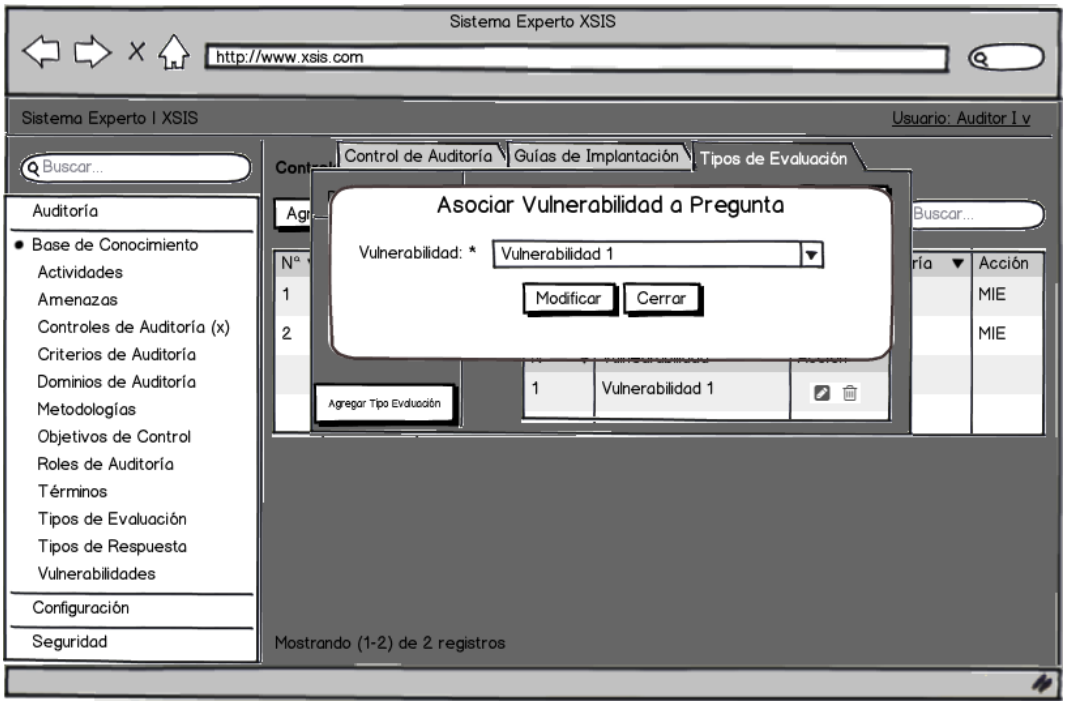


j. Pregunta - Vulnerabilidad

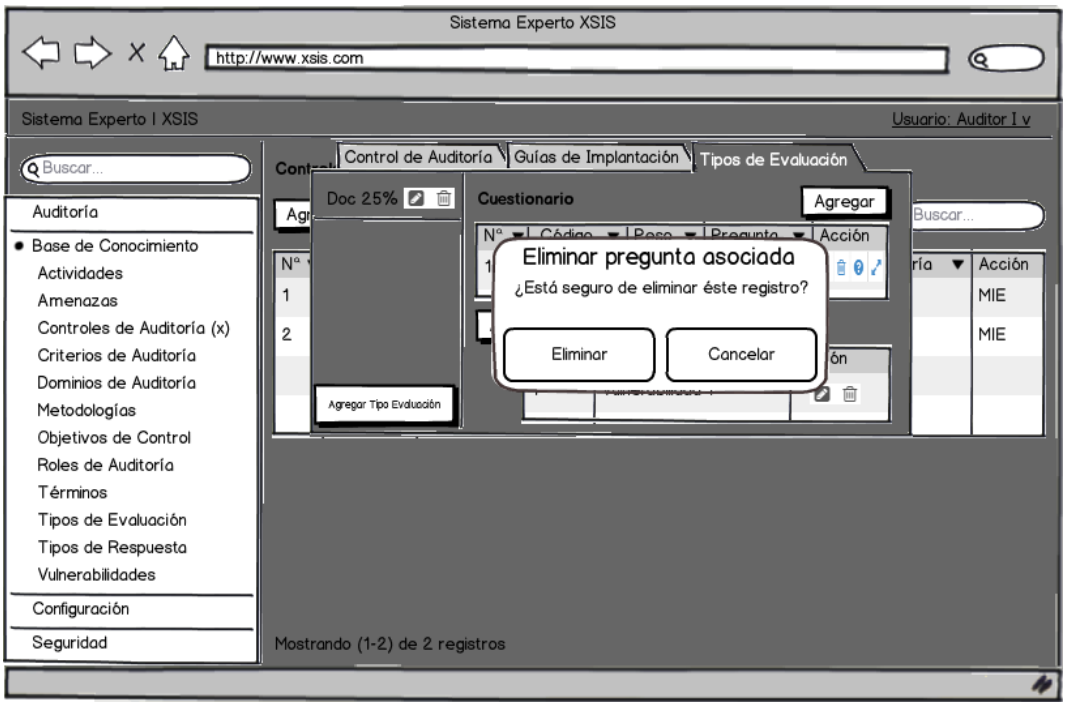
- **Asociar pregunta – vulnerabilidad**



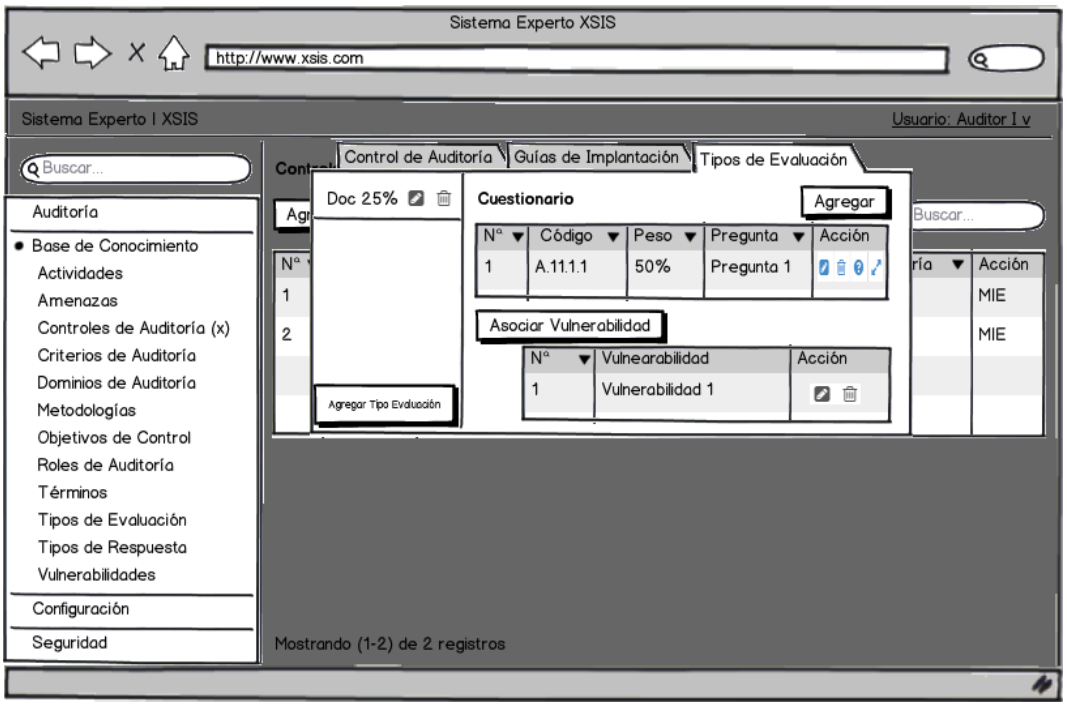
- **Modificar asociación pregunta – vulnerabilidad**



- **Eliminar asociación pregunta – vulnerabilidad**

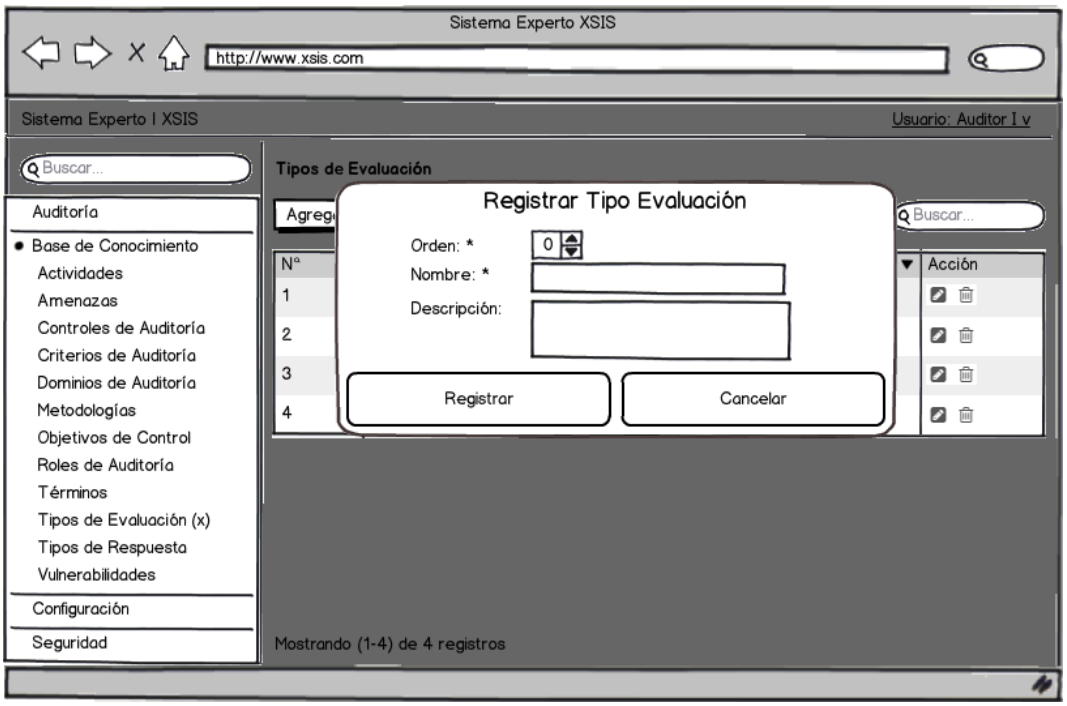


- **Listar vulnerabilidades – pregunta**

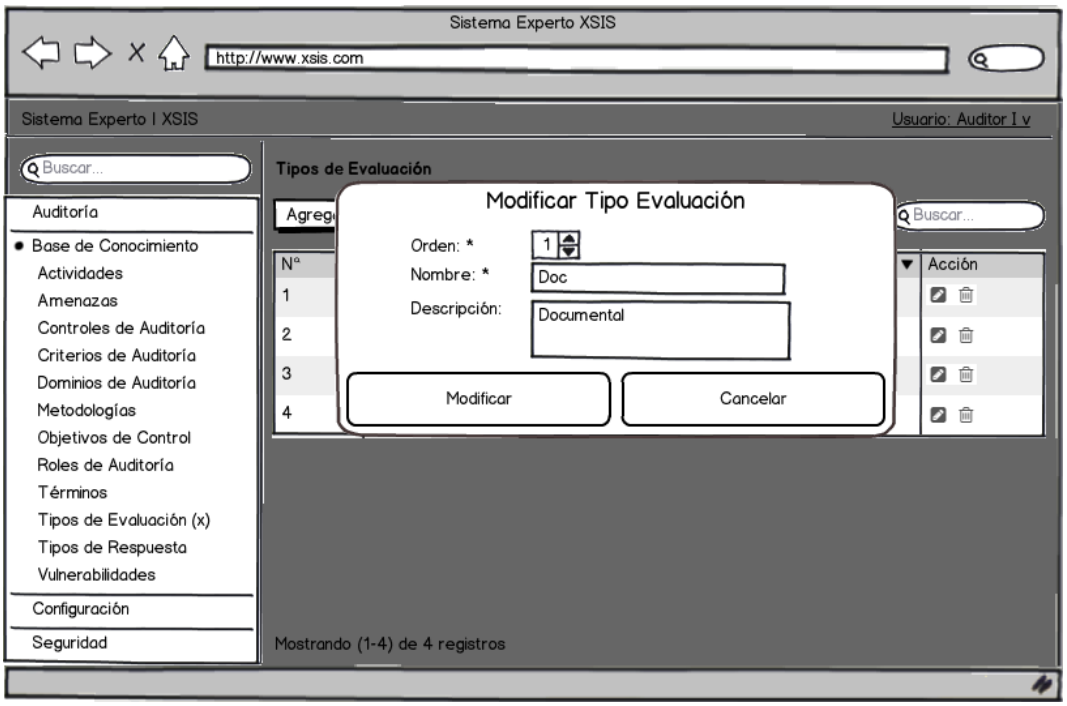


k. Tipos de Evaluación

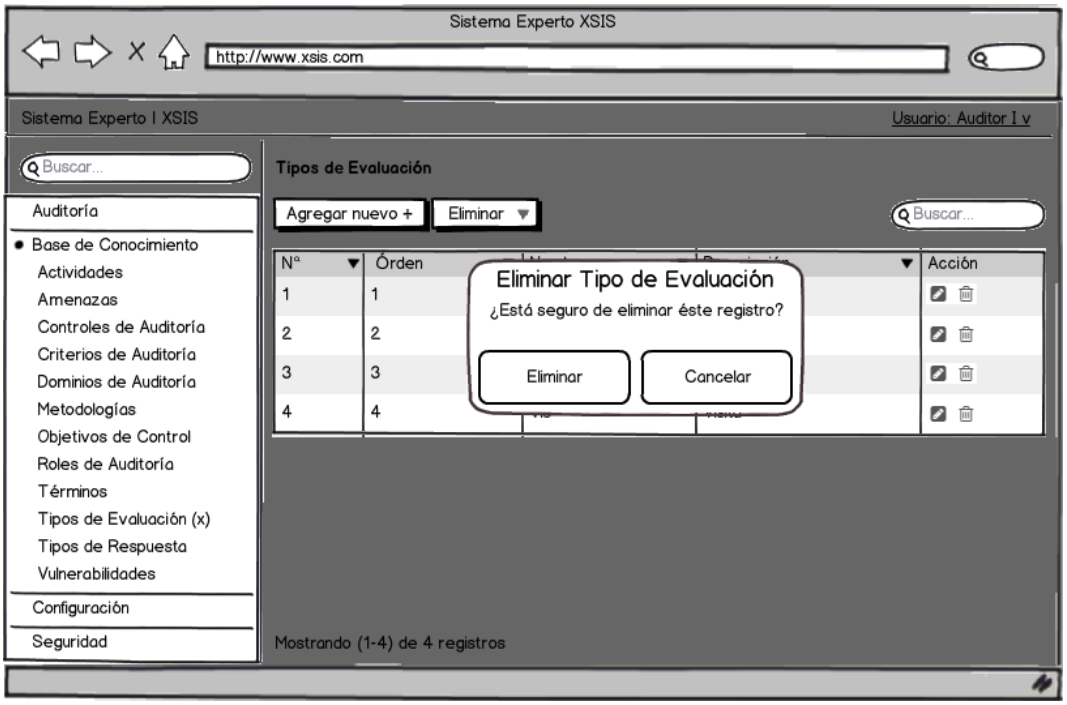
- **Registrar tipo evaluación**



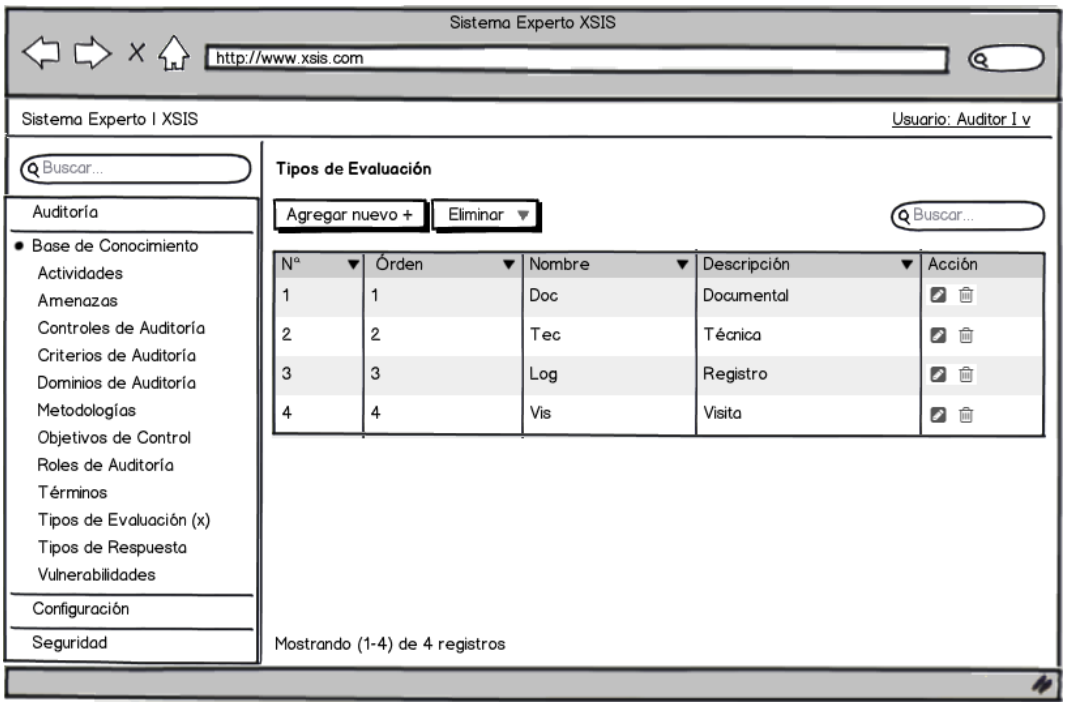
- **Modificar tipo evaluación**



- **Eliminar tipo evaluación**

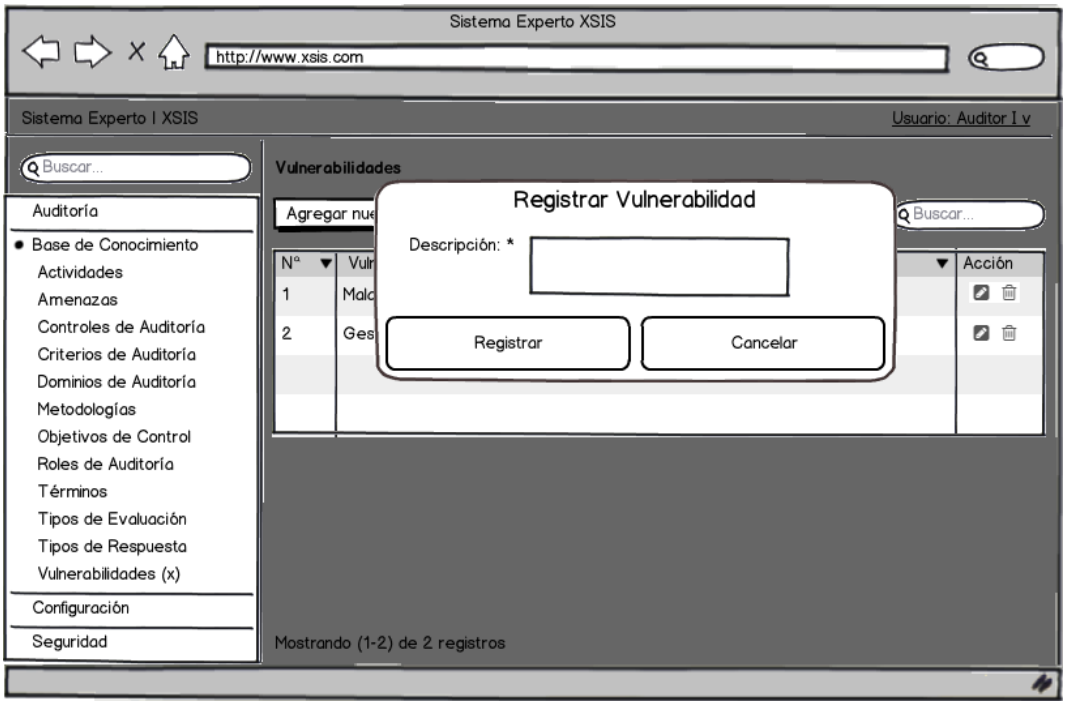


- **Listar tipos de evaluación**

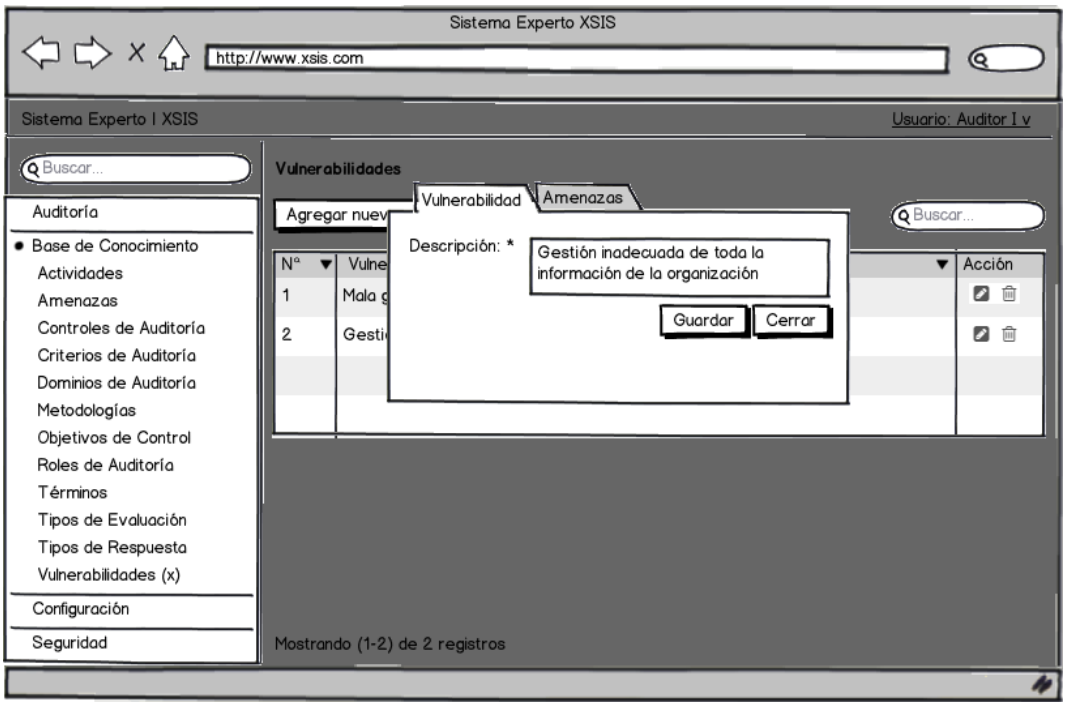


l. Vulnerabilidad

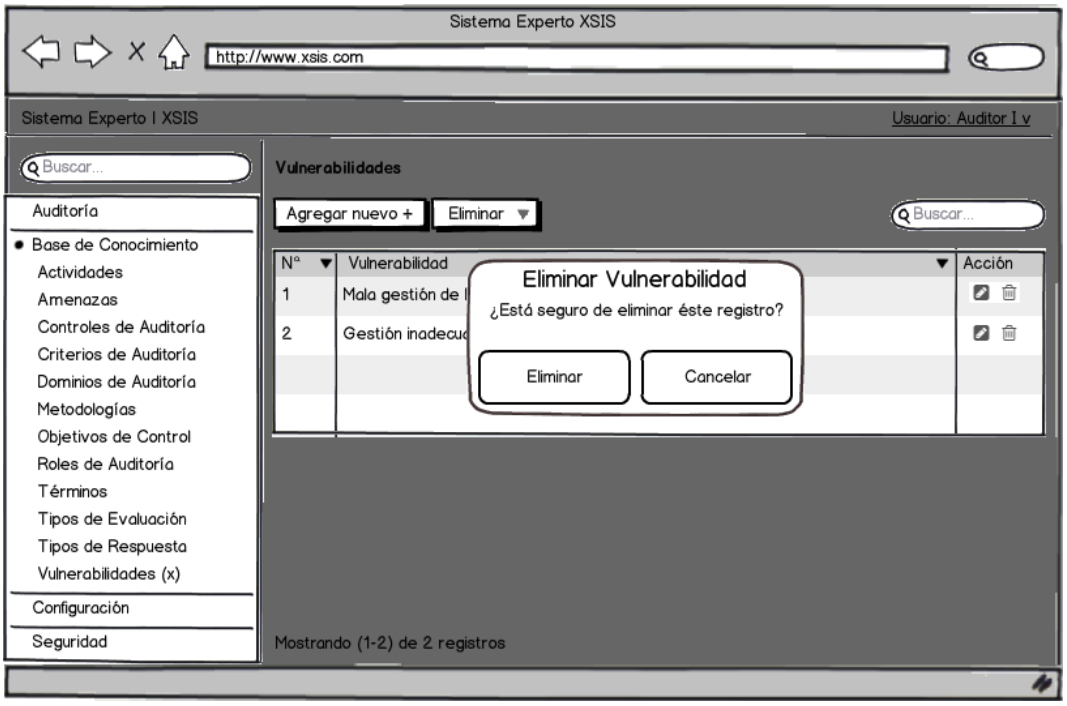
- **Registrar vulnerabilidad**



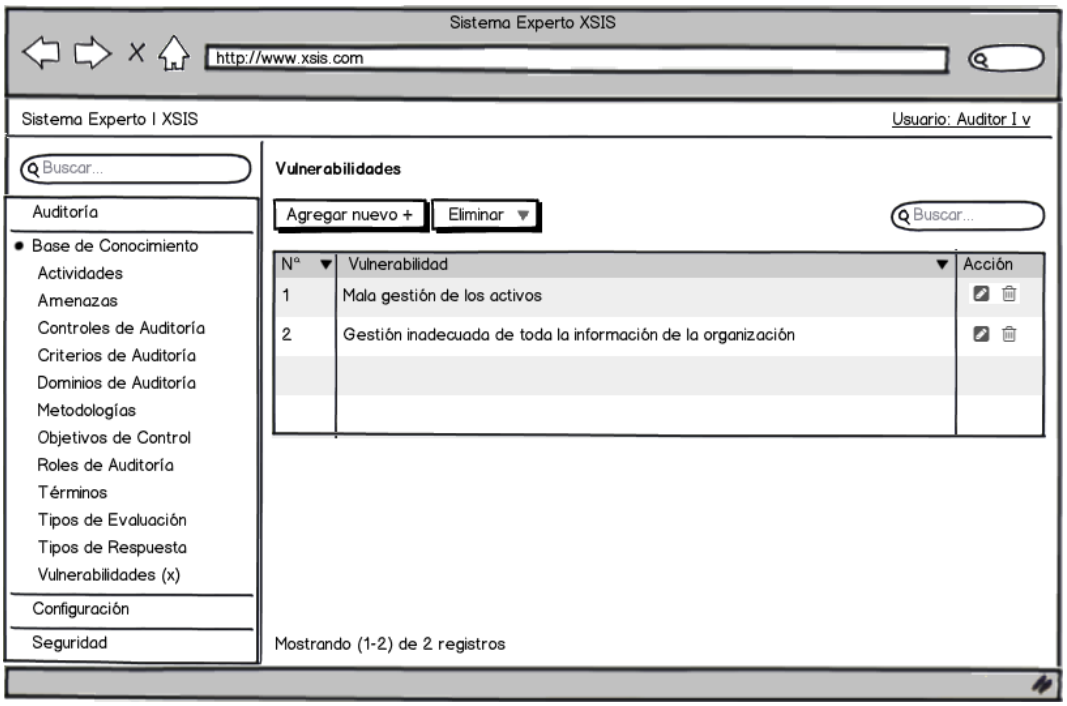
- **Modificar vulnerabilidad**



- **Eliminar vulnerabilidad**

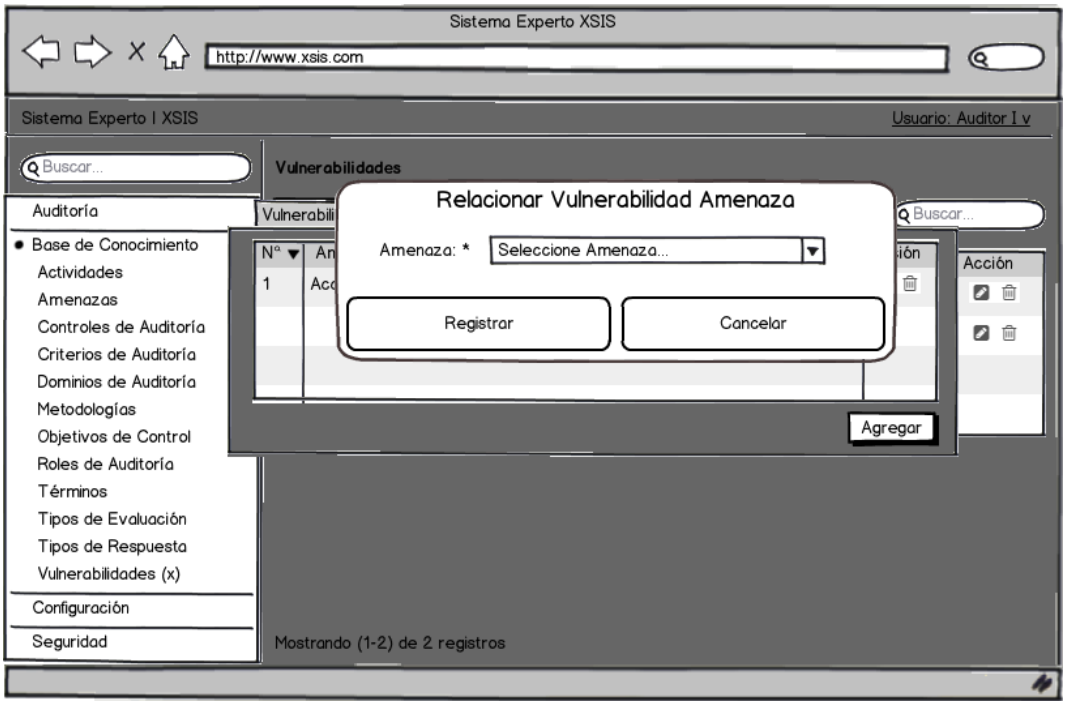


- **Listar vulnerabilidades**

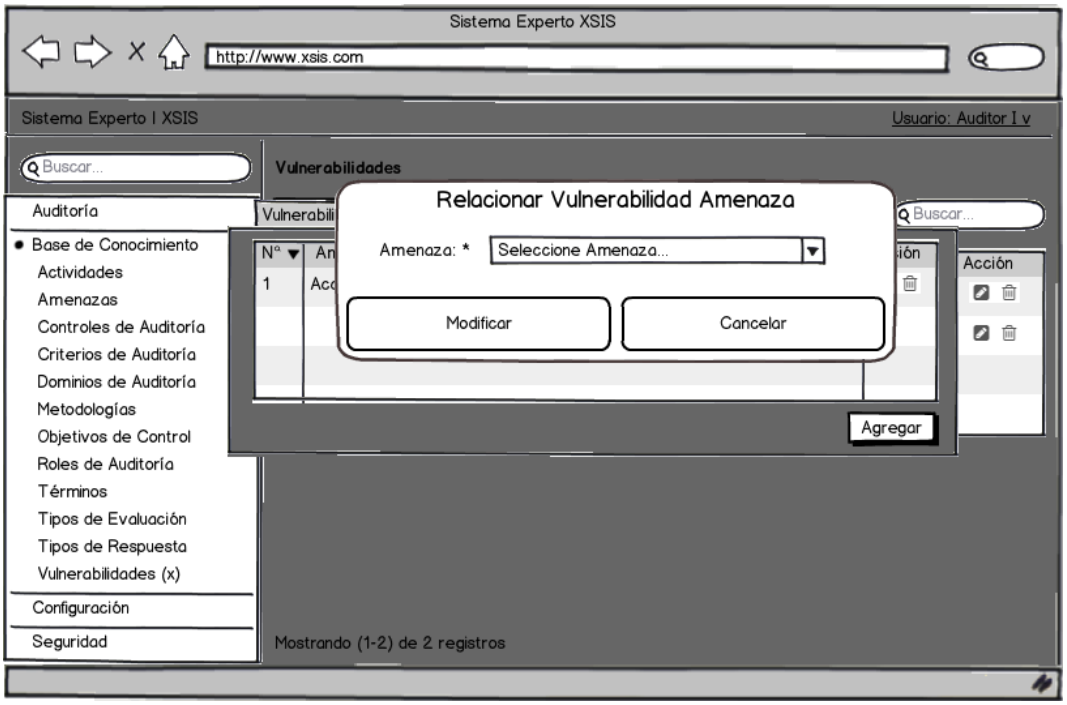


m. Vulnerabilidad - Amenaza

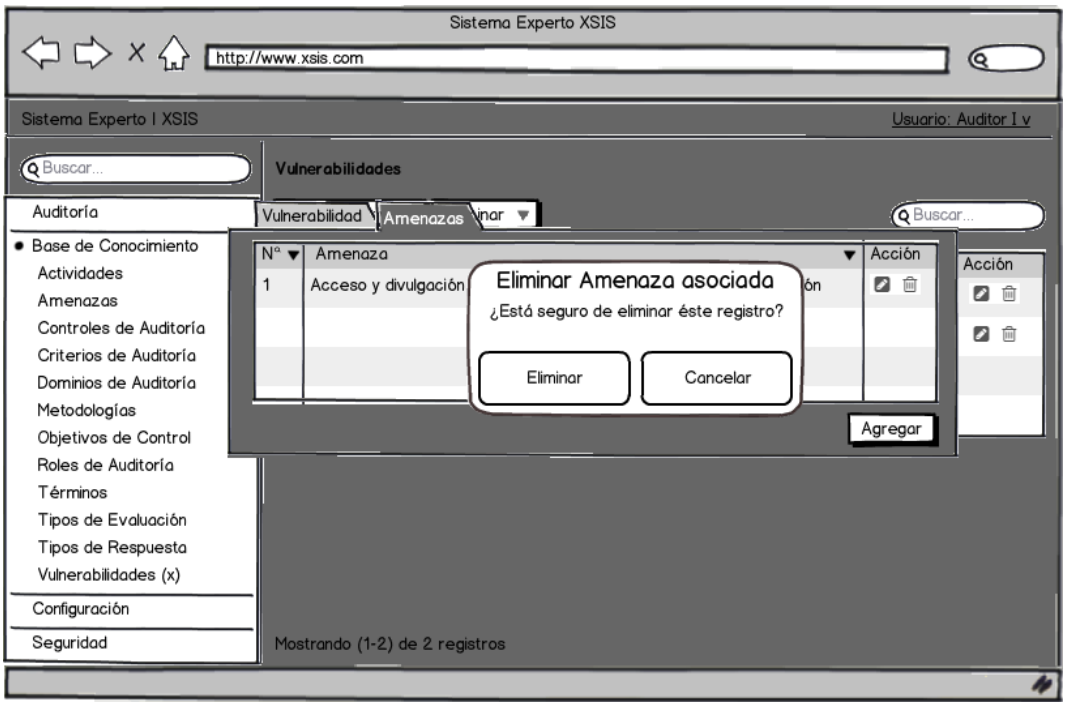
- **Asociar vulnerabilidad amenaza**



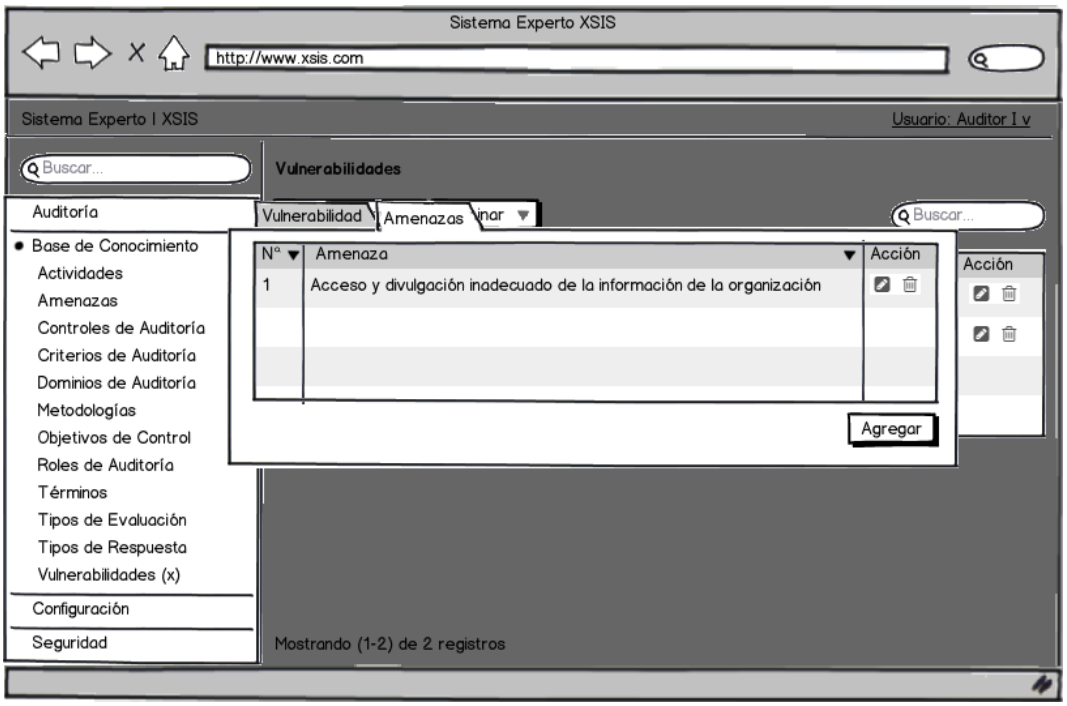
- **Modificar asociación vulnerabilidad – amenaza**



- **Eliminar asociación vulnerabilidad – amenaza**

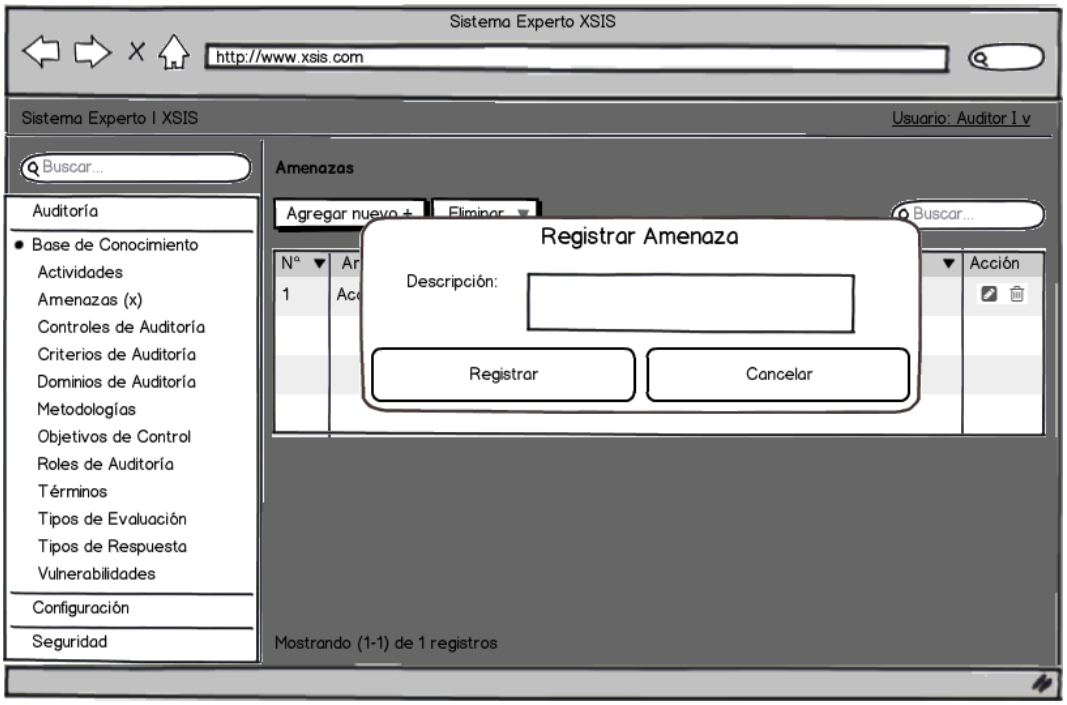


- **Listar vulnerabilidades – amenazas**

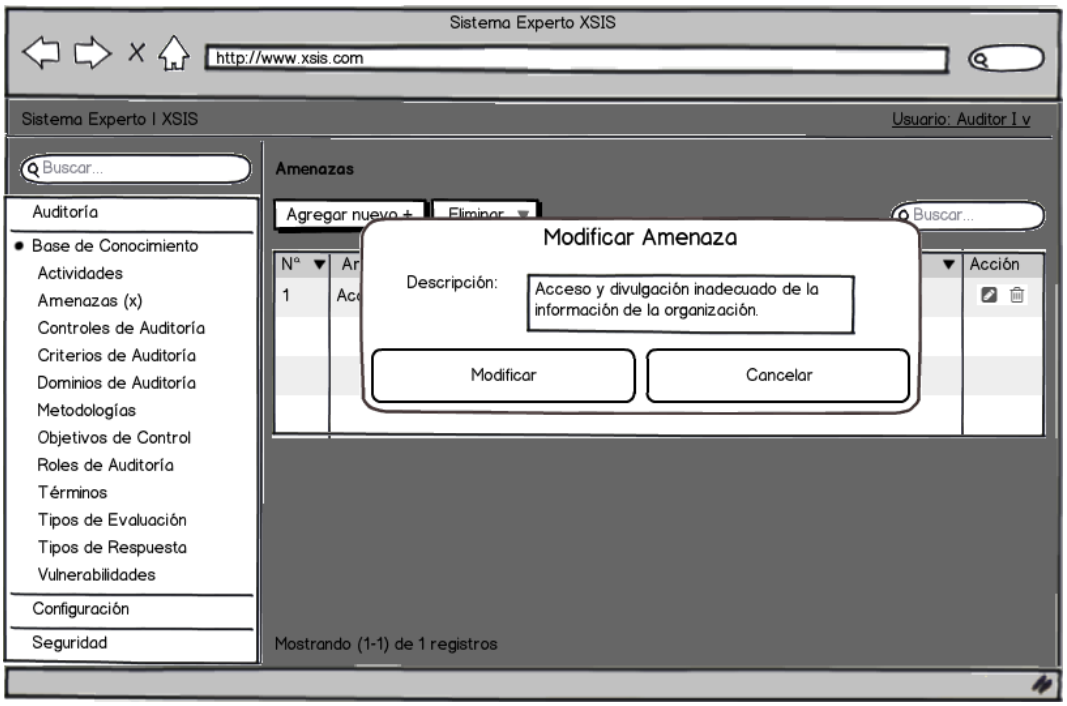


n. Amenazas

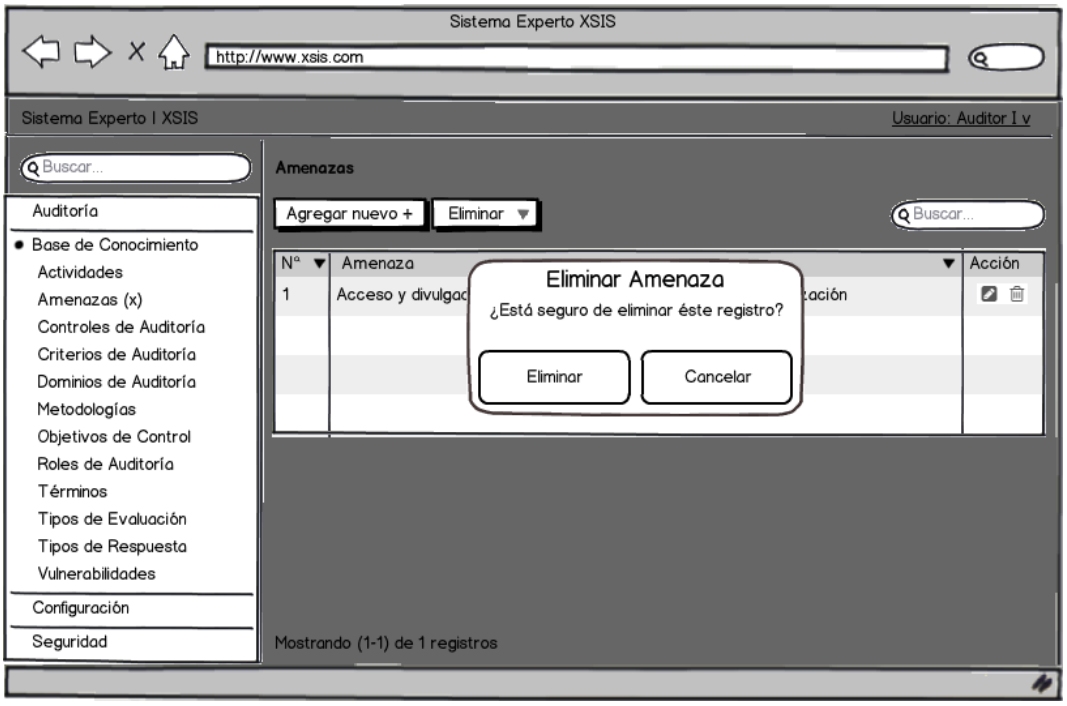
- **Registrar amenaza**



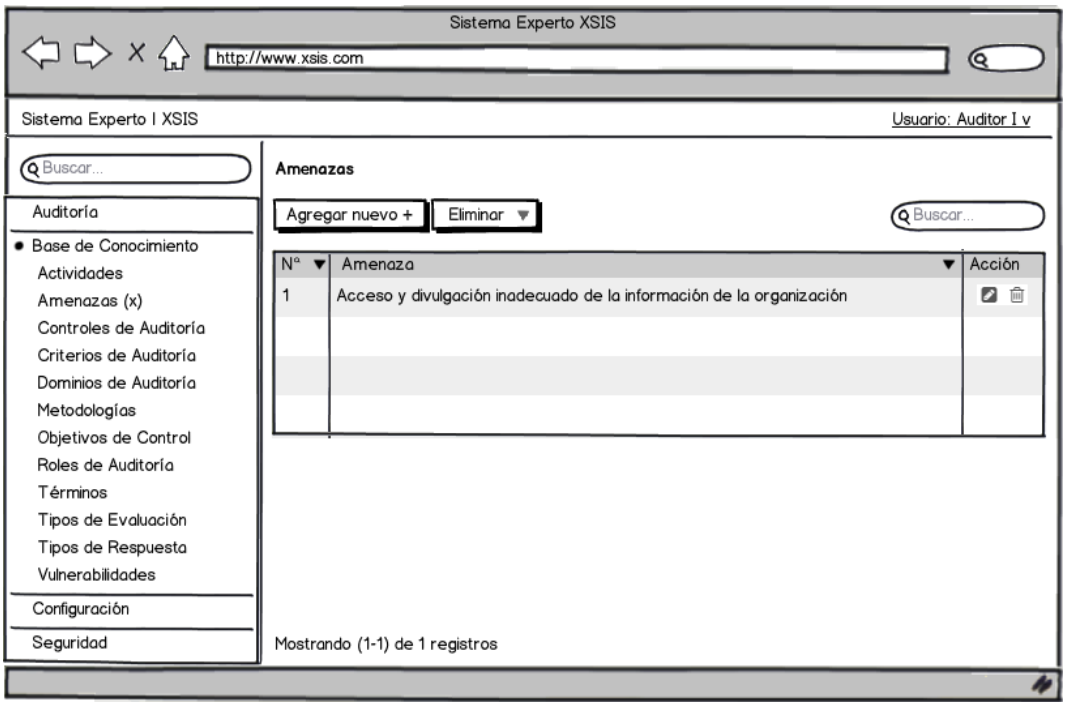
- **Modificar amenaza**



- **Eliminar amenaza**

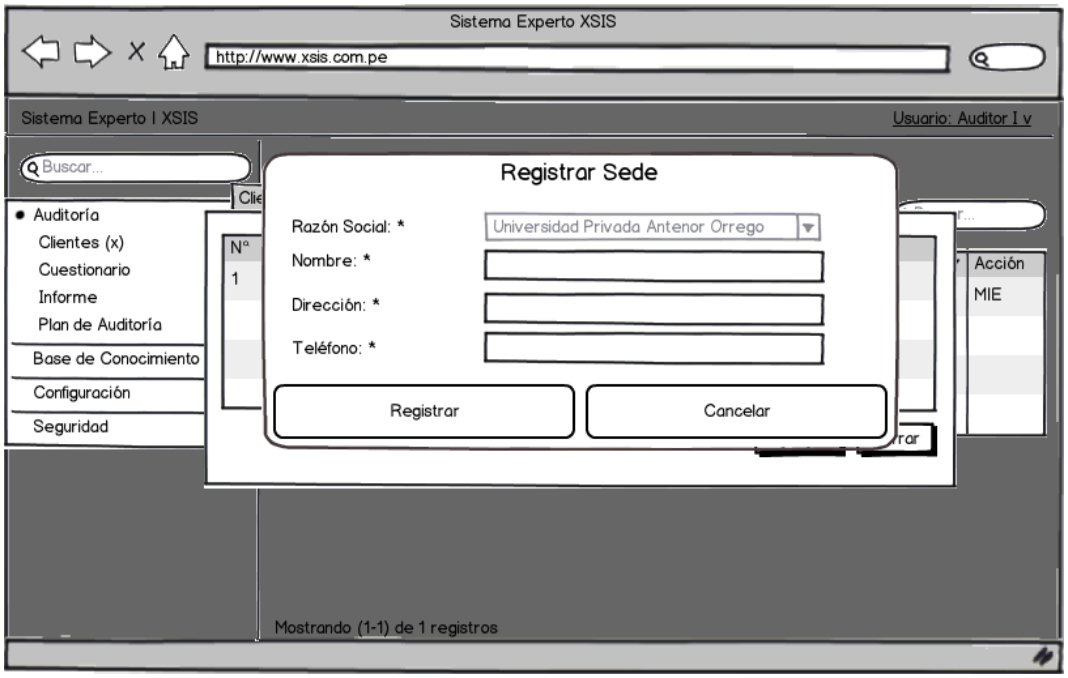


- **Listar amenazas**

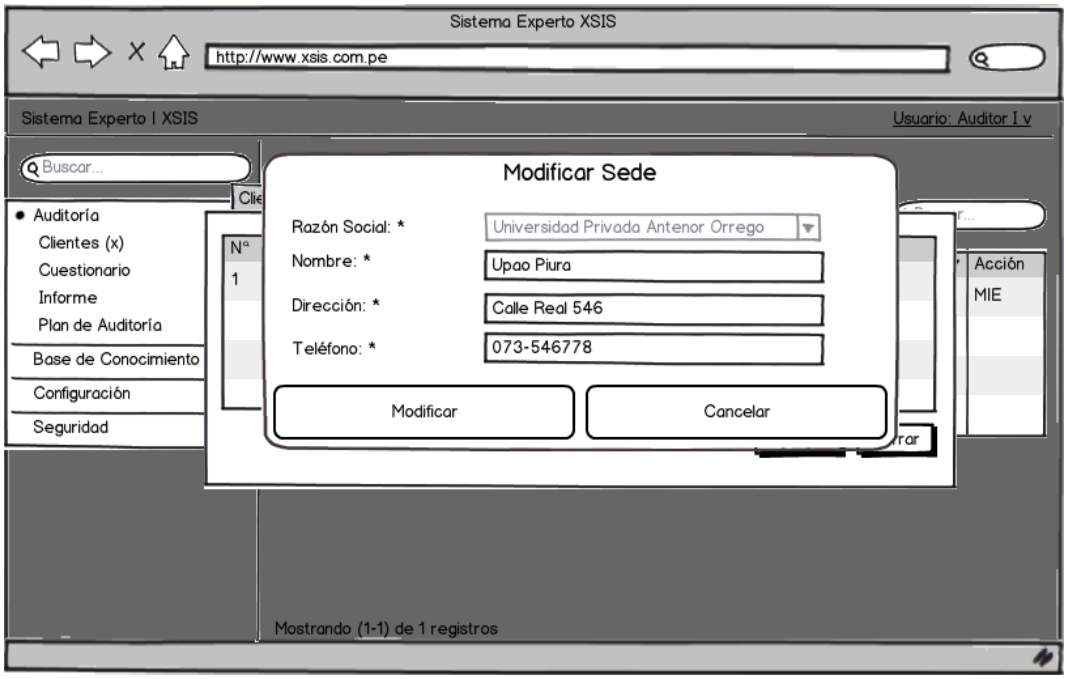


Módulo Auditoría

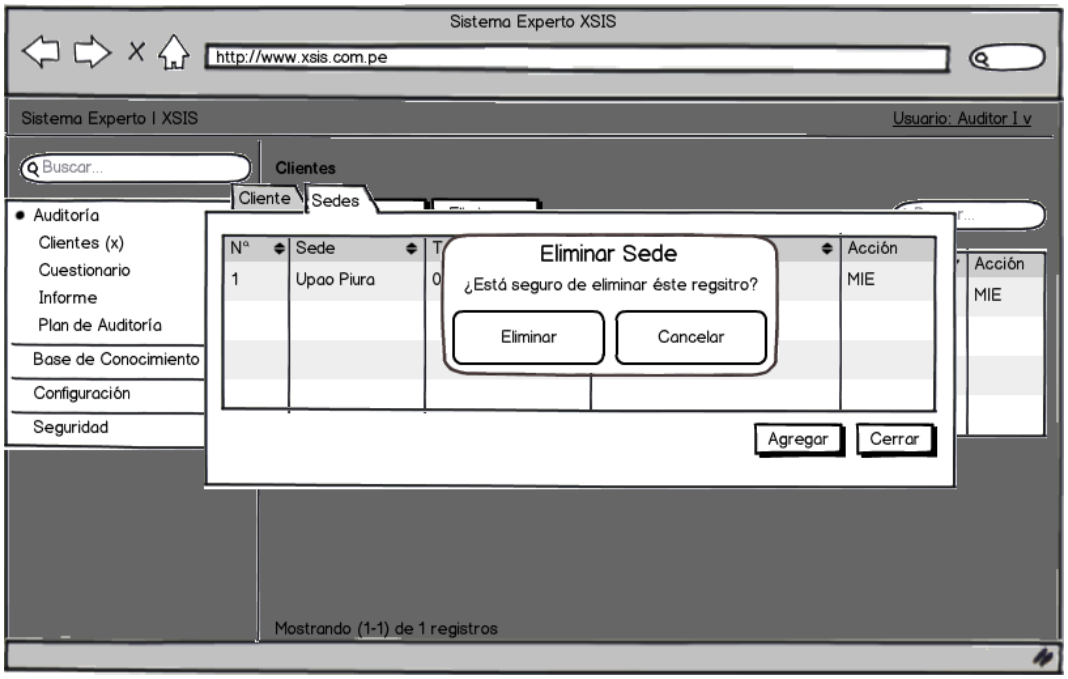
- **Registrar sedes**



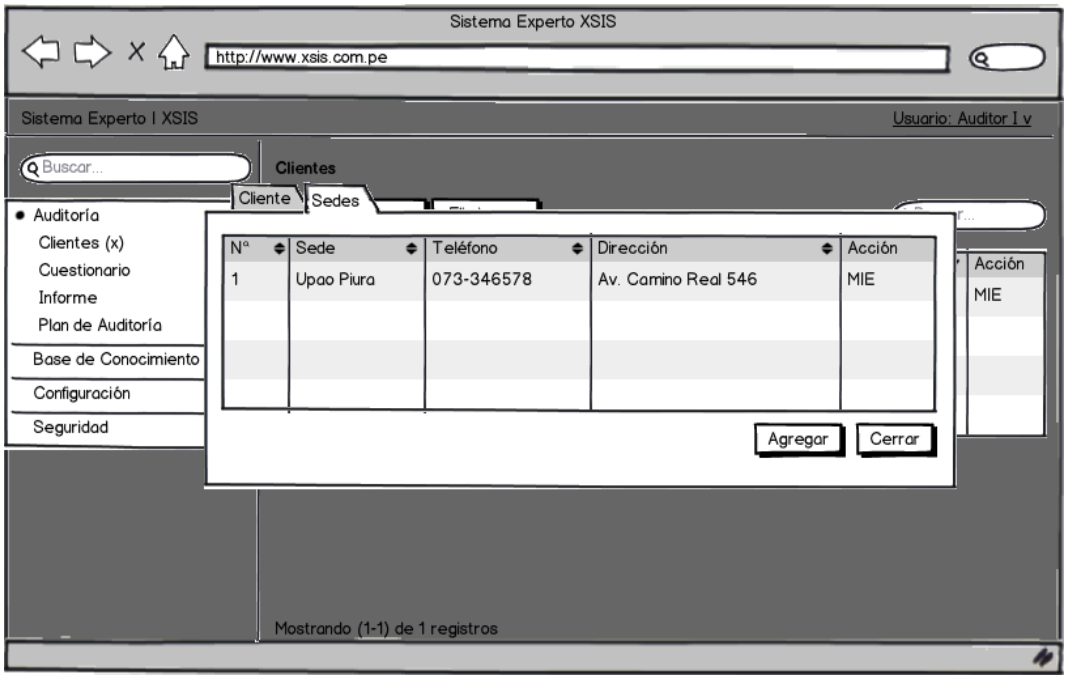
- **Modificar sede**



- **Eliminar sede**

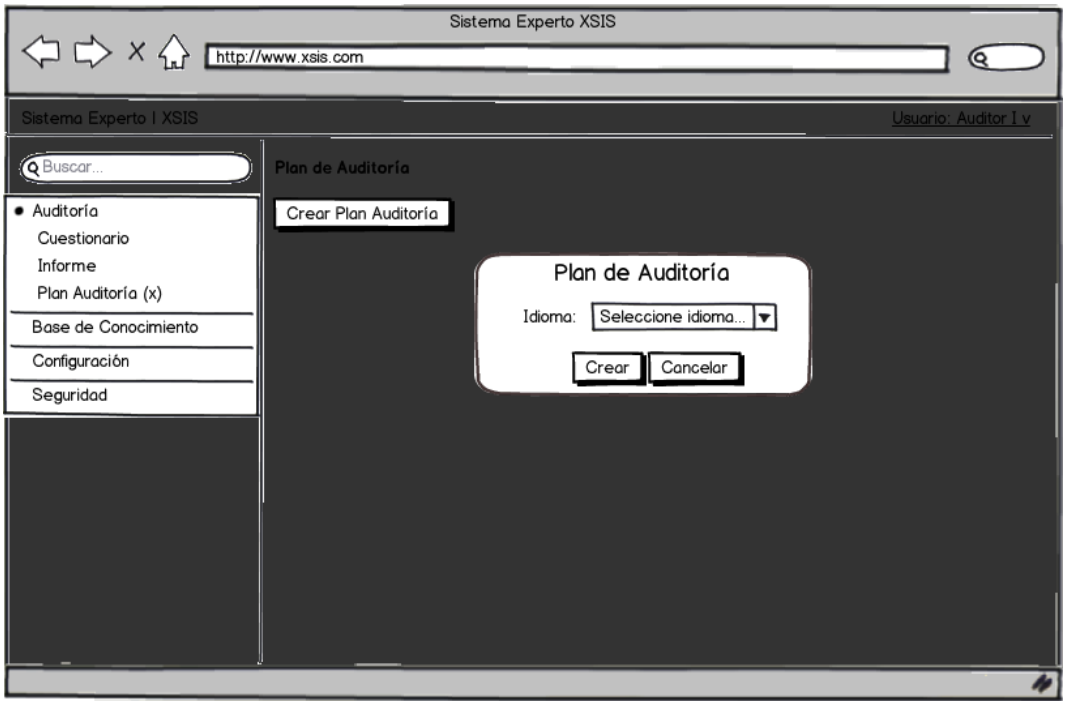


- **Listar sedes**

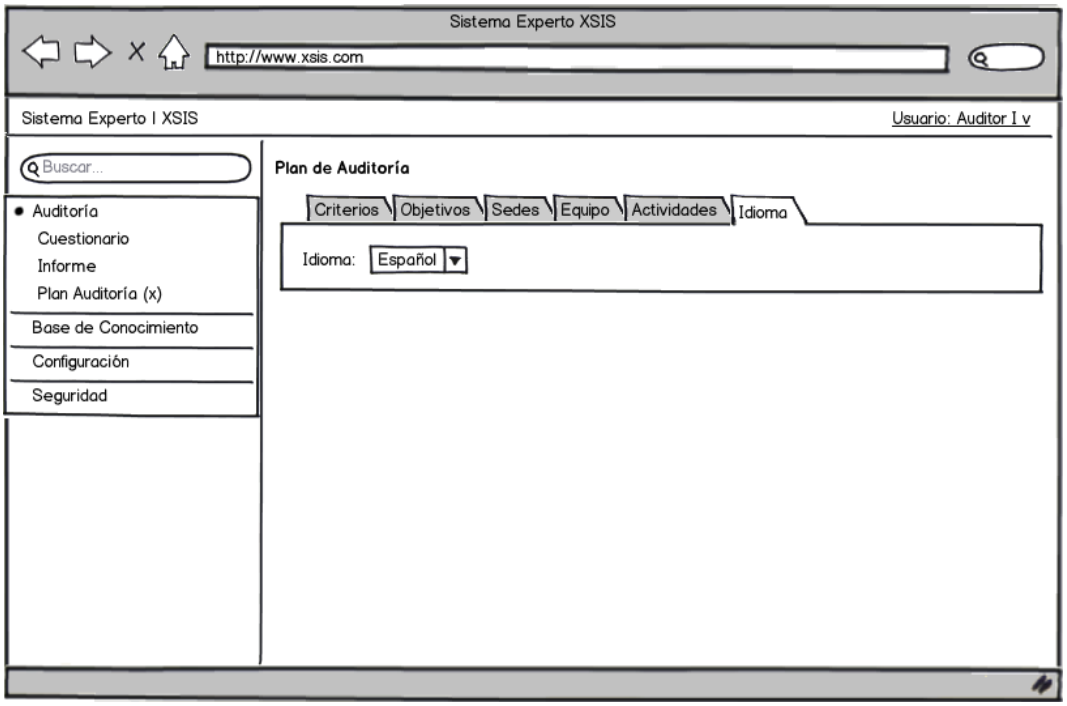


a. Plan auditoría

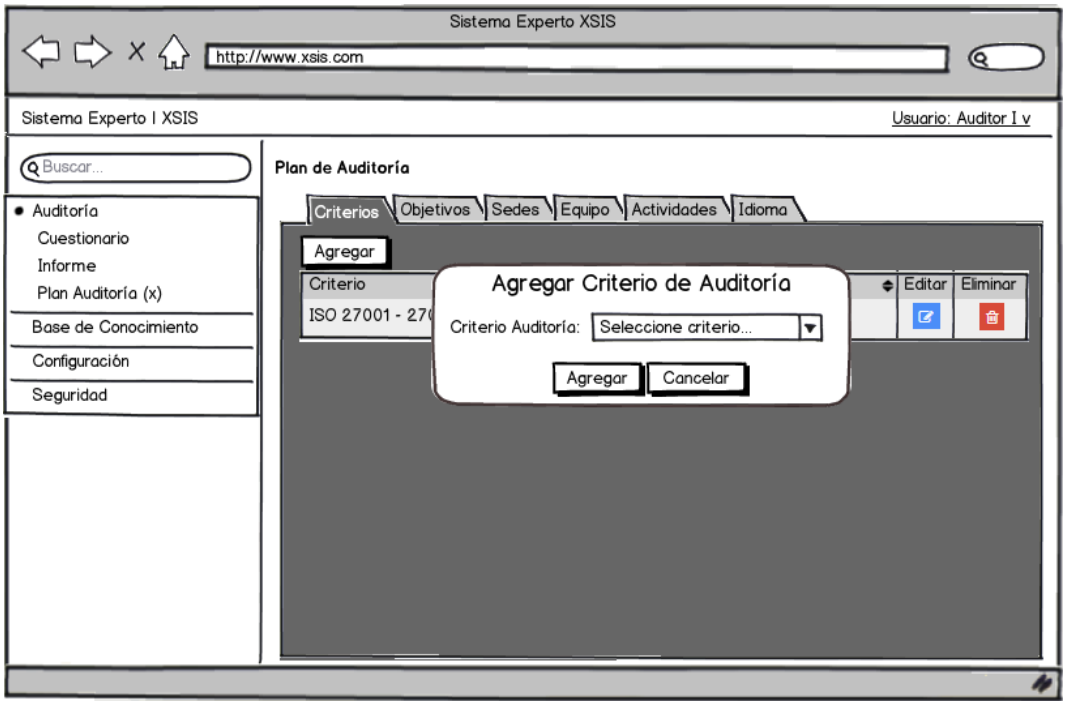
- **Crear plan auditoría**



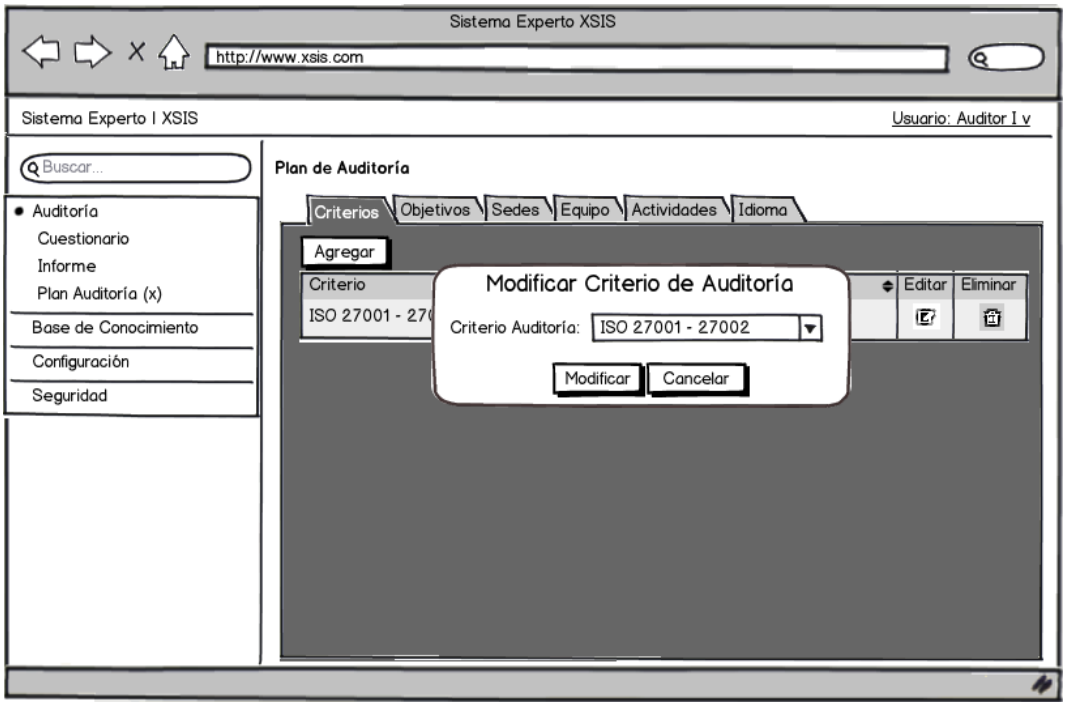
- **Modificar idioma plan auditoría**



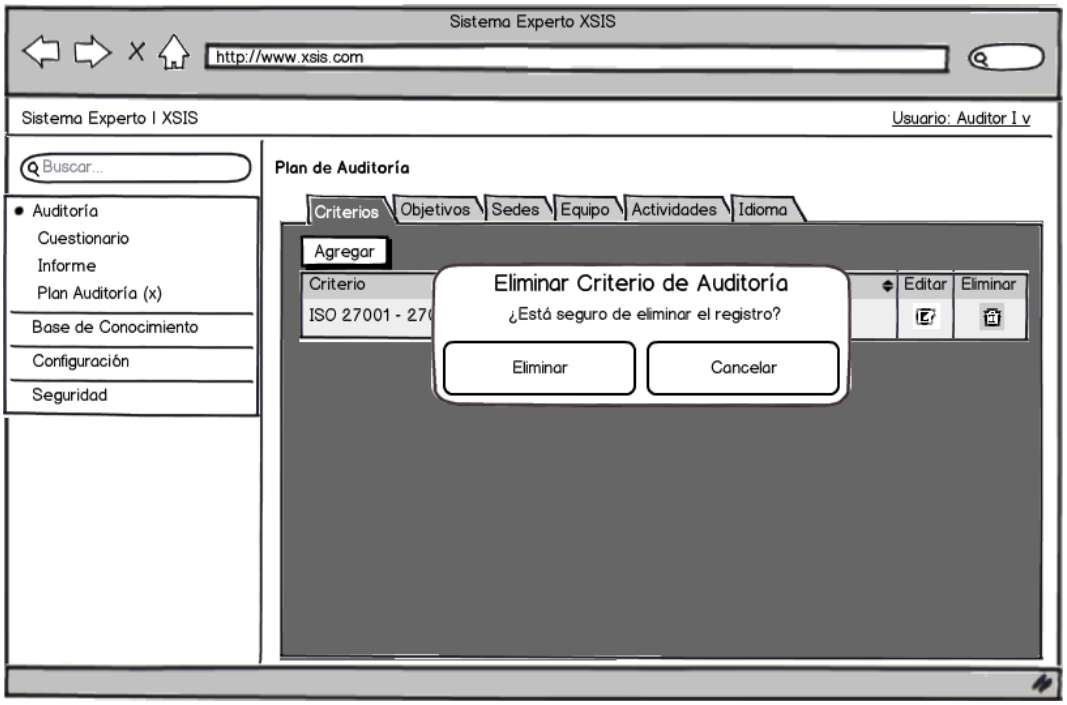
- **Registrar criterio - plan auditoría**



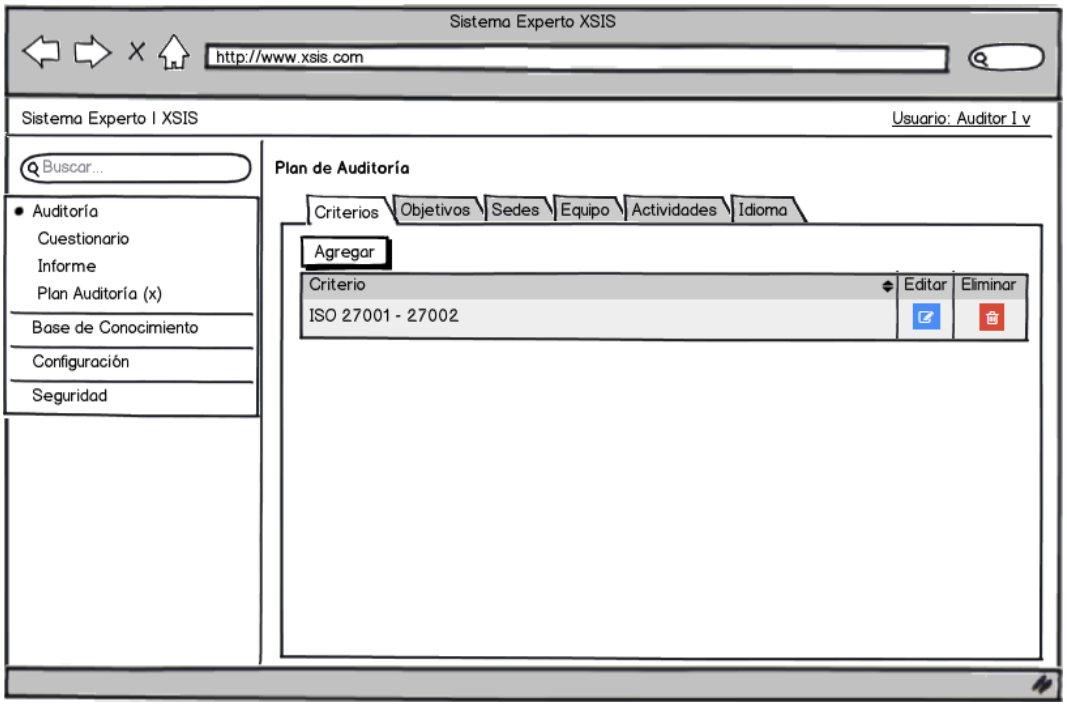
- **Modificar criterio – plan auditoría**



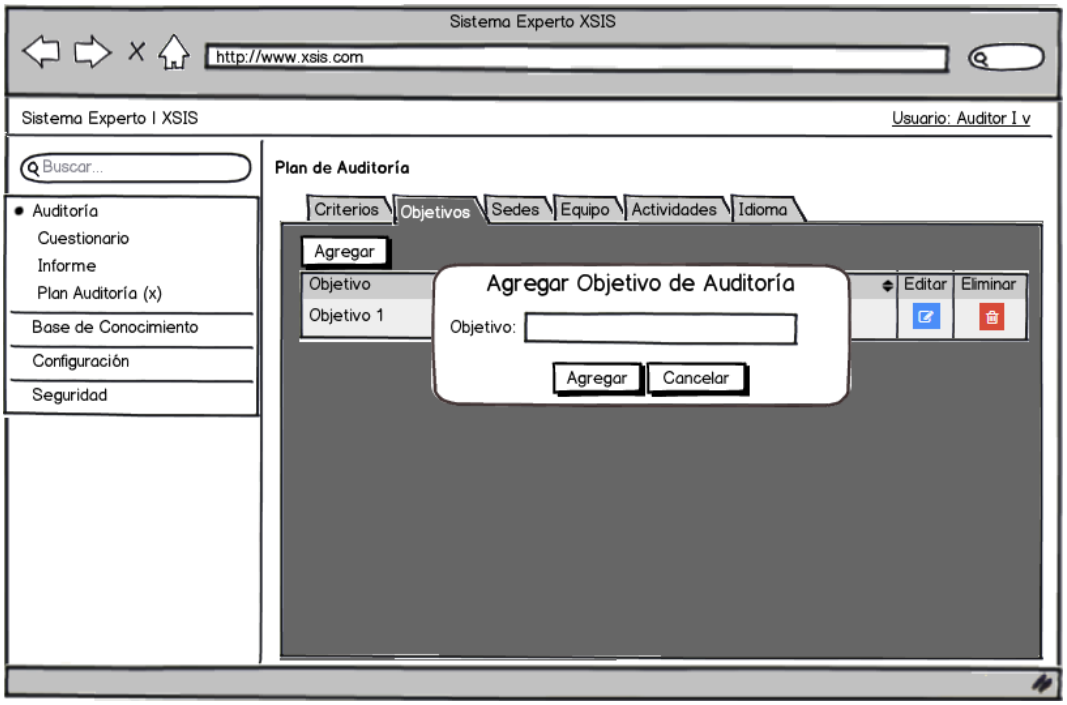
- **Eliminar criterio – plan auditoría**



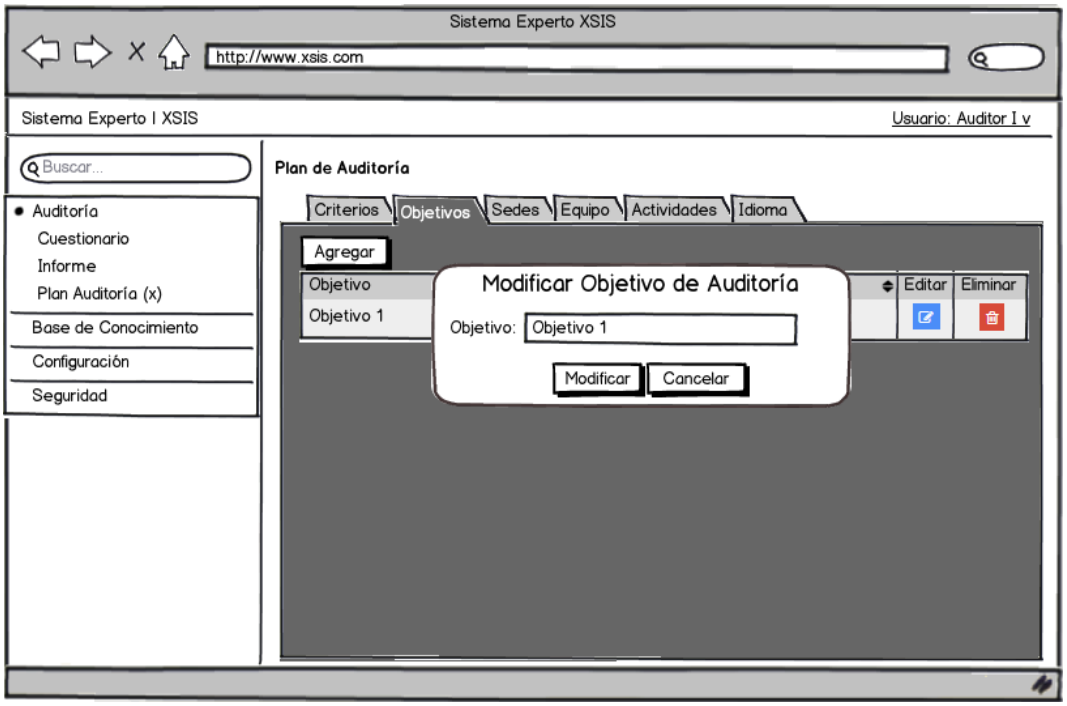
- **Listar criterios – plan auditoría**



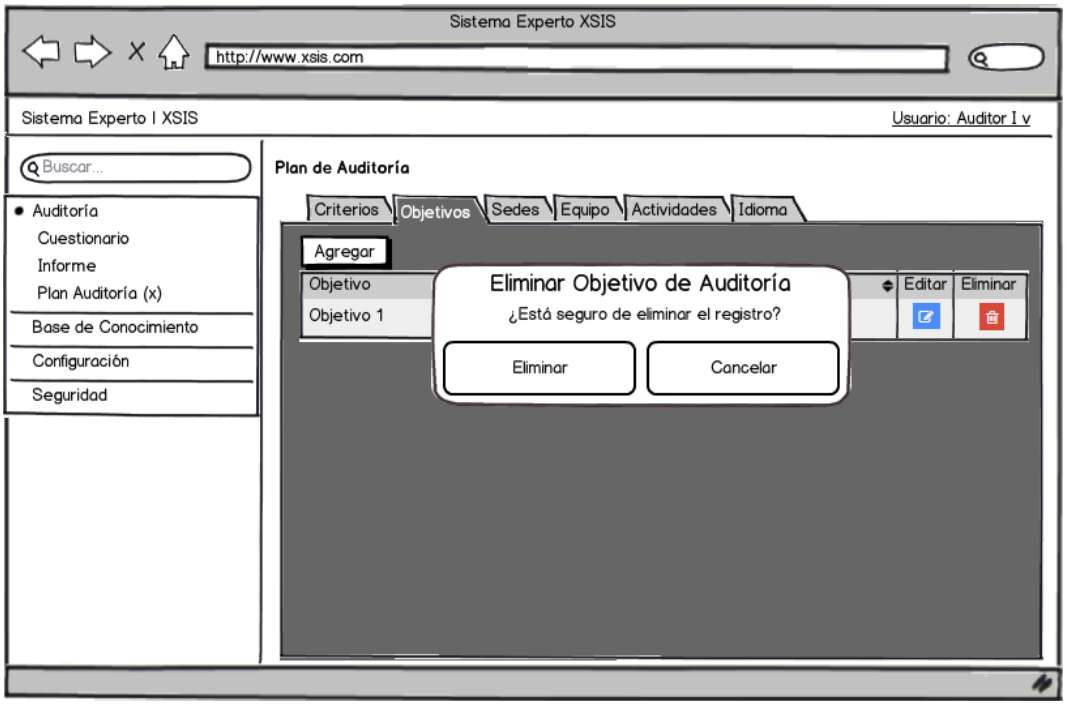
- **Registrar objetivo del plan auditoría**



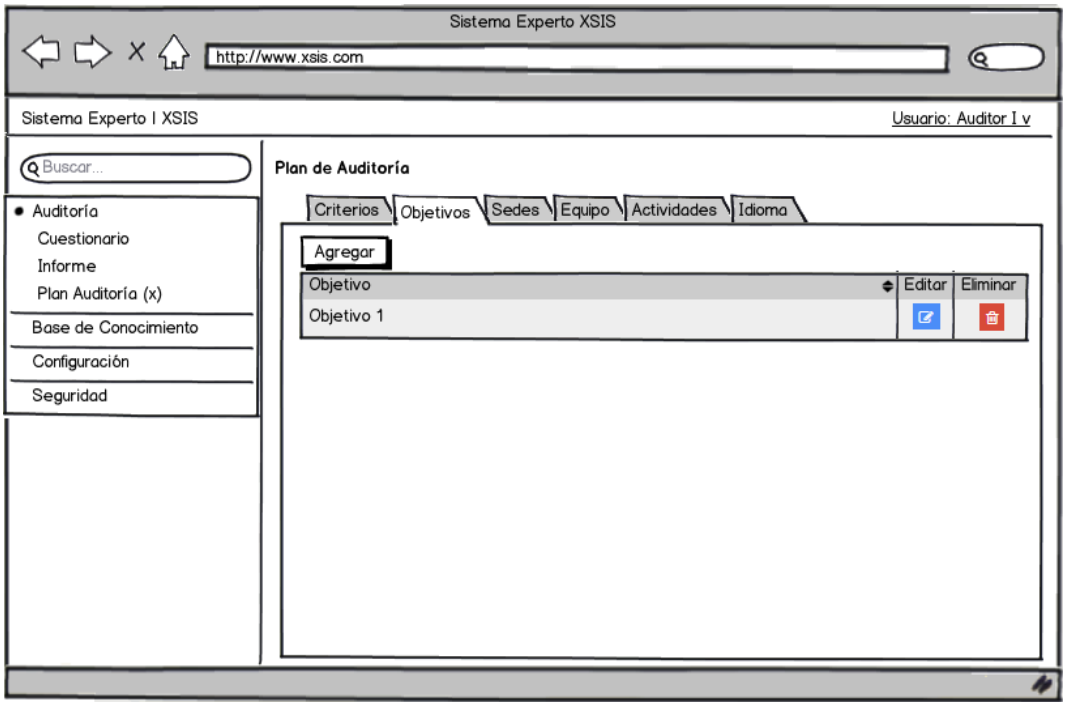
- **Modificar objetivo del plan auditoría**



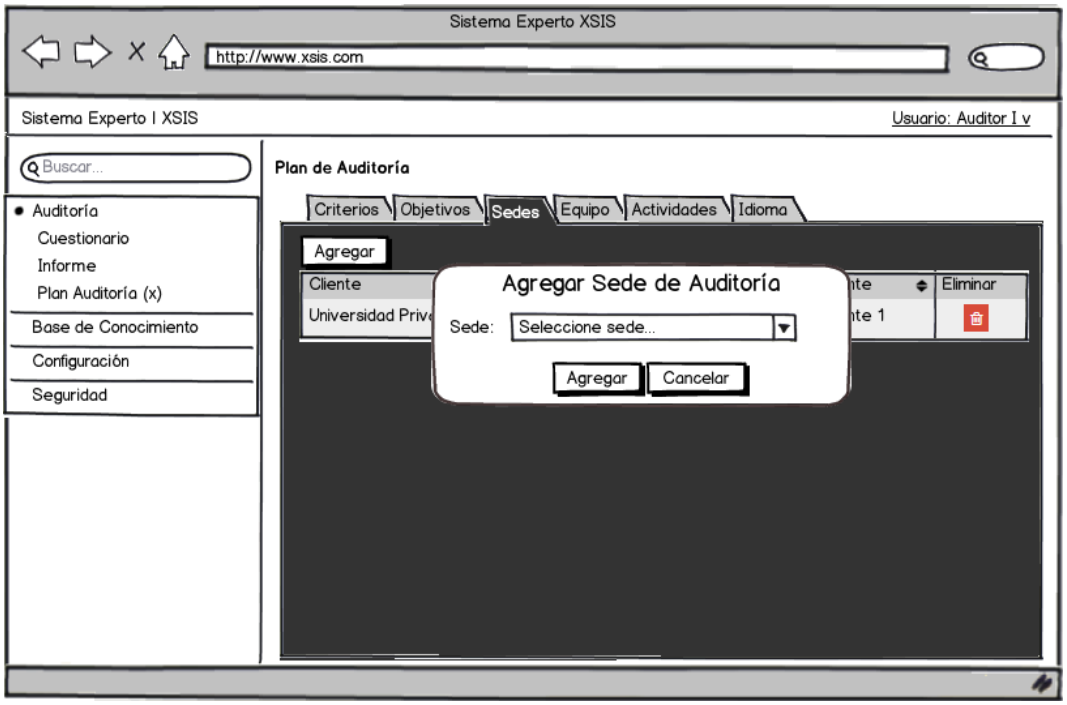
- **Eliminar objetivo del plan de auditoría**



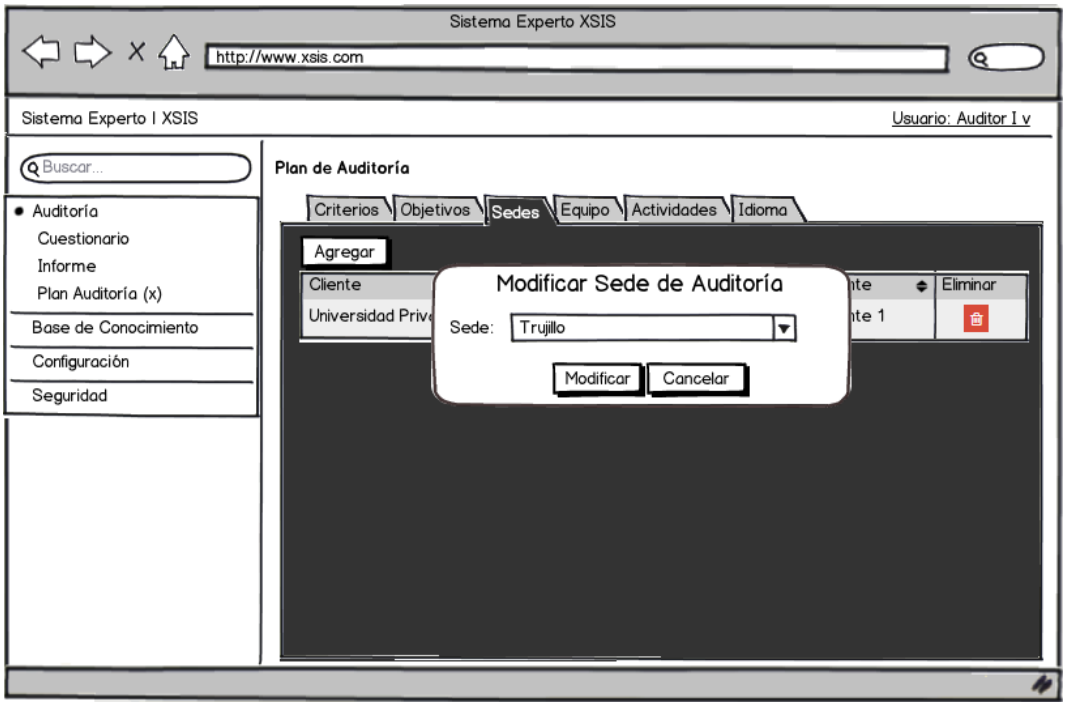
- **Listar objetivos del plan de auditoría**



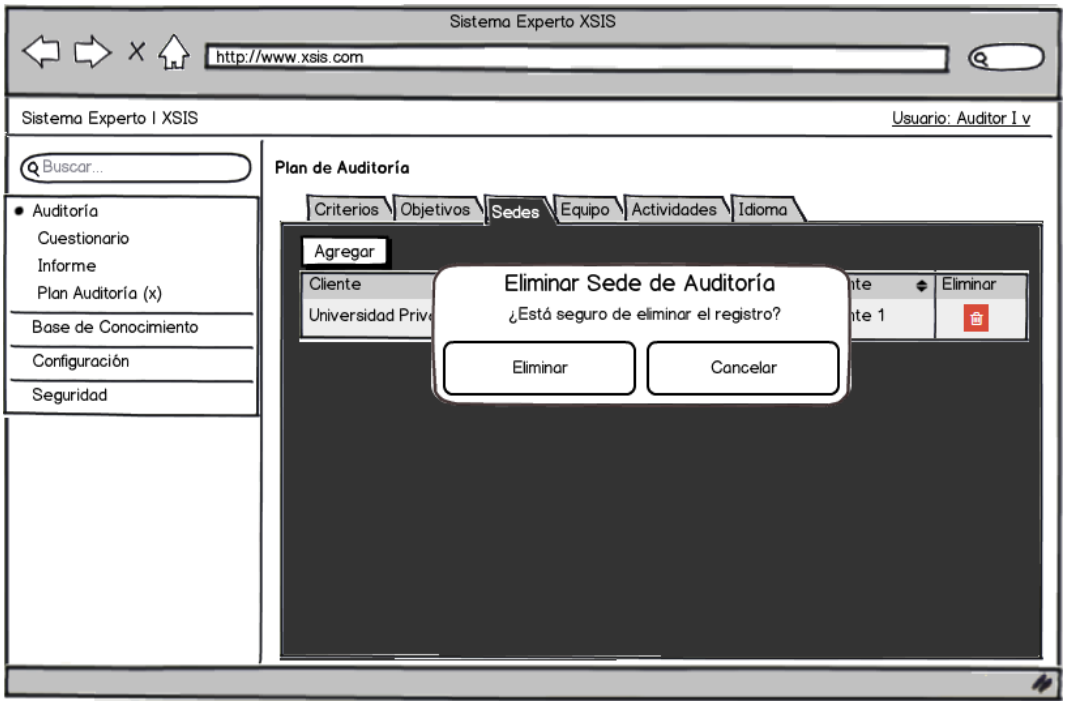
- **Registrar sede – plan auditoría**



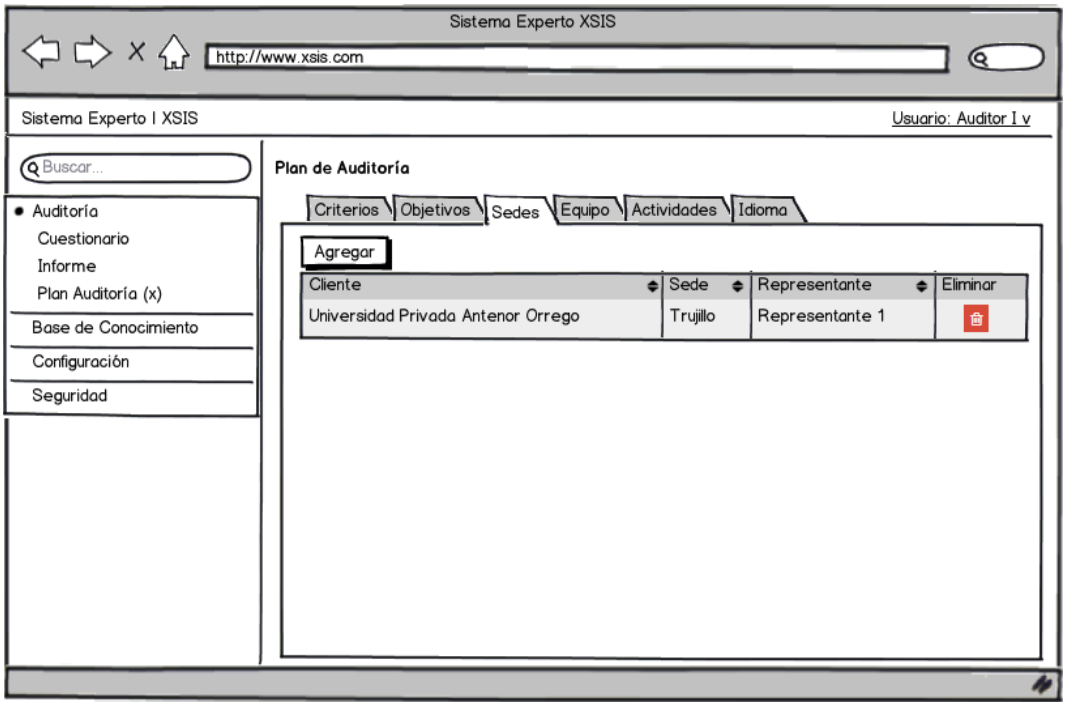
- **Modificar sede – plan auditoría**



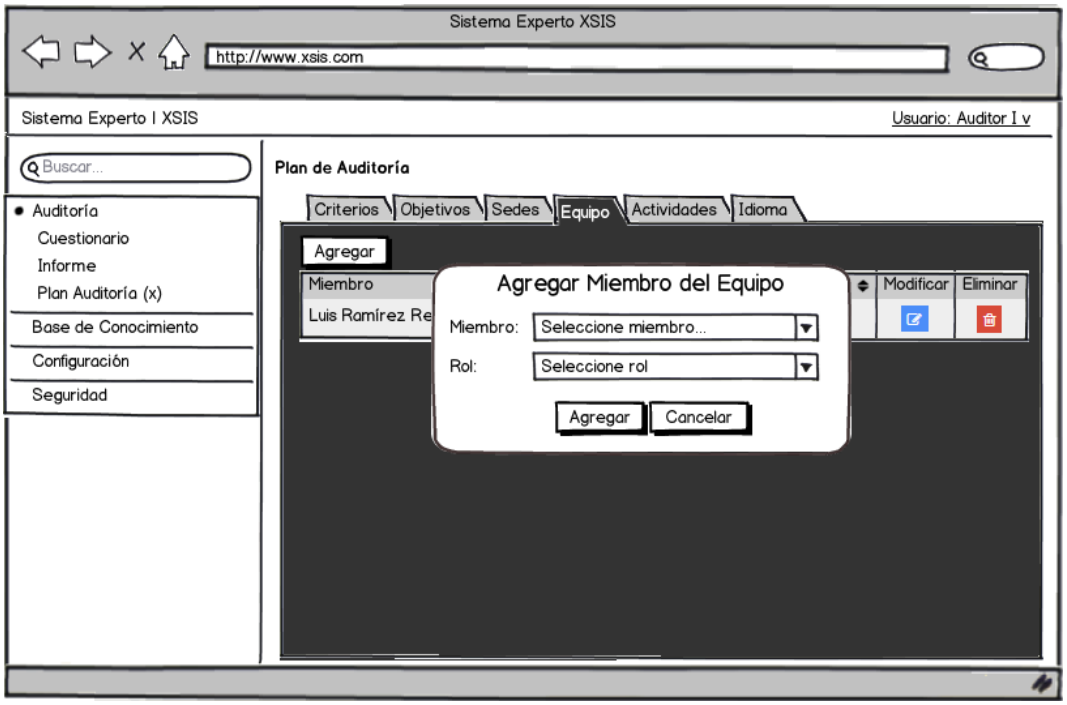
- **Eliminar sede – plan auditoría**



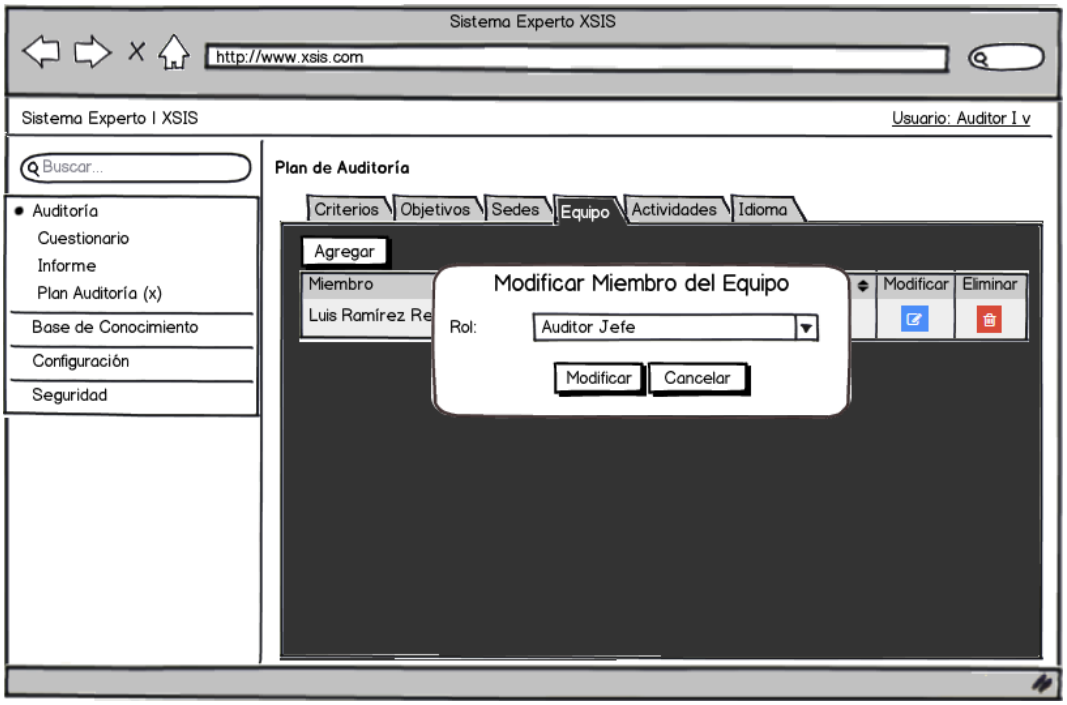
- **Listar sedes- plan auditoría**



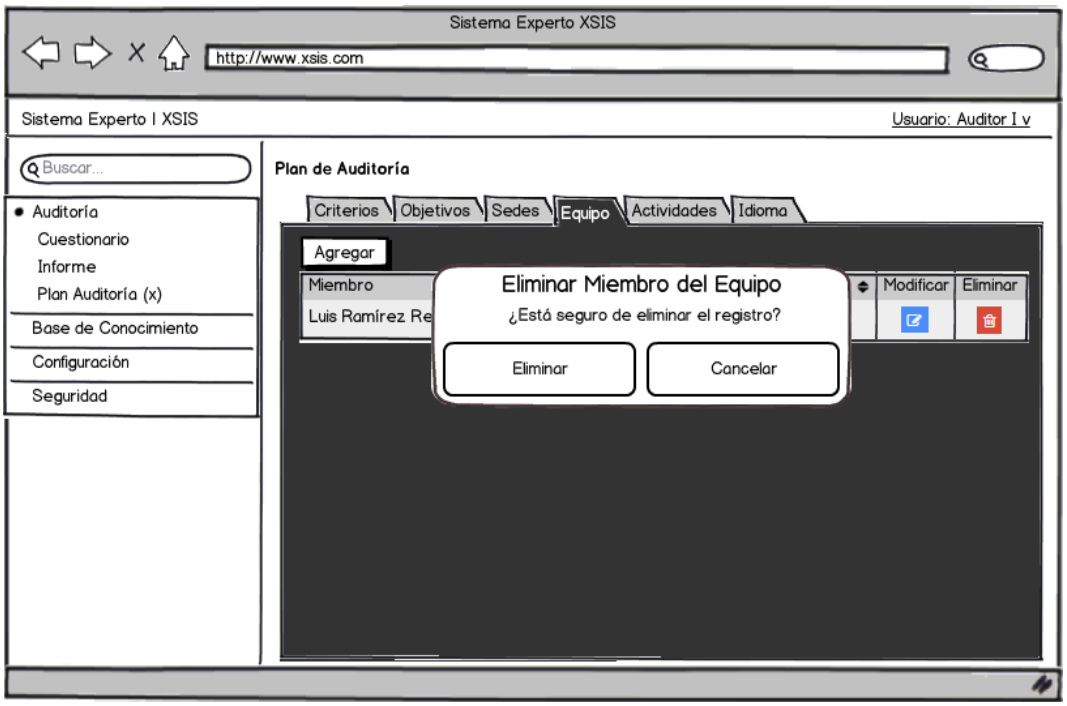
- **Registrar miembro equipo – plan auditoría**



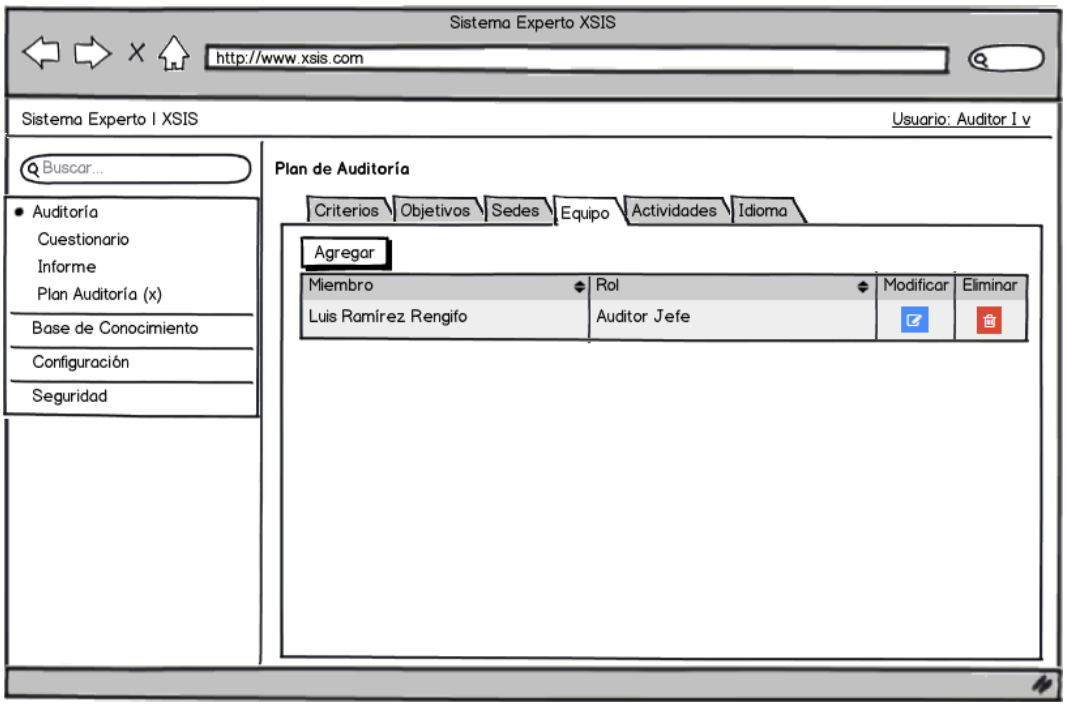
- **Modificar miembro equipo – plan auditoría**



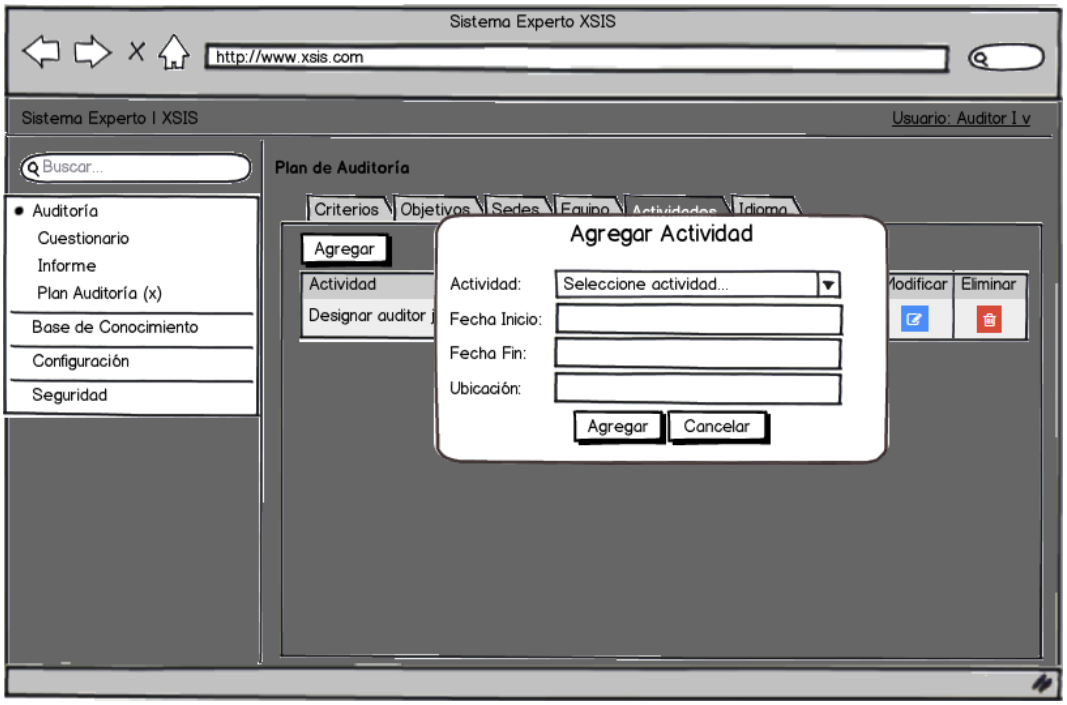
- **Eliminar miembro equipo – plan auditoría**



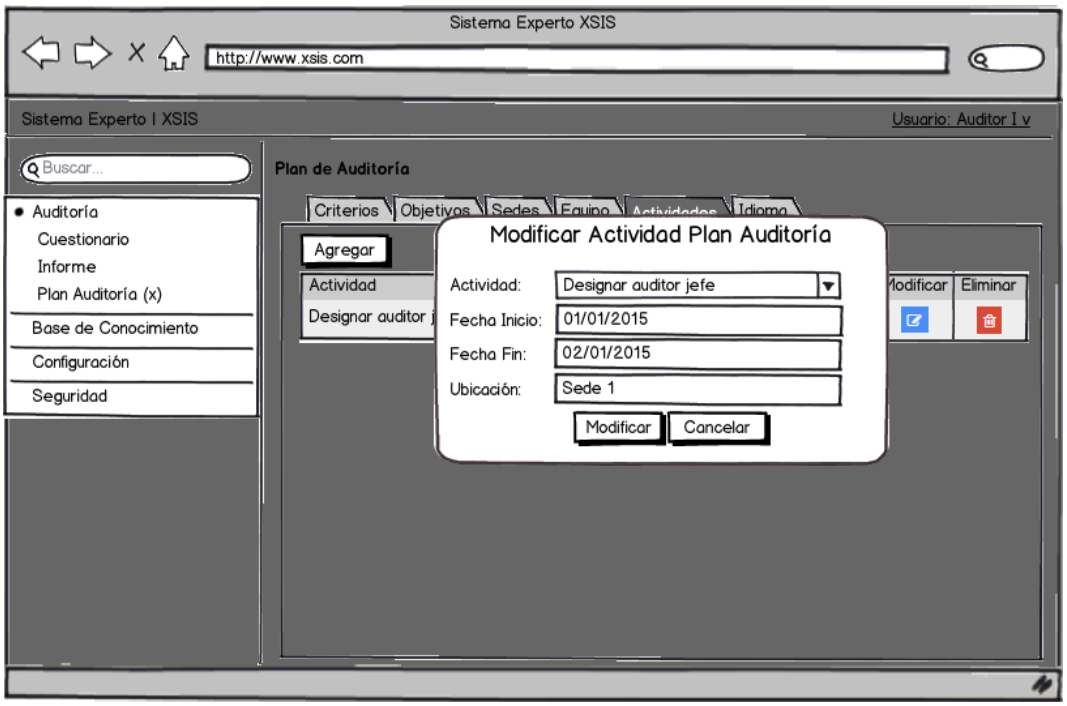
- **Listar equipo – plan auditoría**



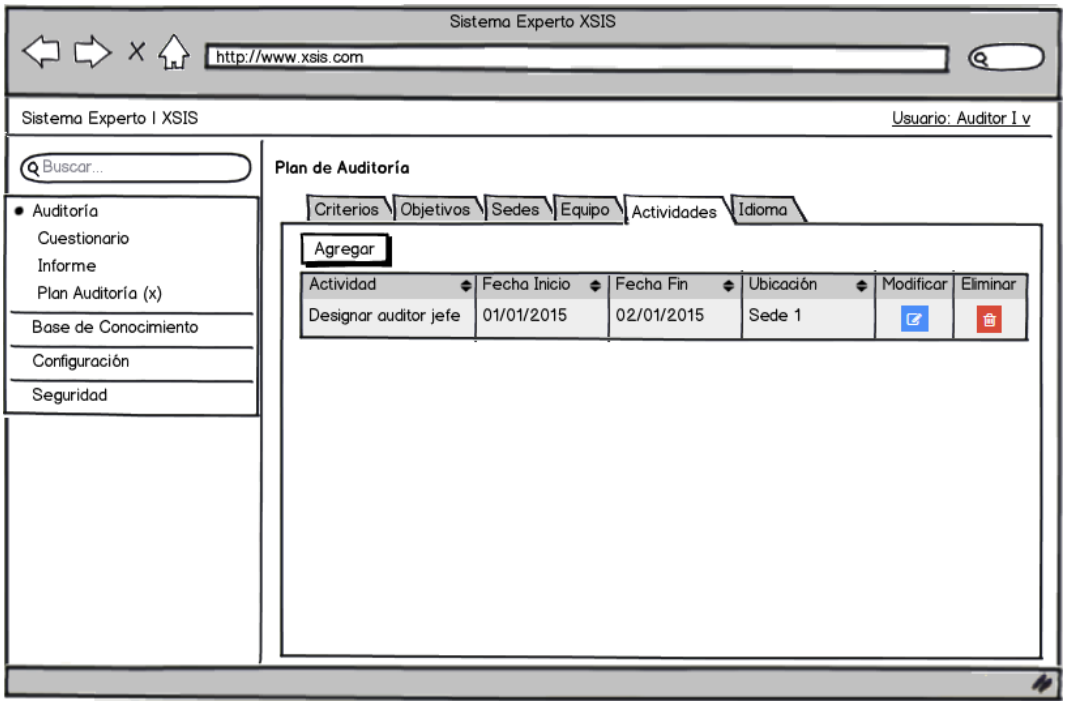
- **Registrar actividad – plan auditoría**



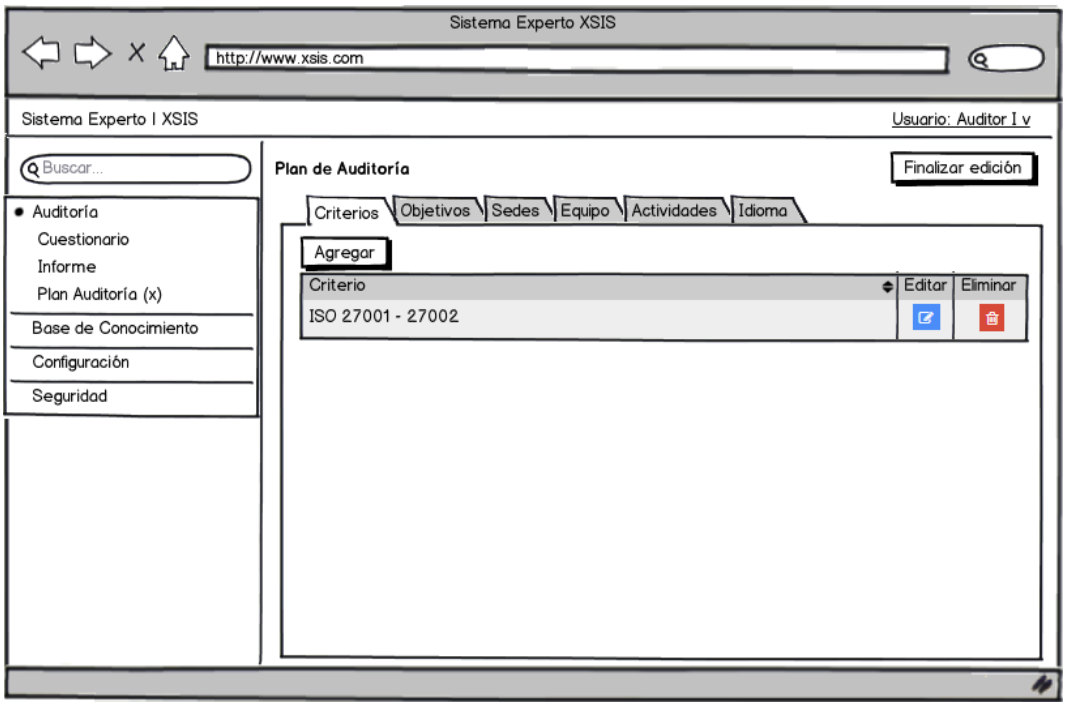
- **Modificar actividad – plan auditoría**



- **Listar actividades – plan auditoría**

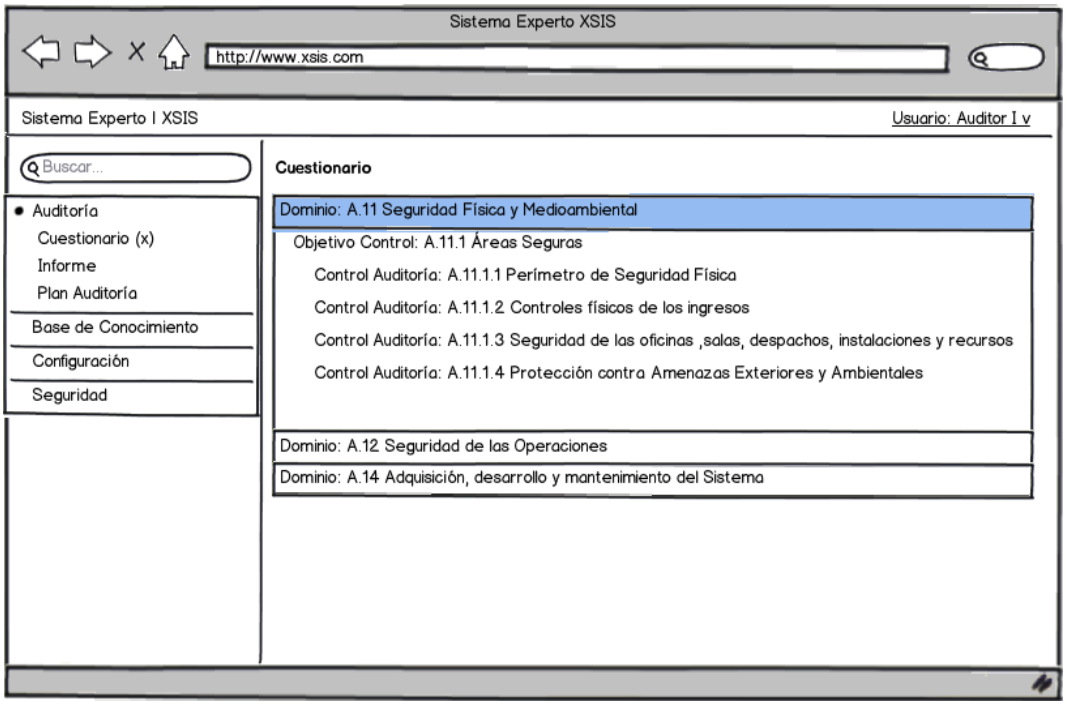


- **Finalizar plan auditoría**

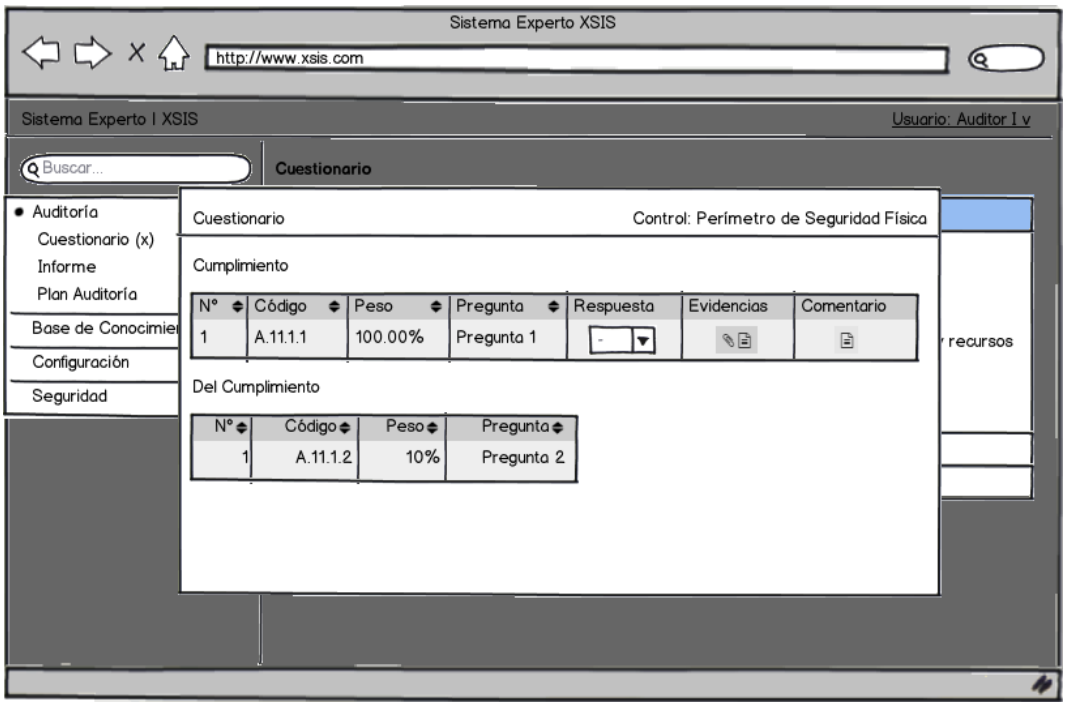


b. Cuestionario

- **Listar controles cuestionario**



- **Completar cuestionario auditoría**



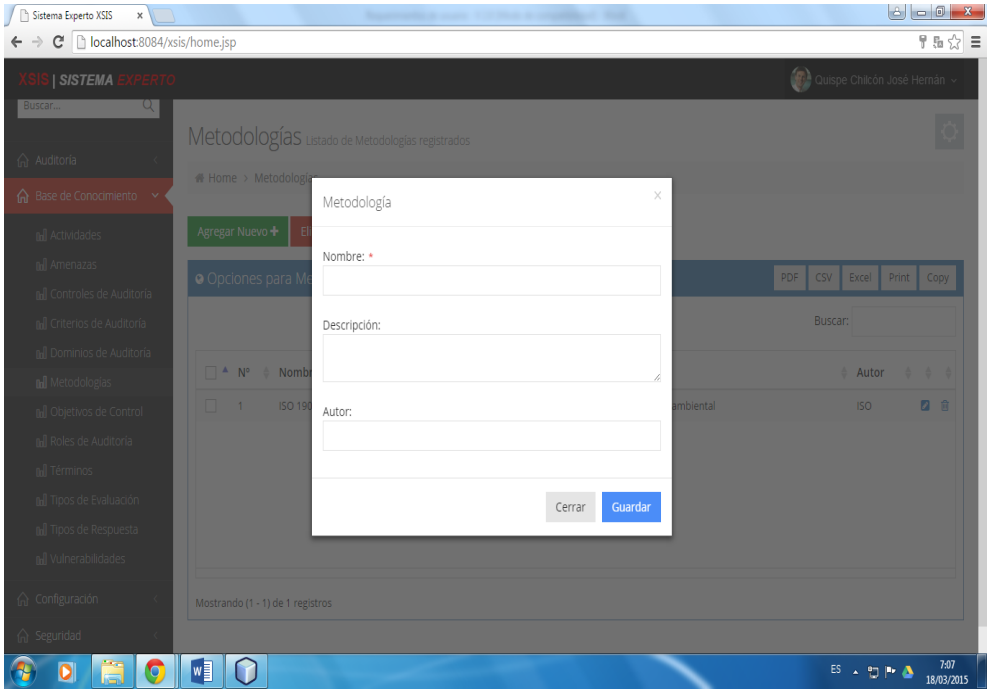
4.4 Implementación

4.4.1 Interfaces del Sistema

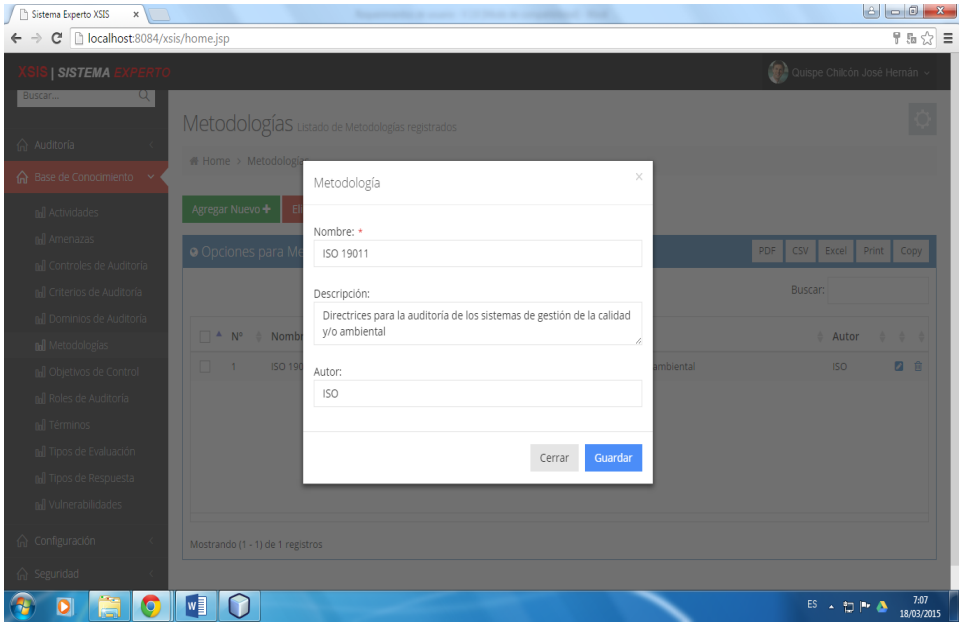
Módulo de Base de Conocimiento

a. Metodología

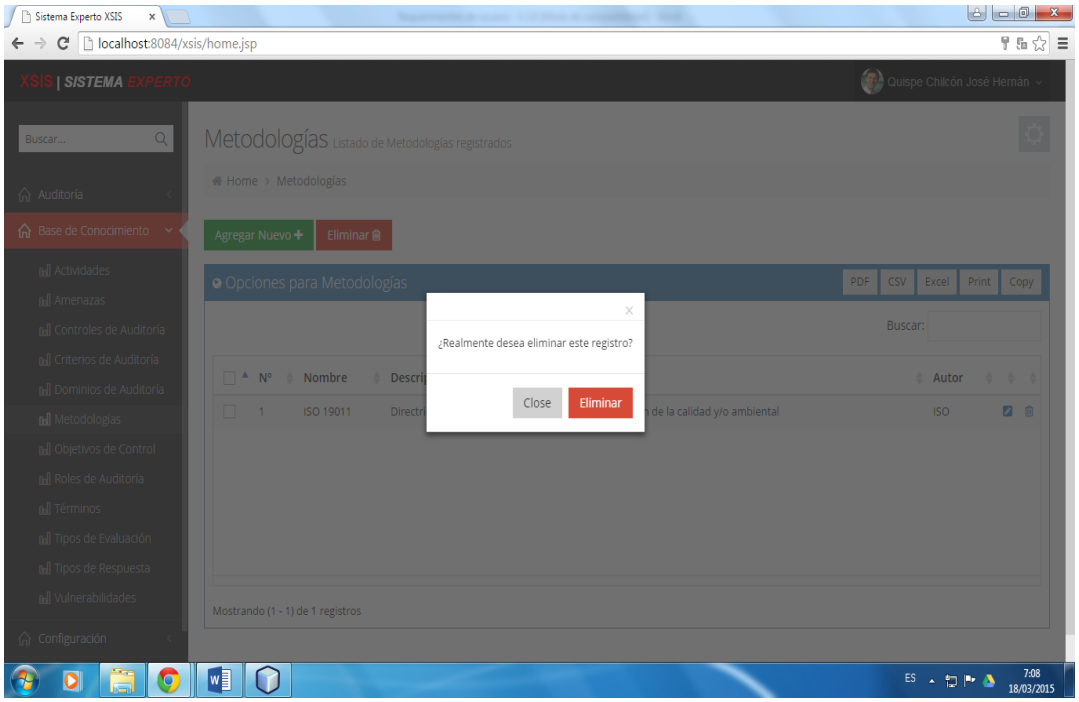
- **Registrar metodología**



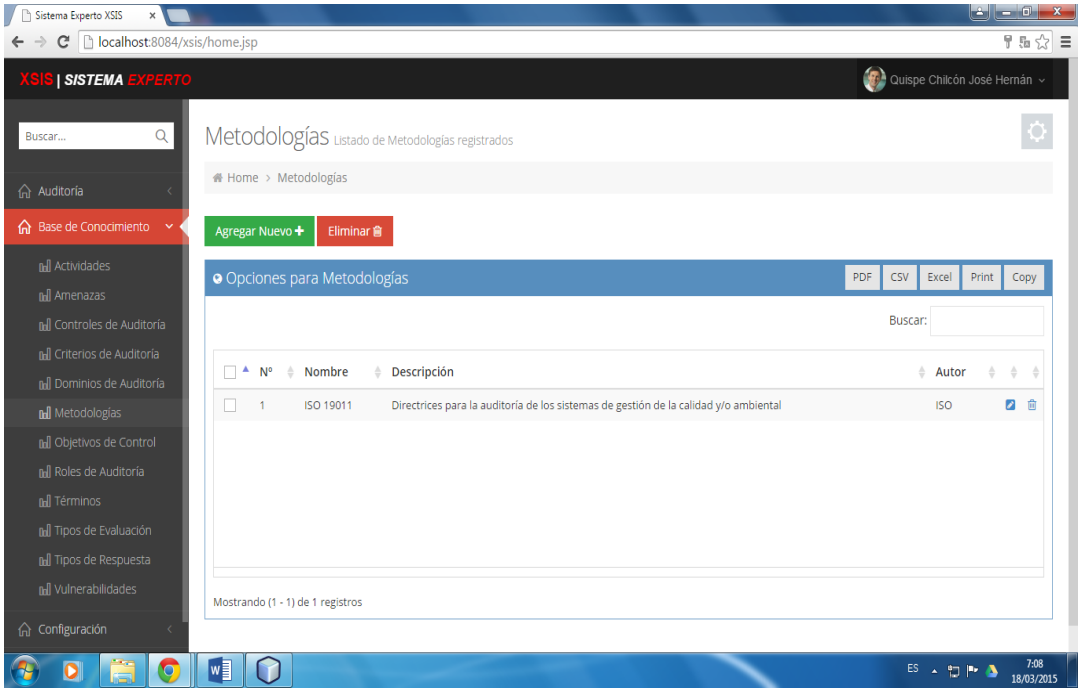
- **Modificar metodología**



- **Eliminar metodología**

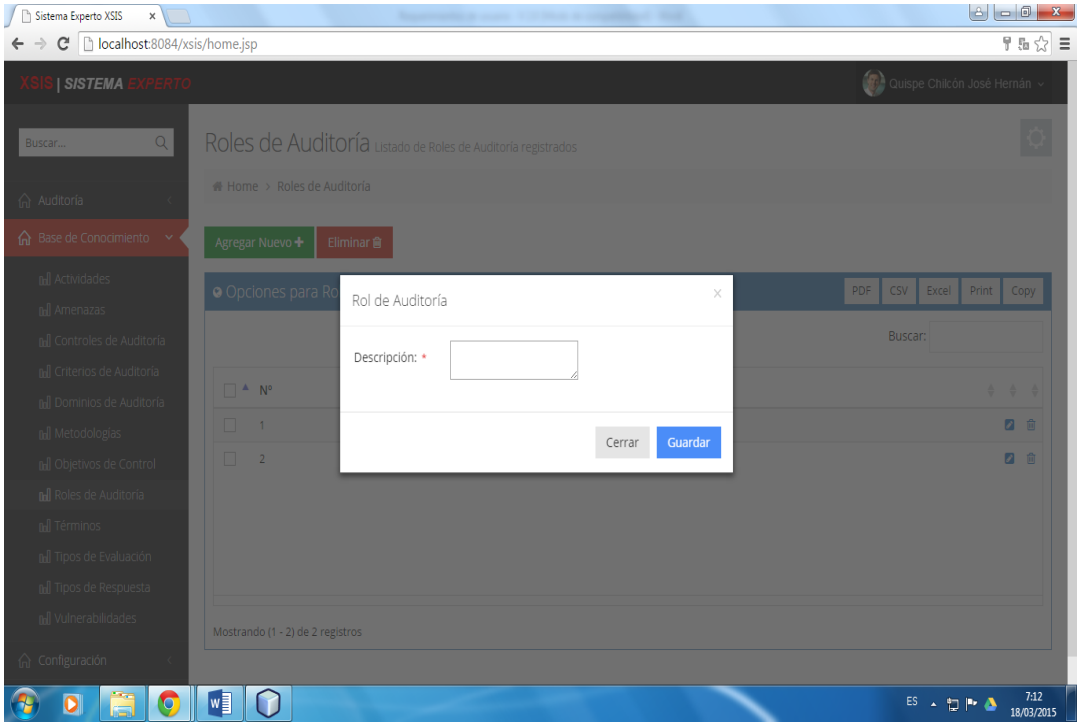


- **Listar metodologías**

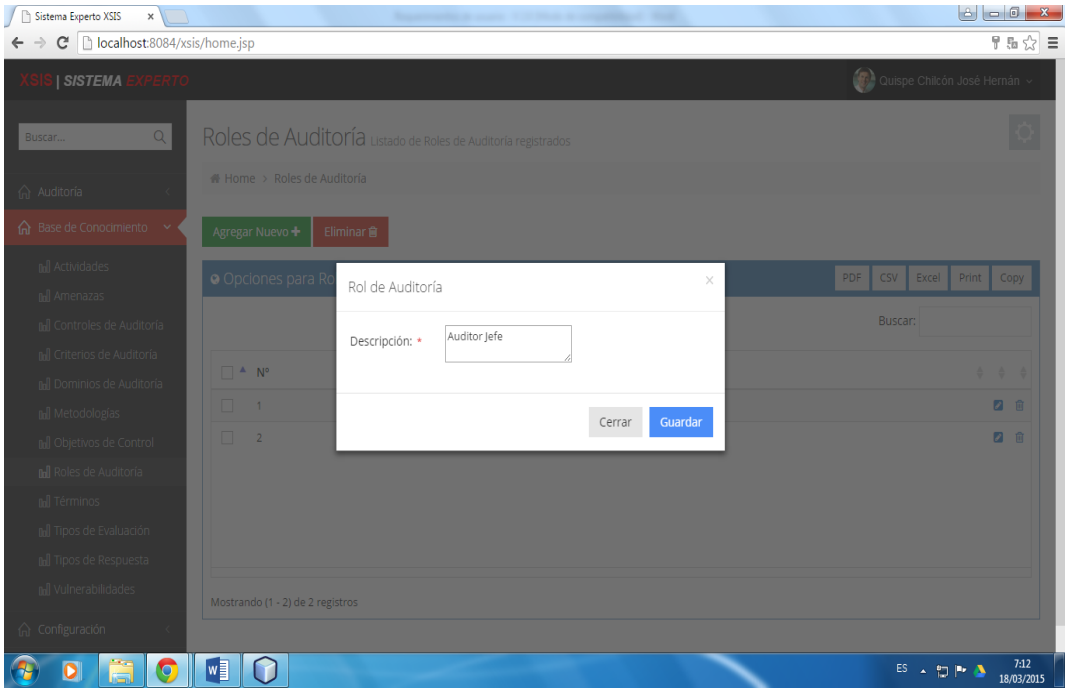


b. Roles auditoría

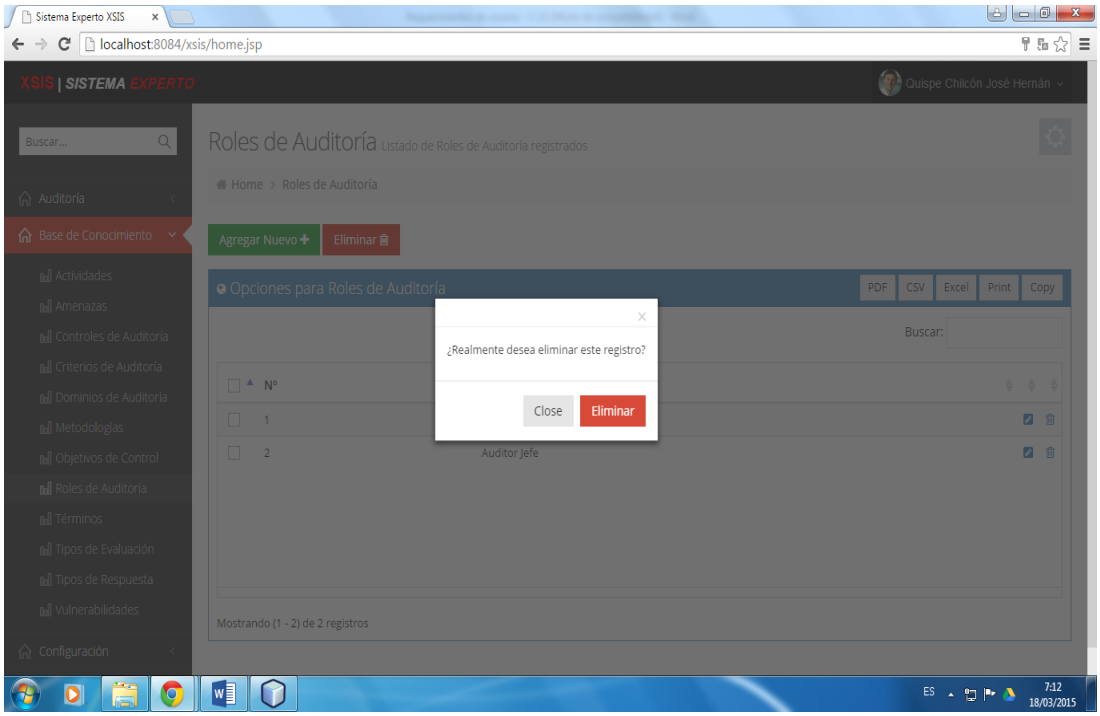
- Registrar rol auditoría



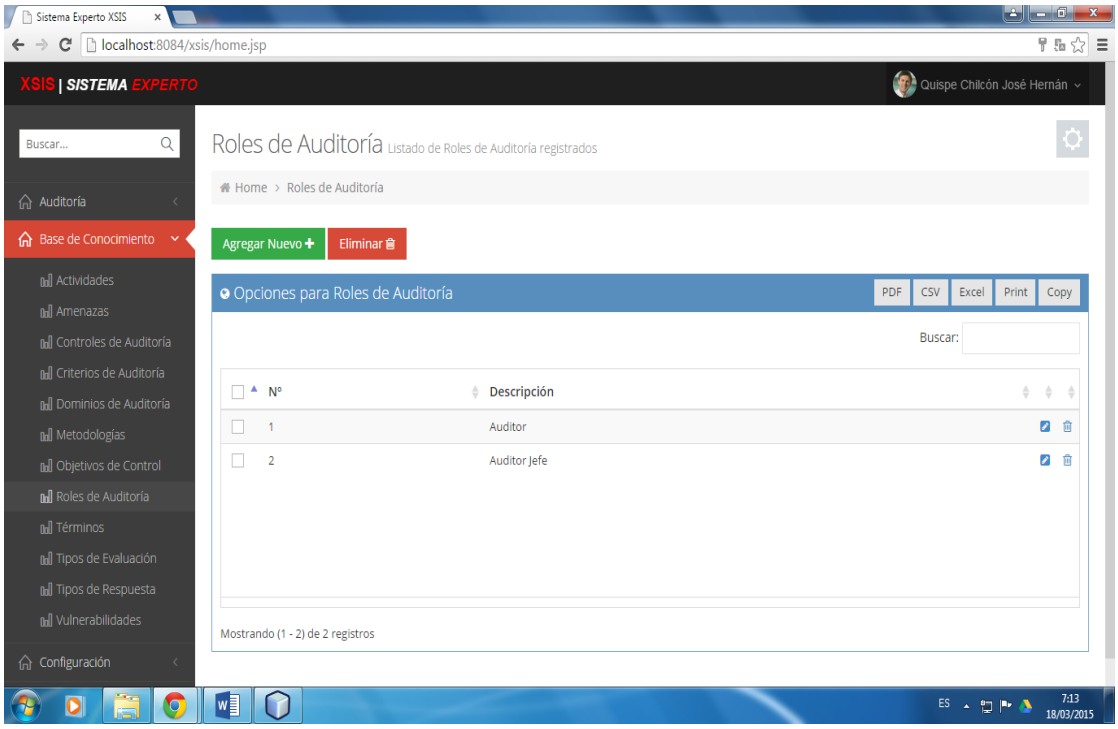
- Modificar rol auditoría



- **Eliminar rol auditoría**

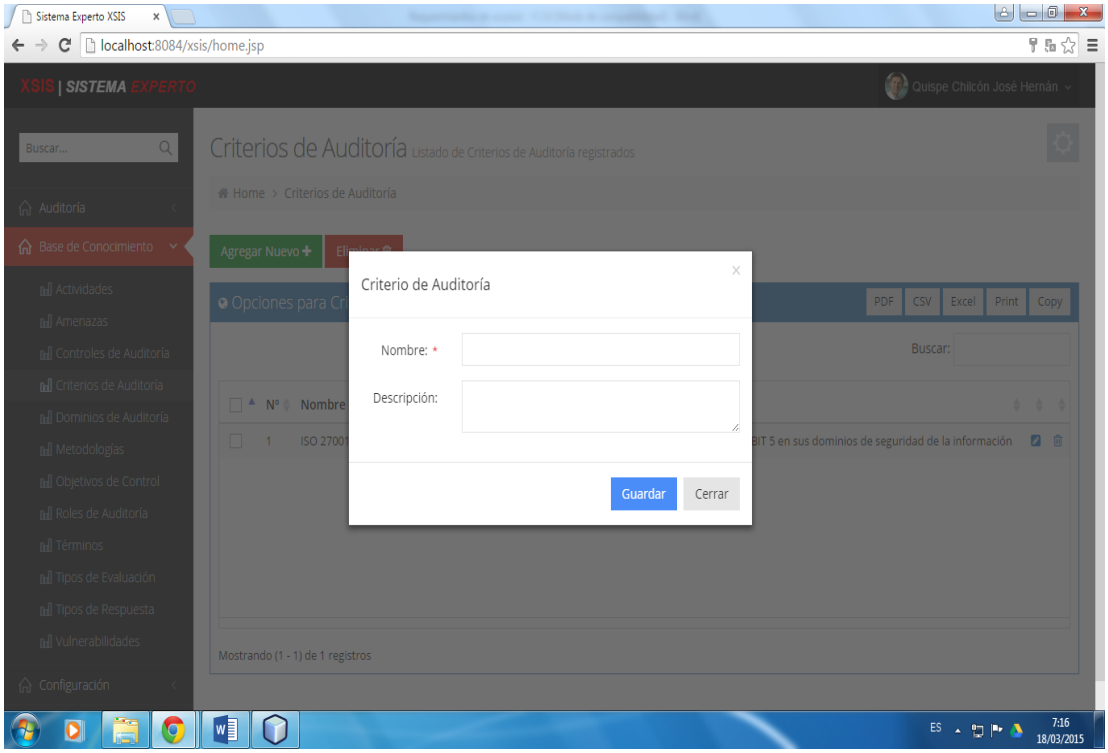


- **Listar roles auditoría**

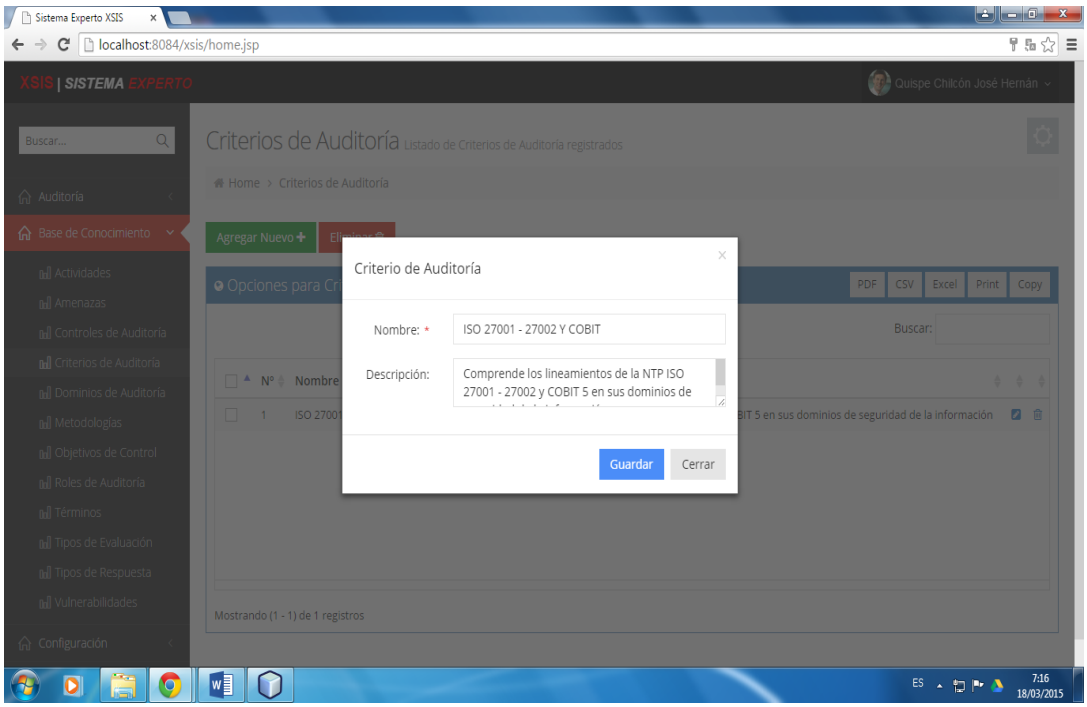


c. Criterios

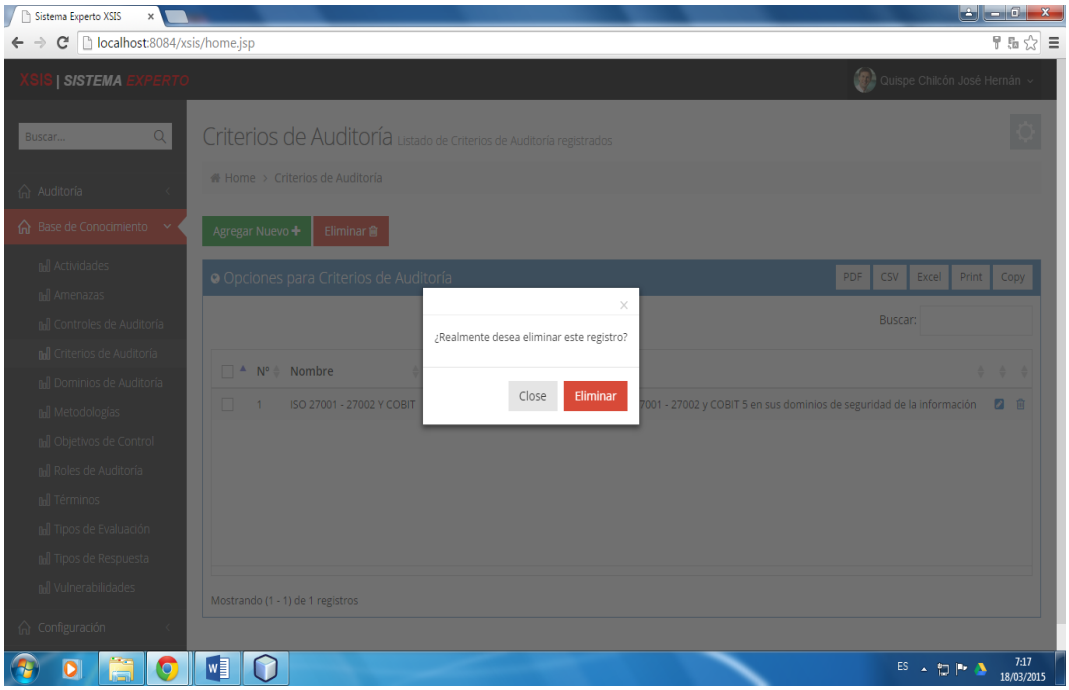
- **Registrar criterio**



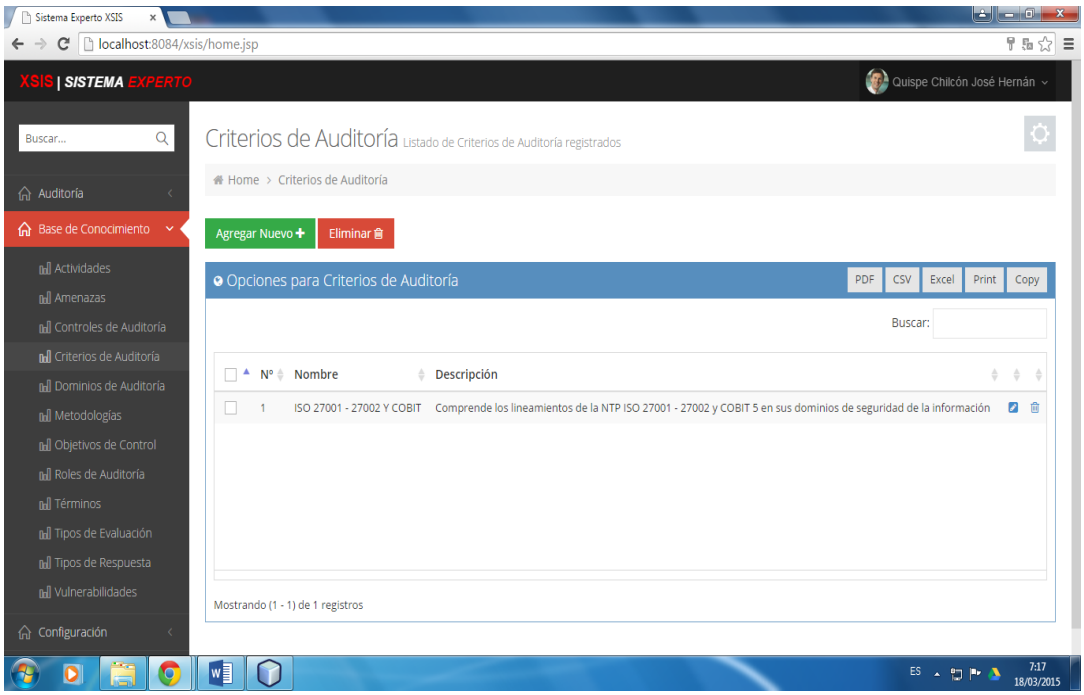
- **Modificar criterio**



- **Eliminar criterio**

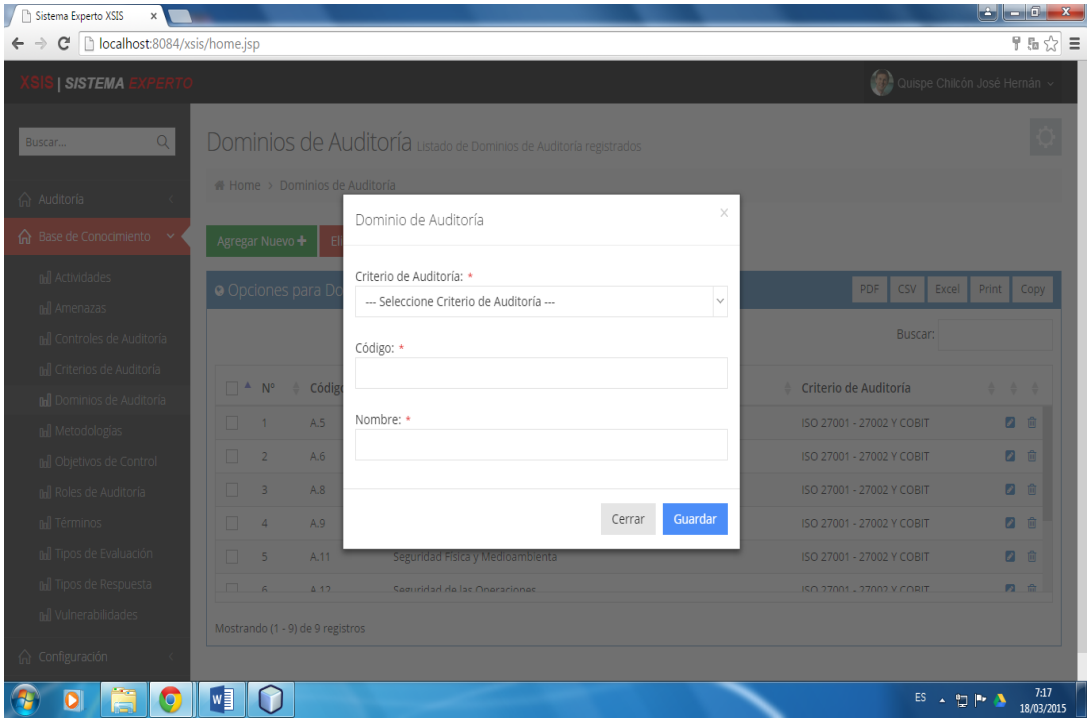


- **Listar criterios**

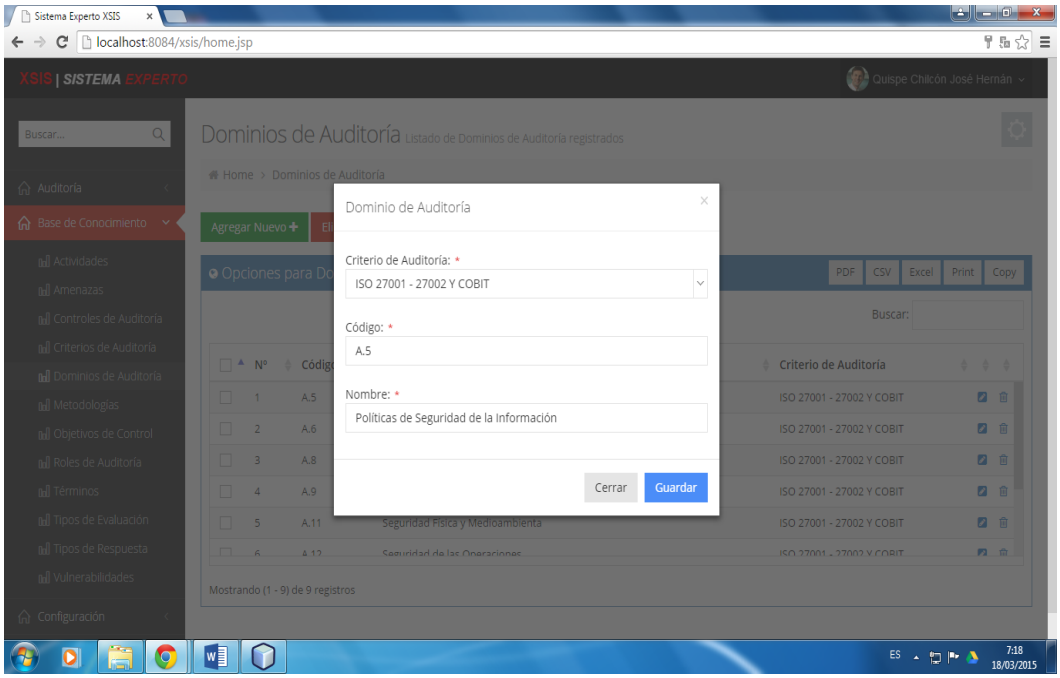


d. Dominios

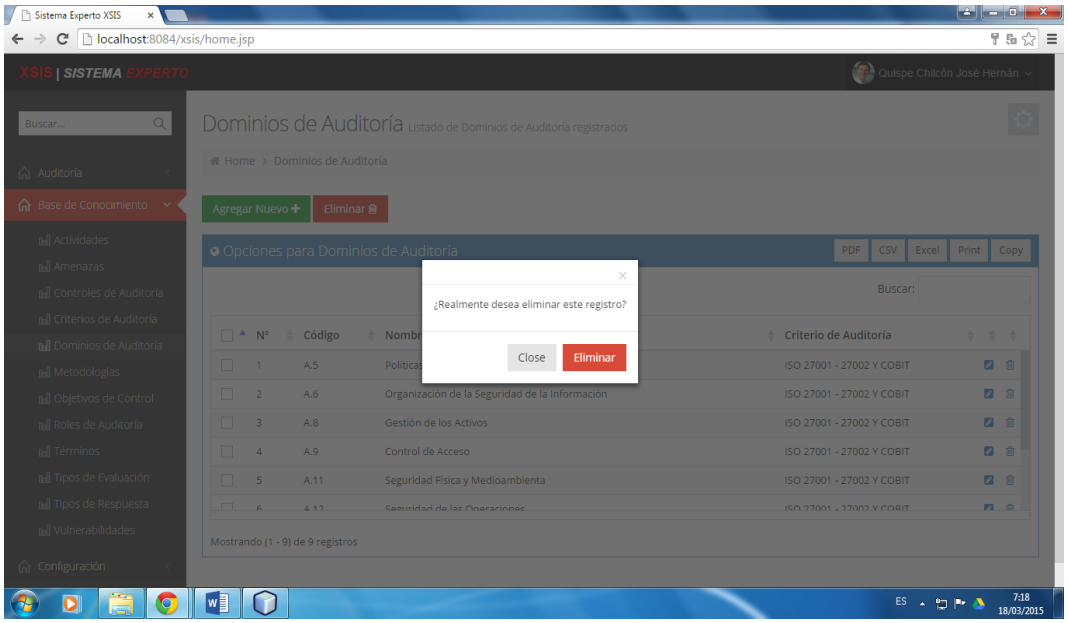
- Registrar dominio



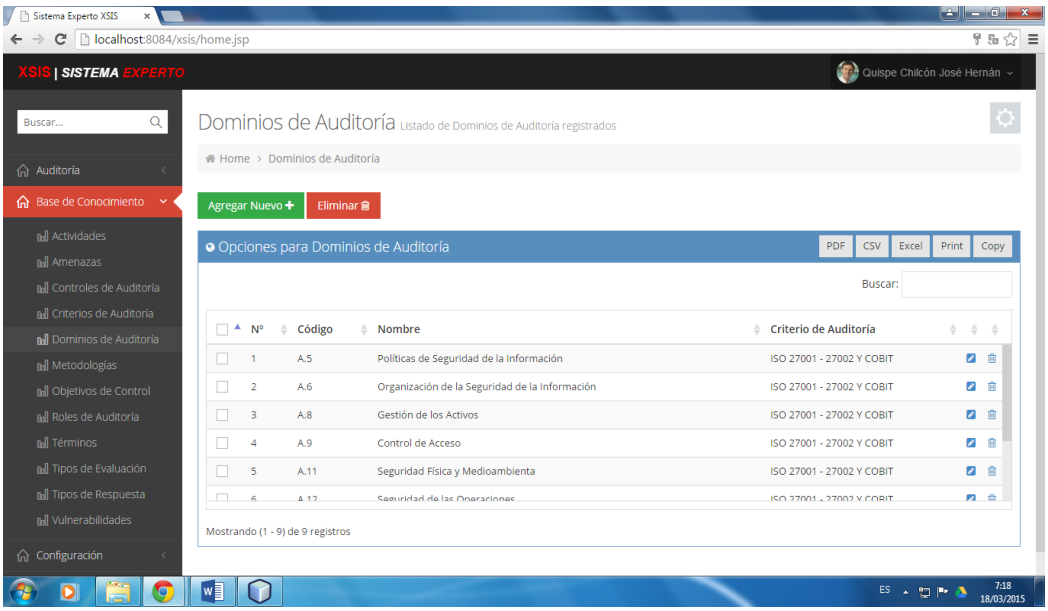
- Modificar dominio



- **Eliminar dominio**

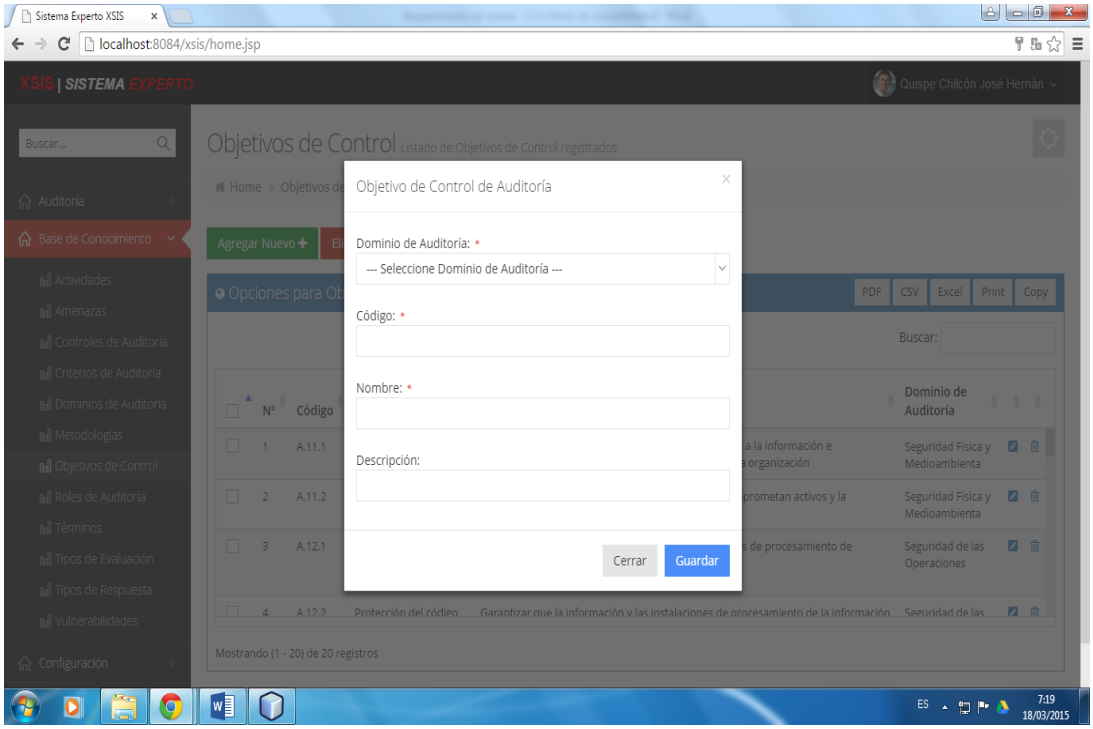


- **Listar dominios**

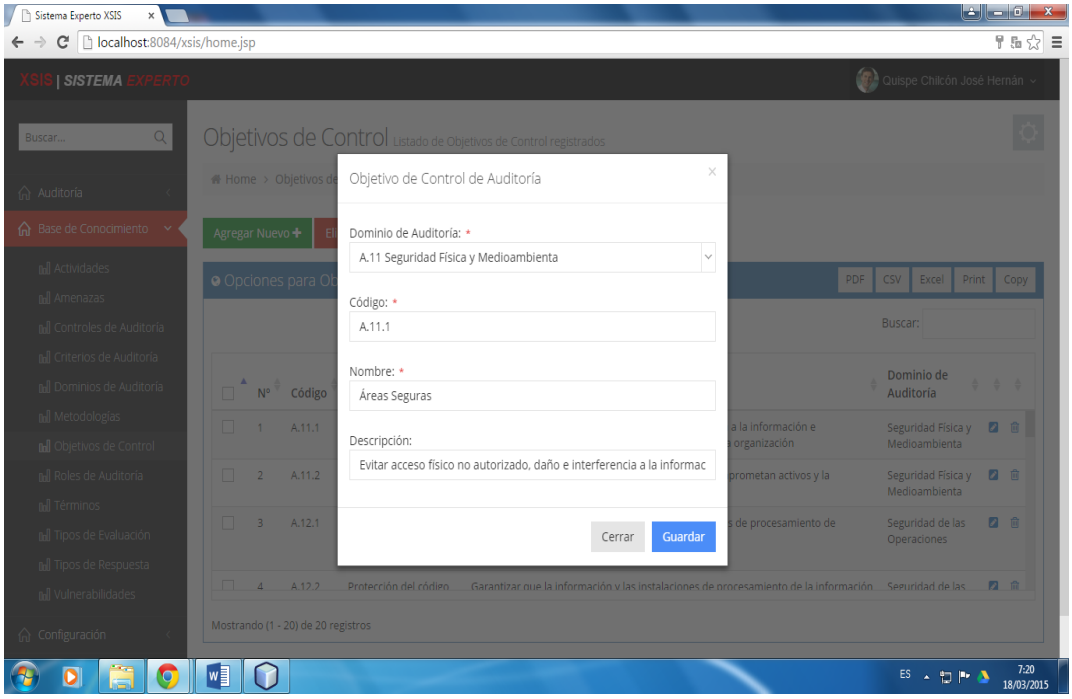


e. Objetivos de control de auditoría

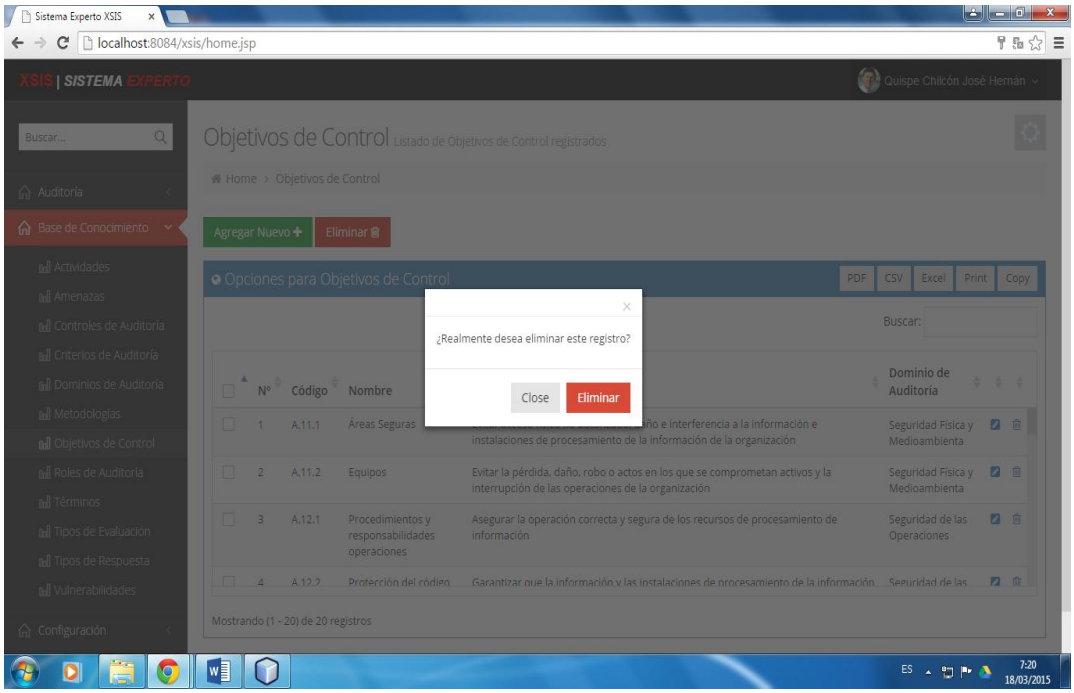
- Registrar objetivo de control



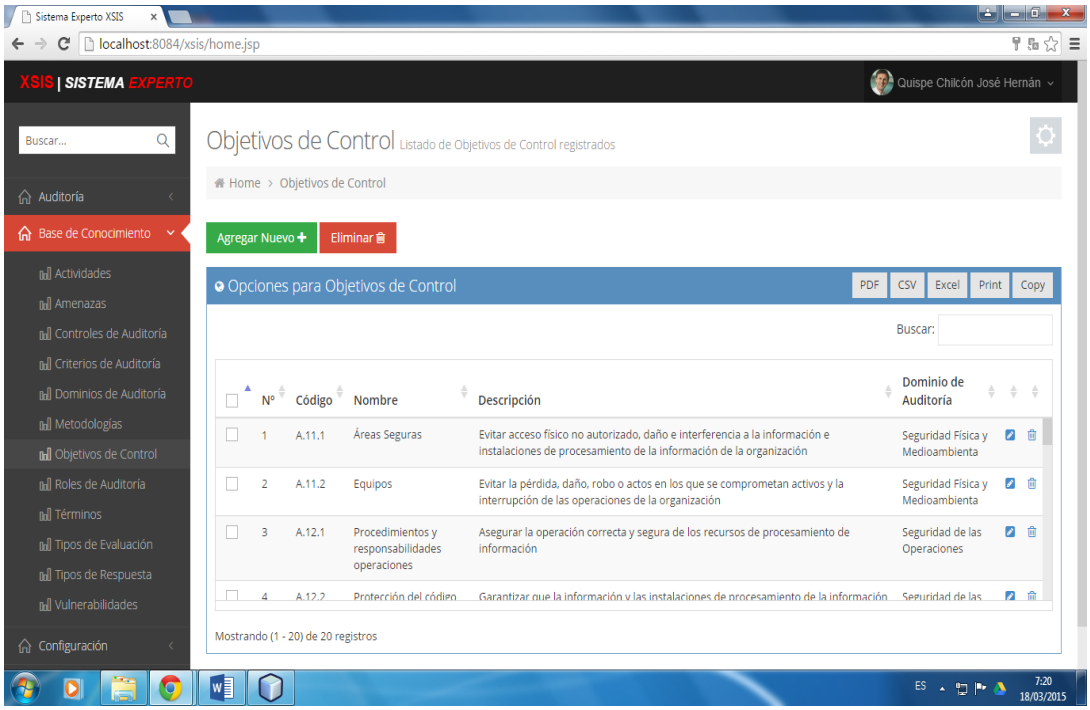
- Modificar objetivo de control



- **Eliminar objetivo de control**

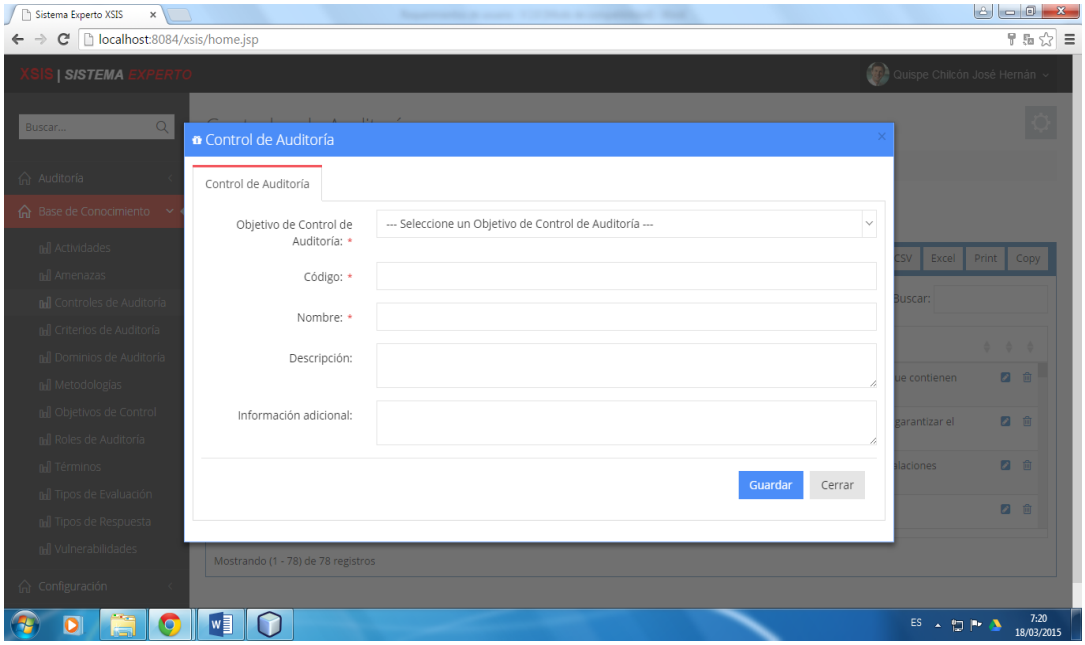


- **Listar objetivos de control**

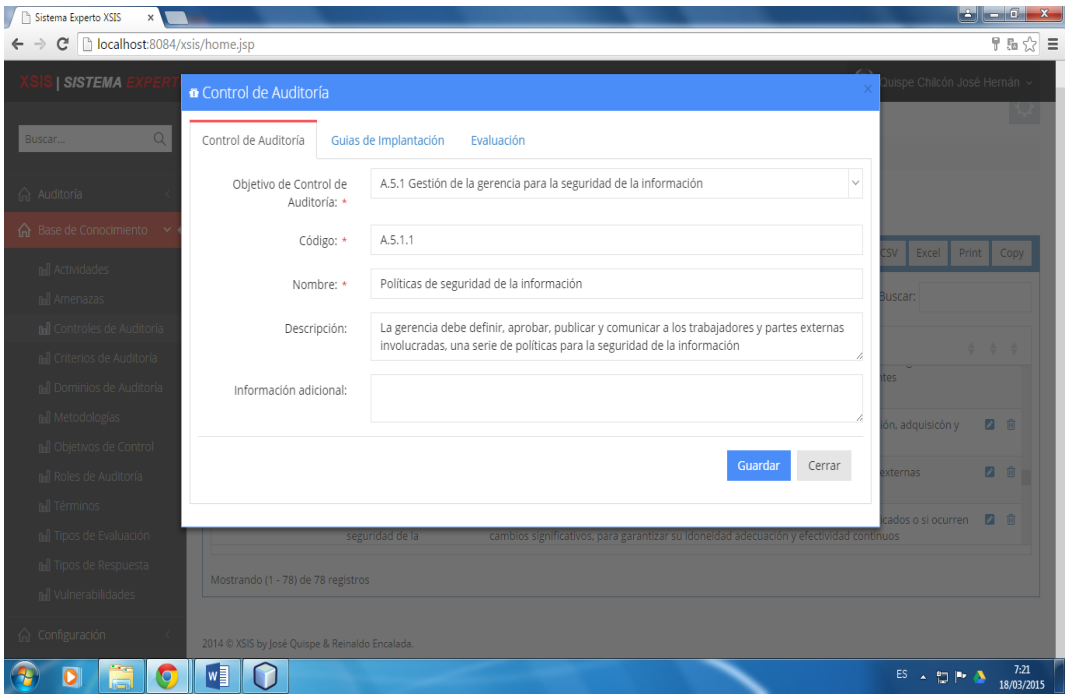


f. Control de Auditoría

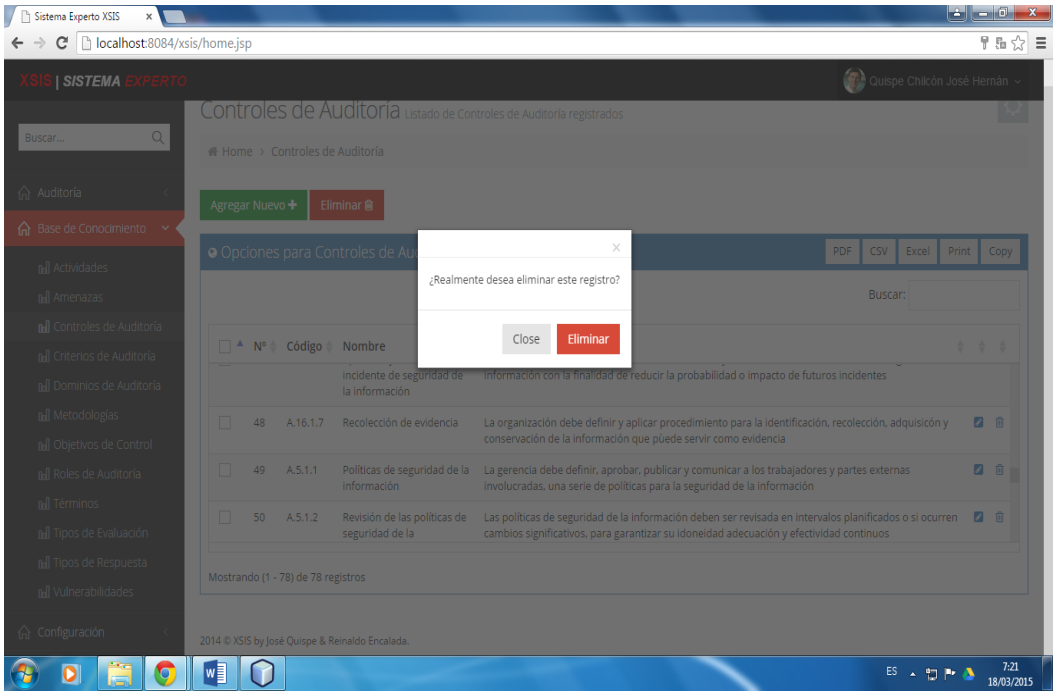
- Registrar Control Auditoría



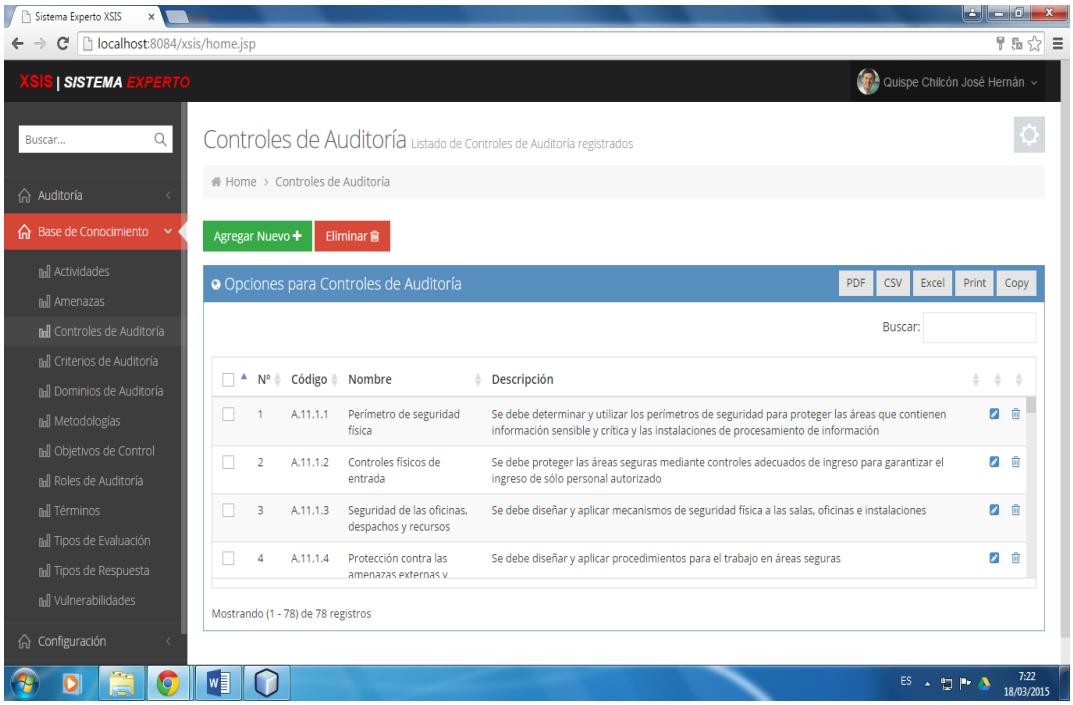
- Modificar control de Auditoría



- **Eliminar Control de Auditoría**

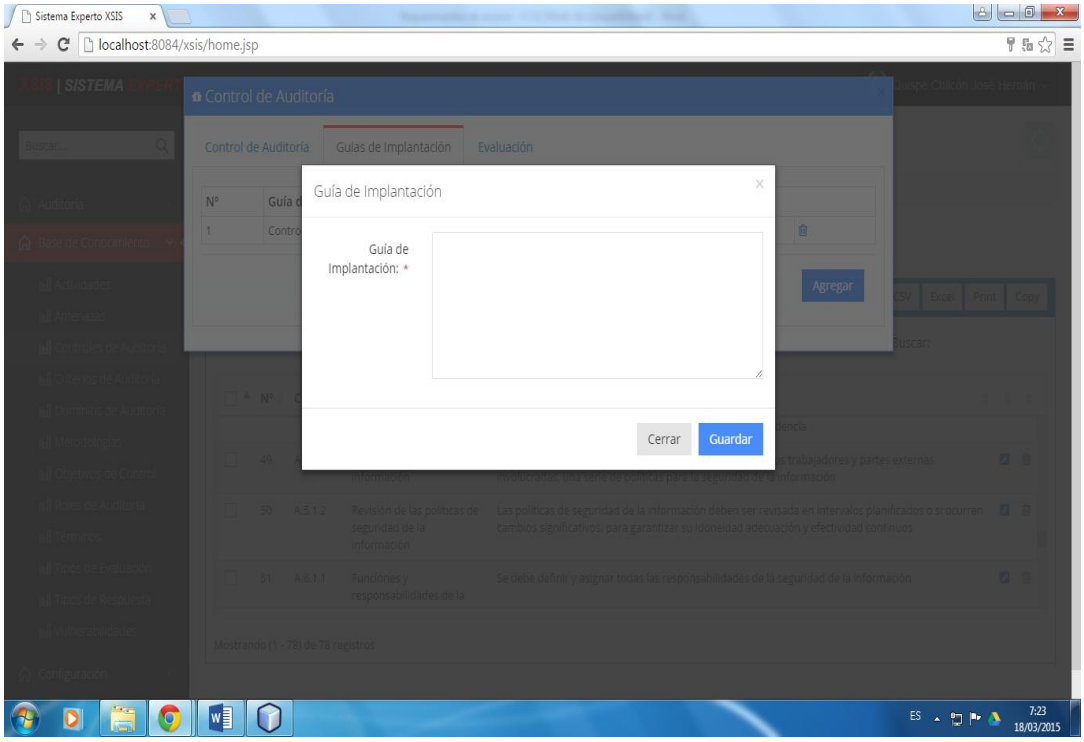


- **Listar controles de Auditoría**

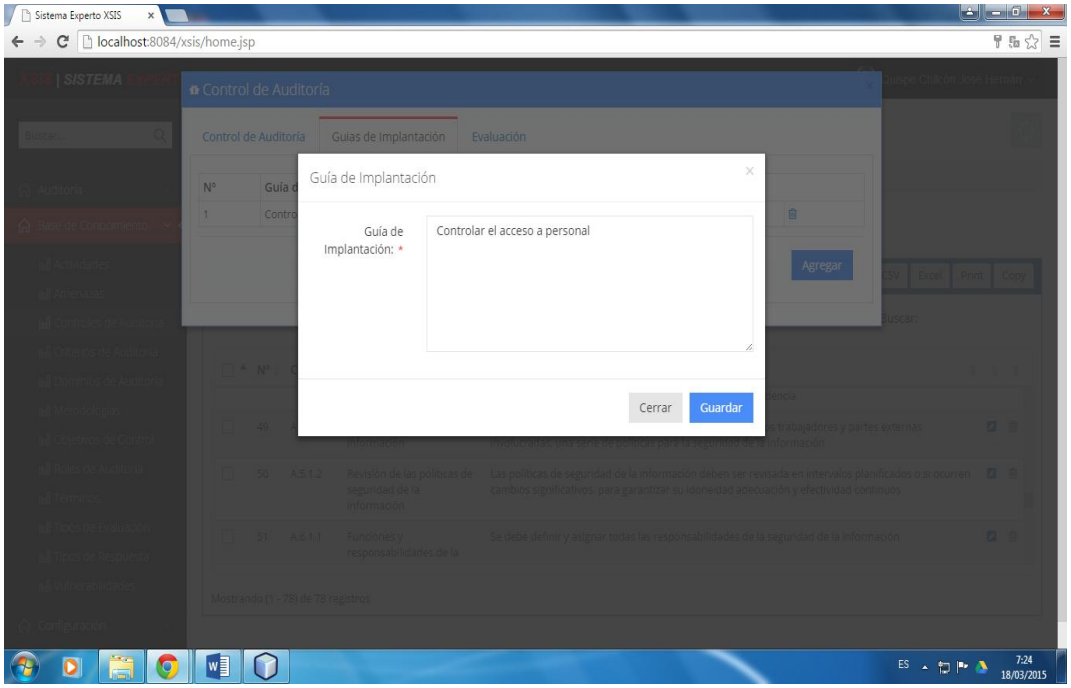


g. Guía de Implantación

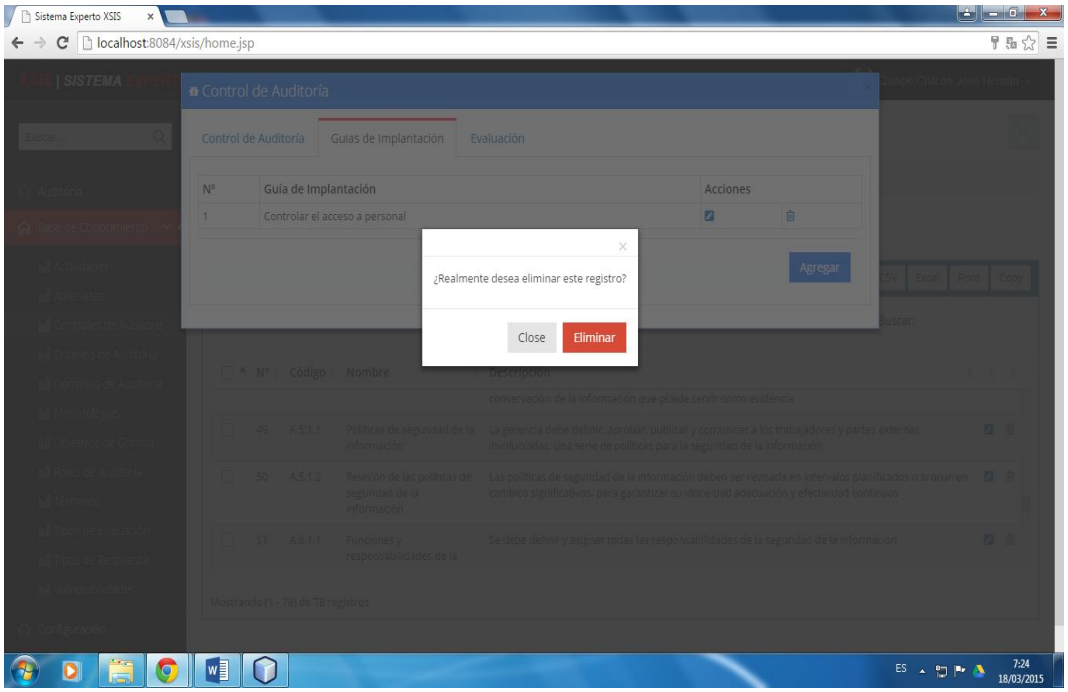
- Registrar guía de implantación



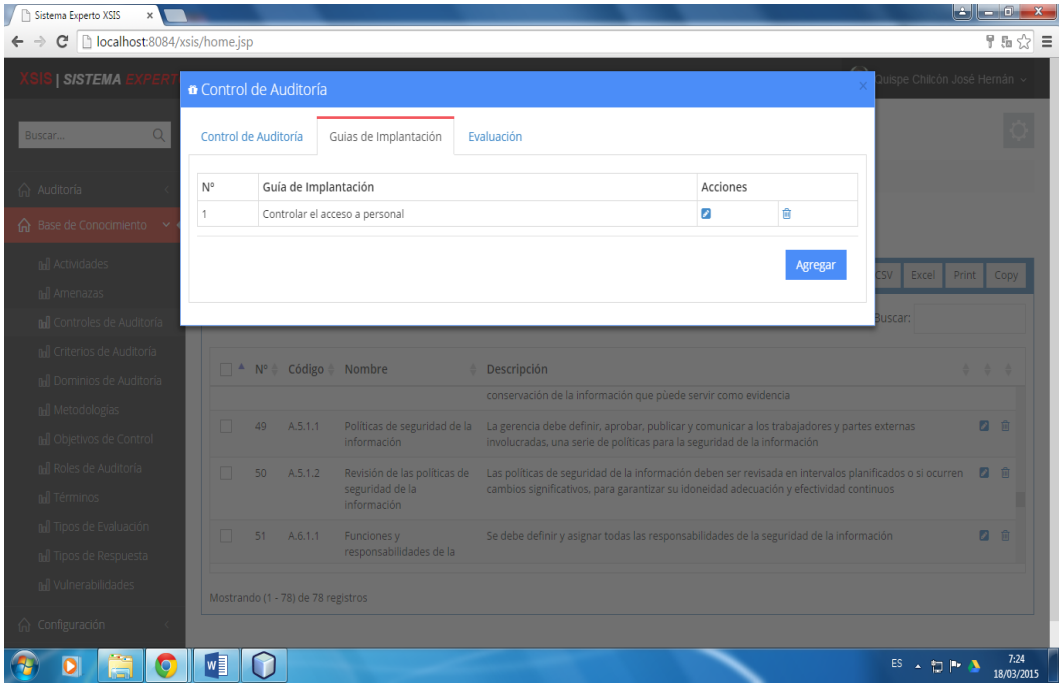
- Modificar guía de implantación



- **Eliminar guía de implantación**

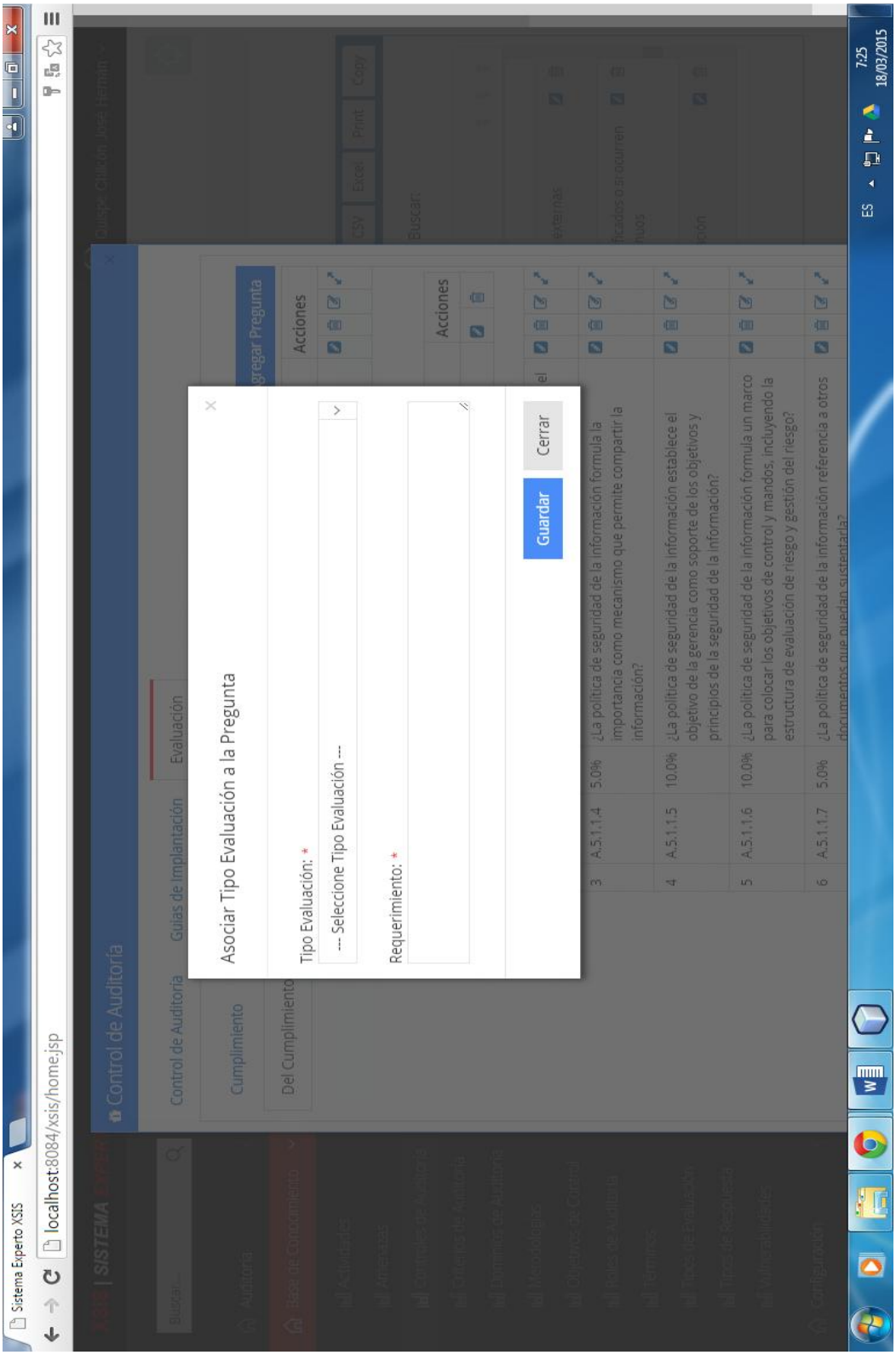


- **Listar guías de implantación**

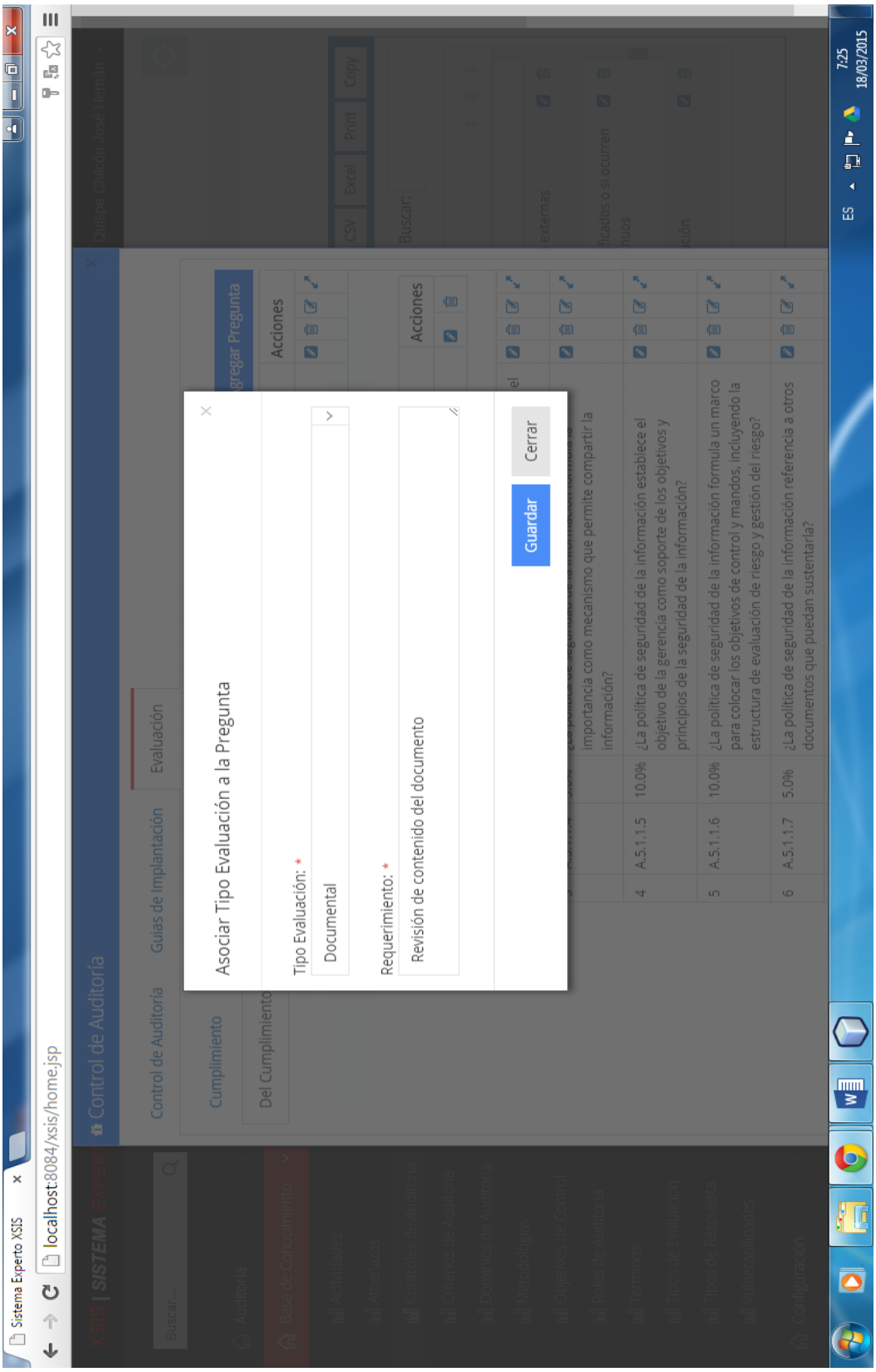


h. Pregunta – Tipo Evaluación

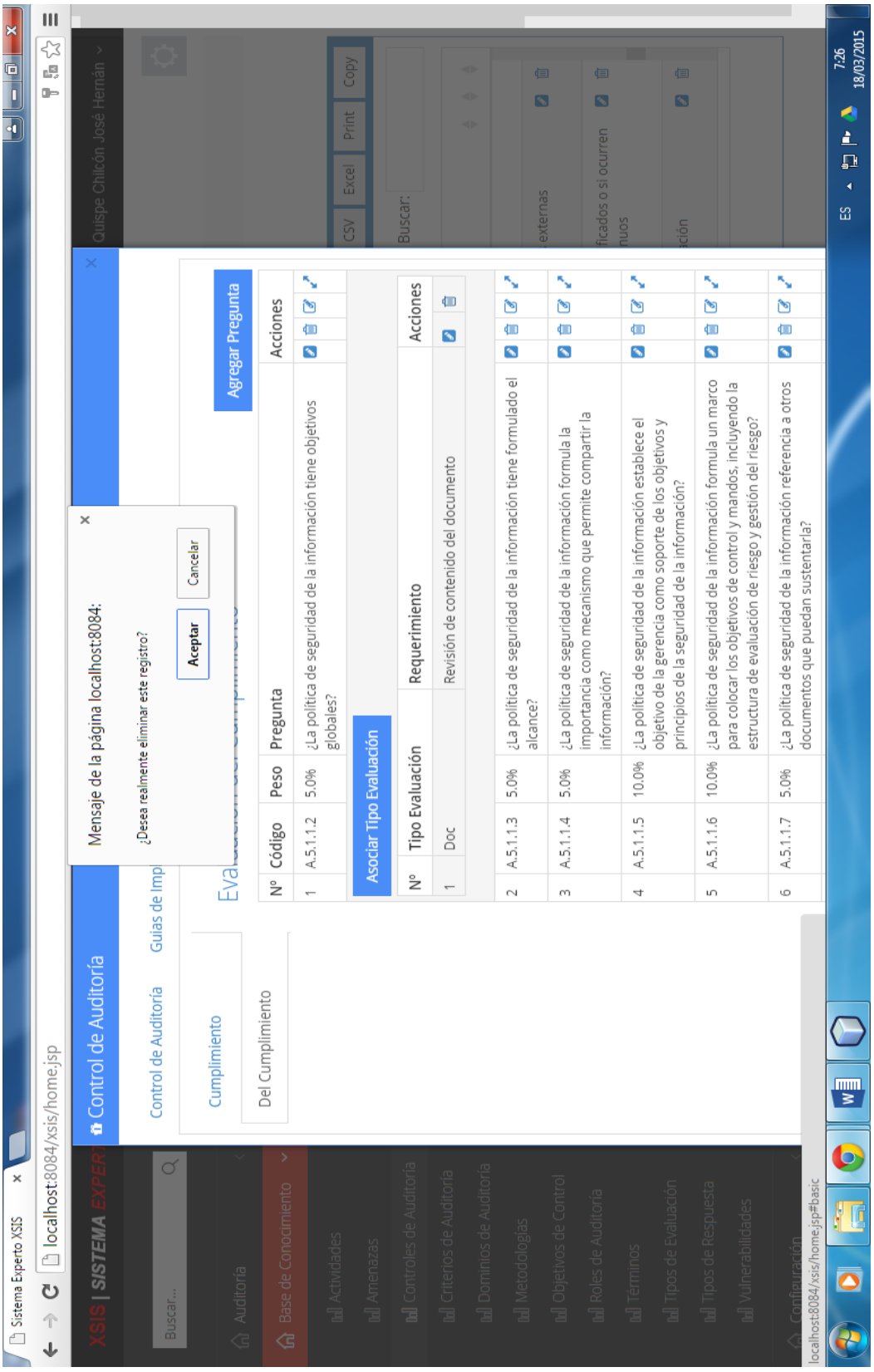
- **Agregar tipo de evaluación – pregunta**



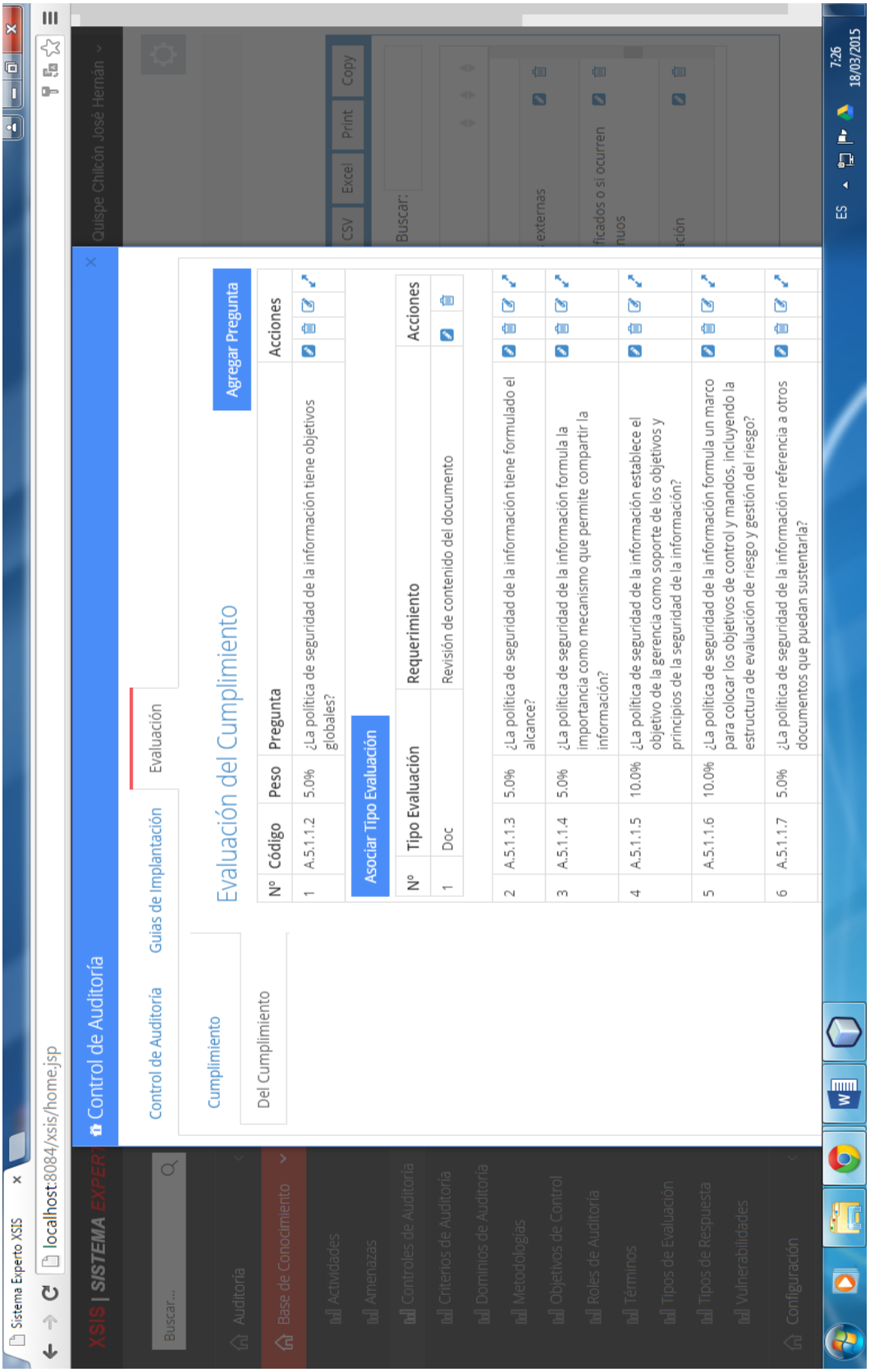
- **Modificar tipo de evaluación – pregunta**



- **Eliminar tipo de evaluación – pregunta**

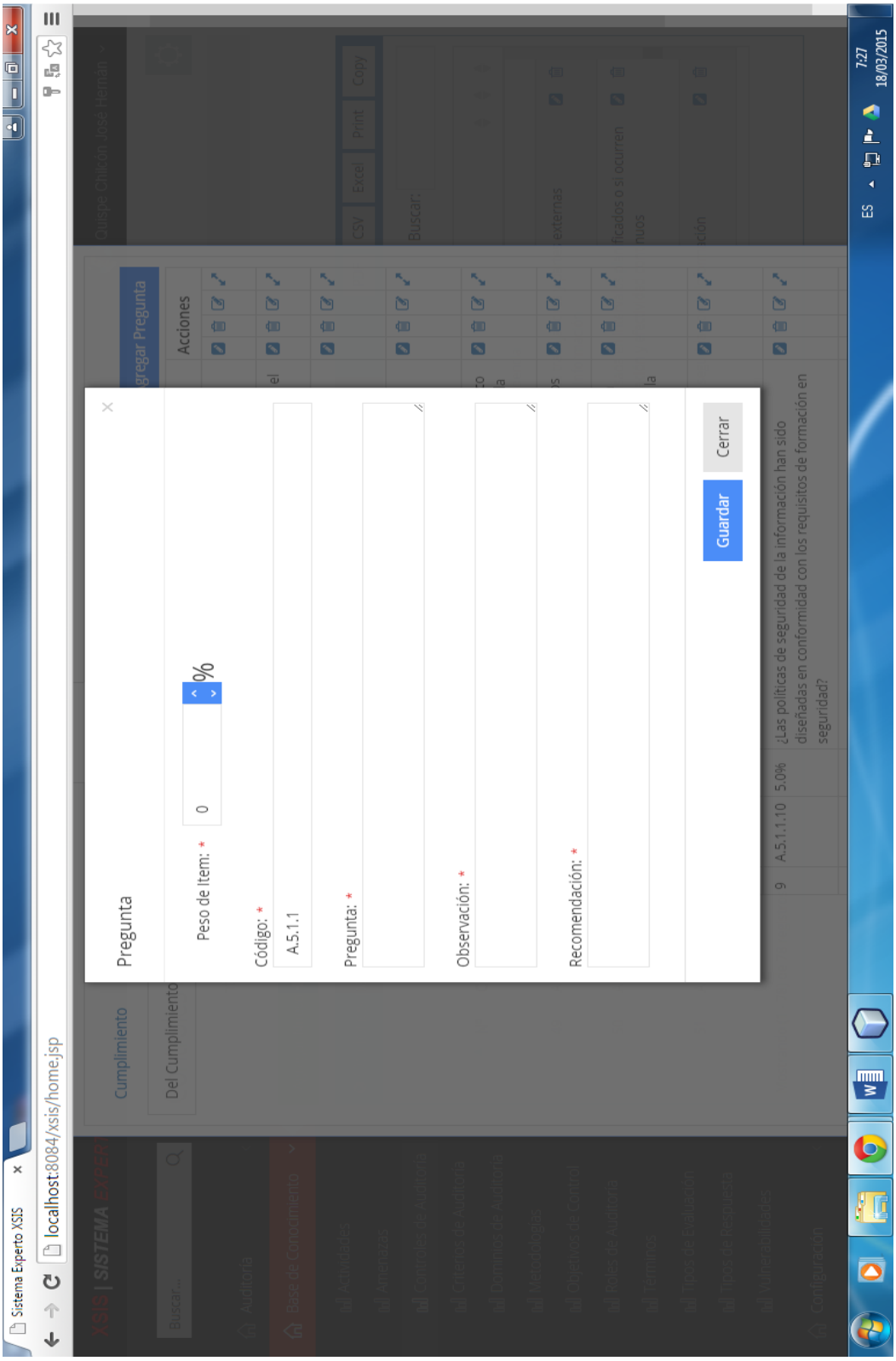


- **Listar tipo de evaluación - pregunta**

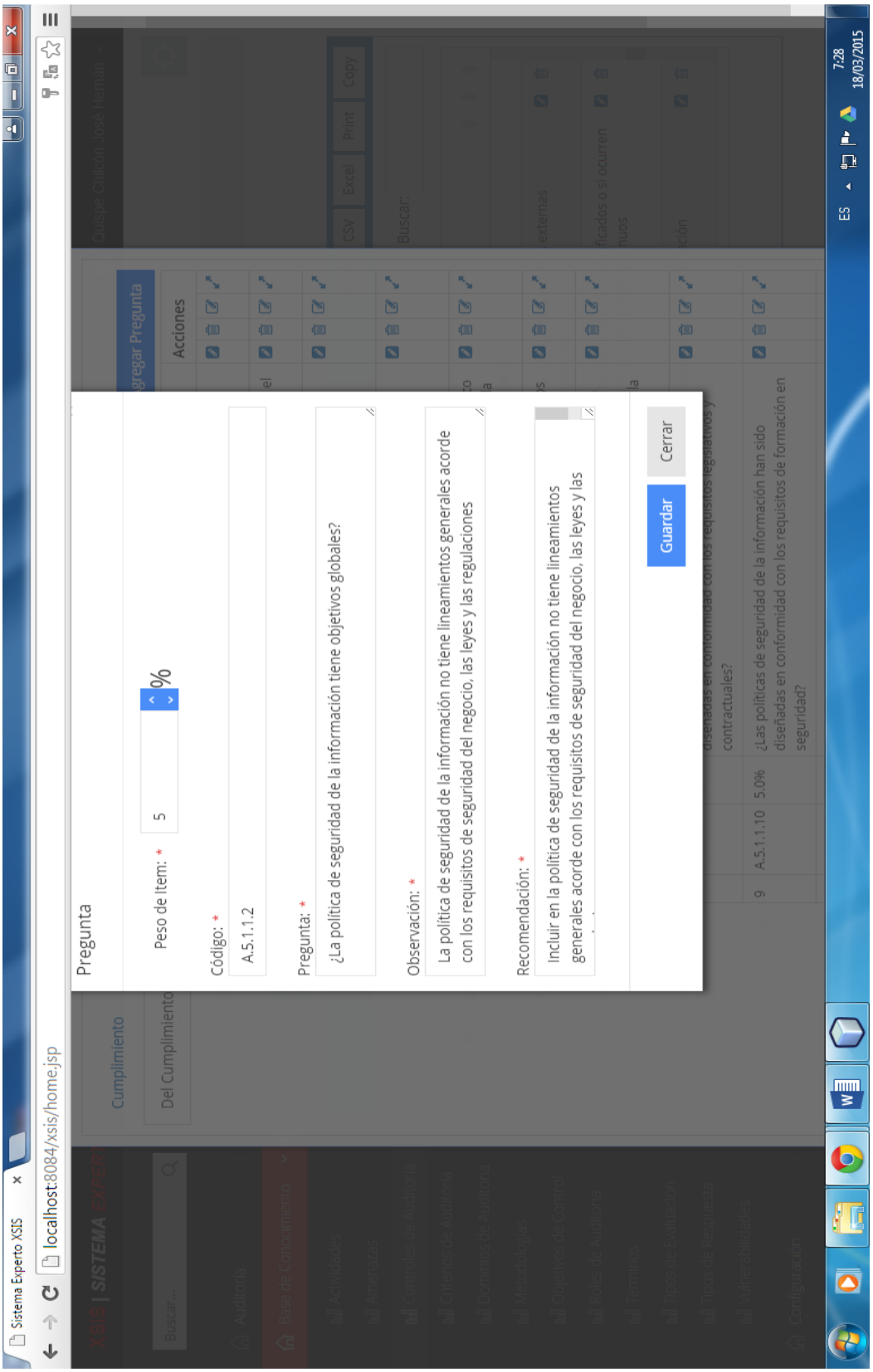


i. Pregunta – control auditoría

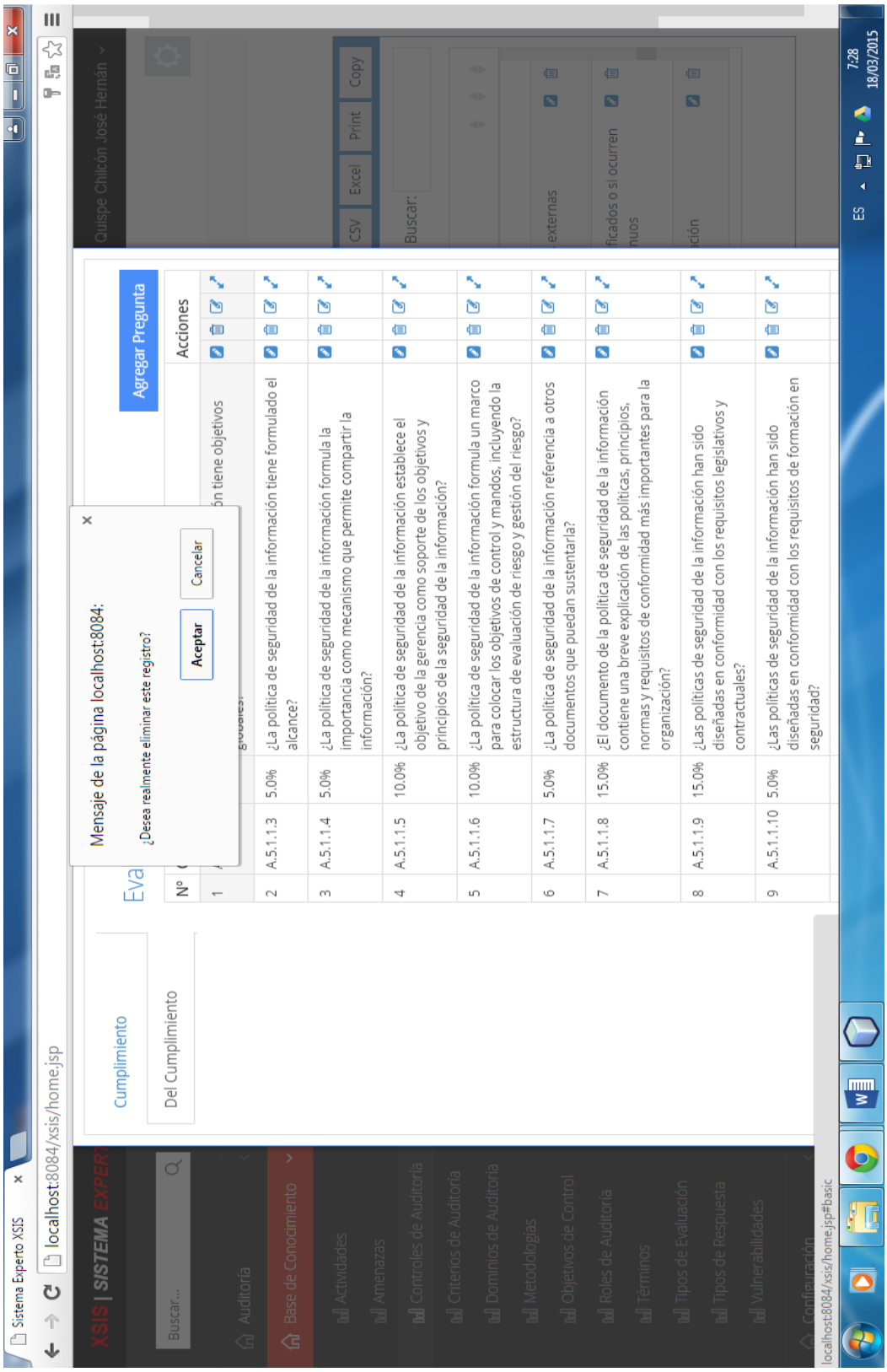
- **Registrar pregunta control auditoría**



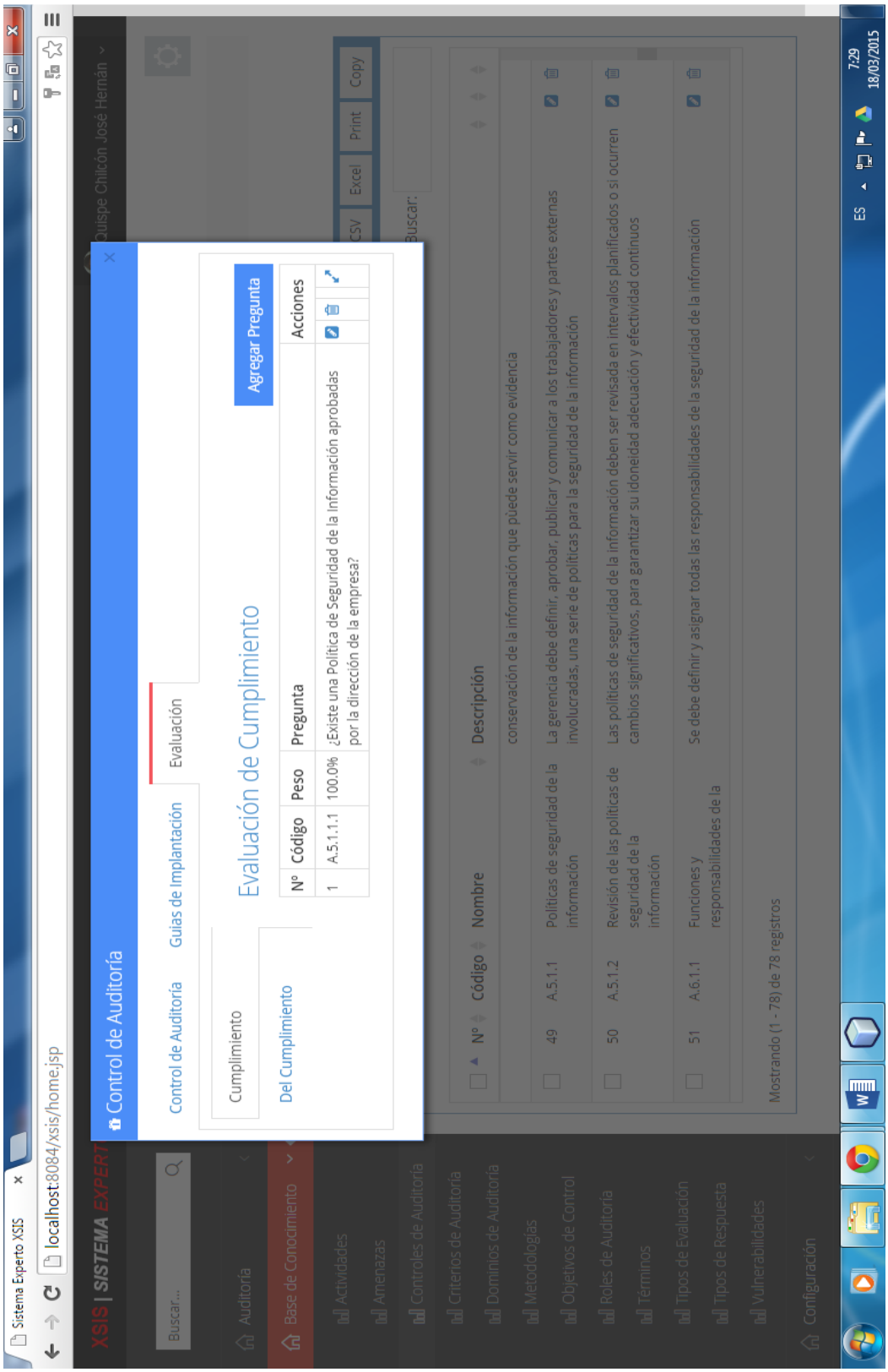
- **Modificar pregunta control auditoría**

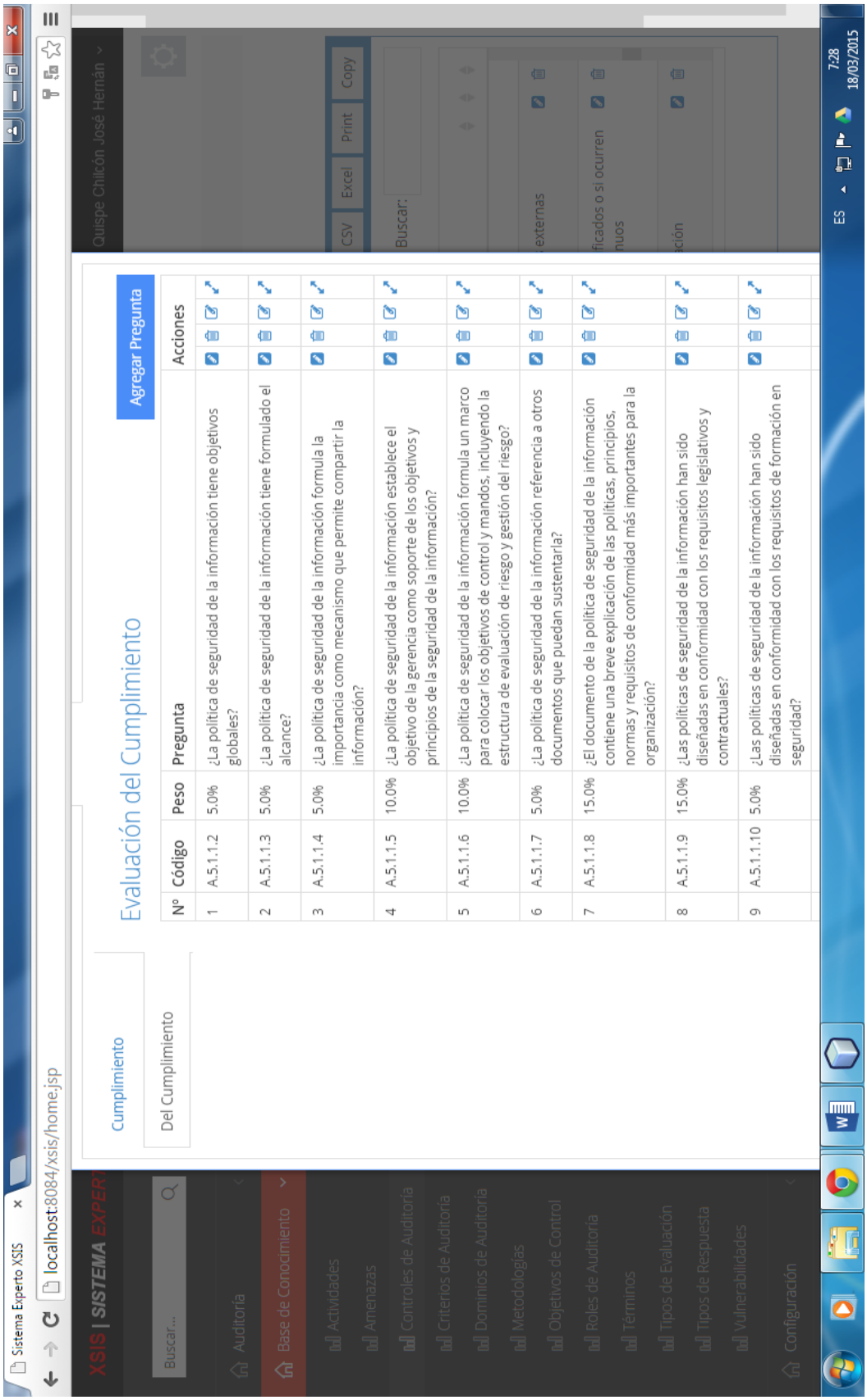


- **Eliminar pregunta control auditoría**



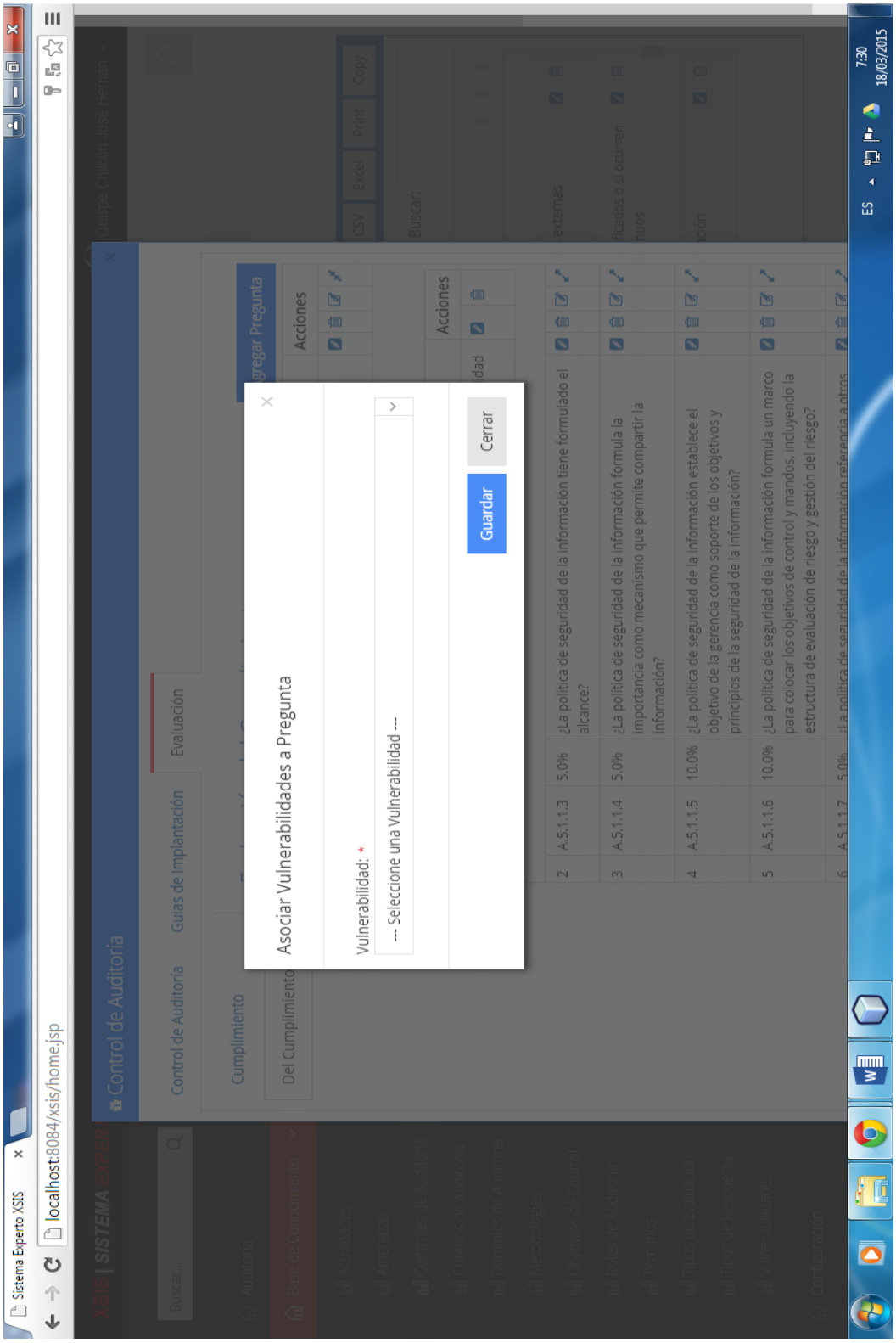
- **Listar preguntas control auditoría**



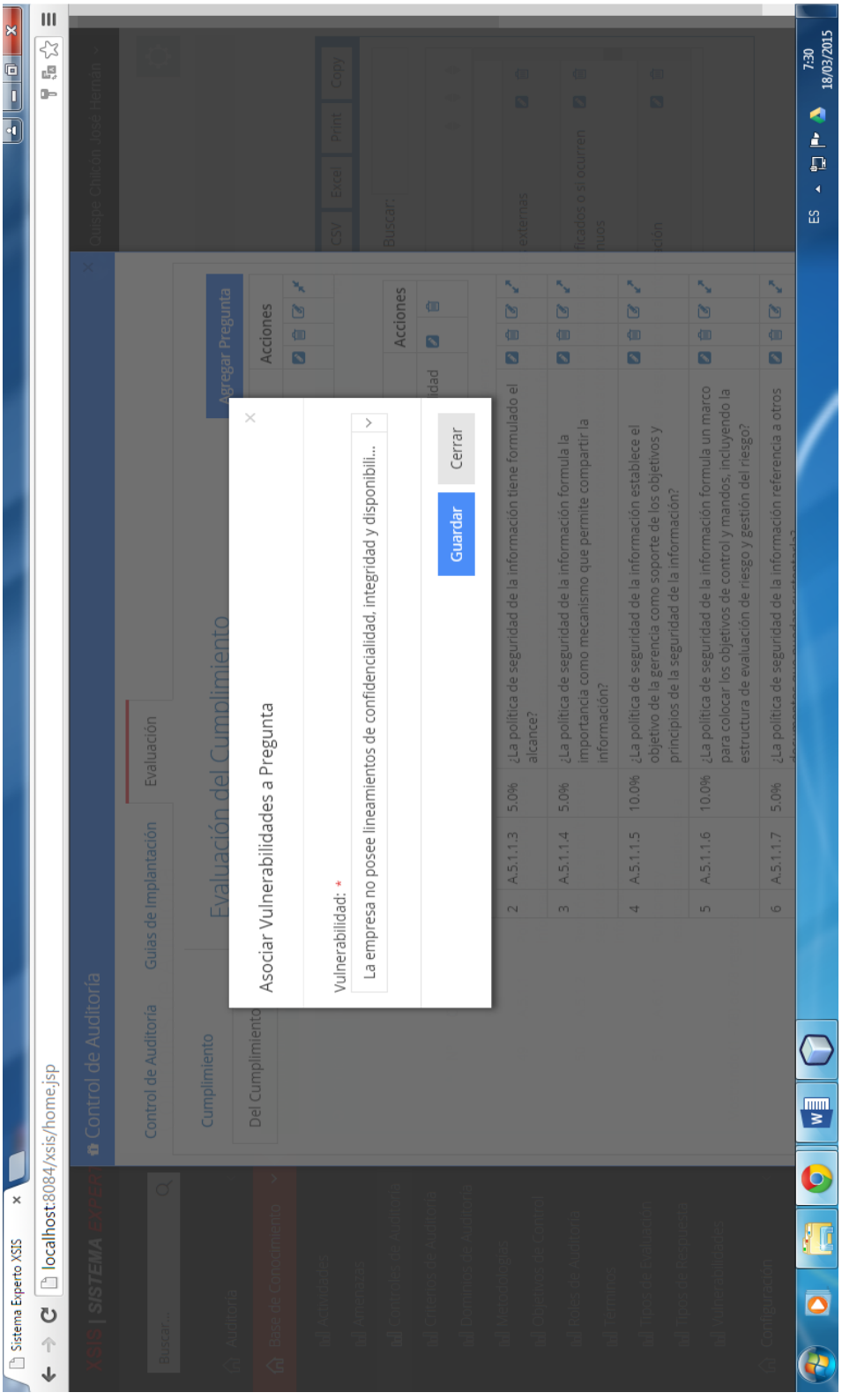

Sistema Experto XSIS
localhost:8084/xsis/home.jsp
XSIS | SISTEMA EXPERT
Quispe Chilcón José Hernán
Buscar...
Auditoría
Base de Conocimiento
Actividades
Amenazas
Controles de Auditoría
Criterios de Auditoría
Dominios de Auditoría
Metodologías
Objetivos de Control
Roles de Auditoría
Términos
Tipos de Evaluacion
Tipos de Respuesta
Vulnerabilidades
Configuración
Cumplimiento
Del Cumplimiento
Evaluación del Cumplimiento
Agregar Pregunta
CSV
Excel
Print
Copy
Buscar:
Nº
Código
Peso
Pregunta
Acciones
1 A.5.1.1.2 5.0% ¿La política de seguridad de la información tiene objetivos globales?
2 A.5.1.1.3 5.0% ¿La política de seguridad de la información tiene formulado el alcance?
3 A.5.1.1.4 5.0% ¿La política de seguridad de la información formula la importancia como mecanismo que permite compartir la información?
4 A.5.1.1.5 10.0% ¿La política de seguridad de la información establece el objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información?
5 A.5.1.1.6 10.0% ¿La política de seguridad de la información formula un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión del riesgo?
6 A.5.1.1.7 5.0% ¿La política de seguridad de la información referencia a otros documentos que puedan sustentarla?
7 A.5.1.1.8 15.0% ¿El documento de la política de seguridad de la información contiene una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización?
8 A.5.1.1.9 15.0% ¿Las políticas de seguridad de la información han sido diseñadas en conformidad con los requisitos legislativos y contractuales?
9 A.5.1.1.10 5.0% ¿Las políticas de seguridad de la información han sido diseñadas en conformidad con los requisitos de formación en seguridad?
ES
7:28
18/03/2015

j. Pregunta - Vulnerabilidad

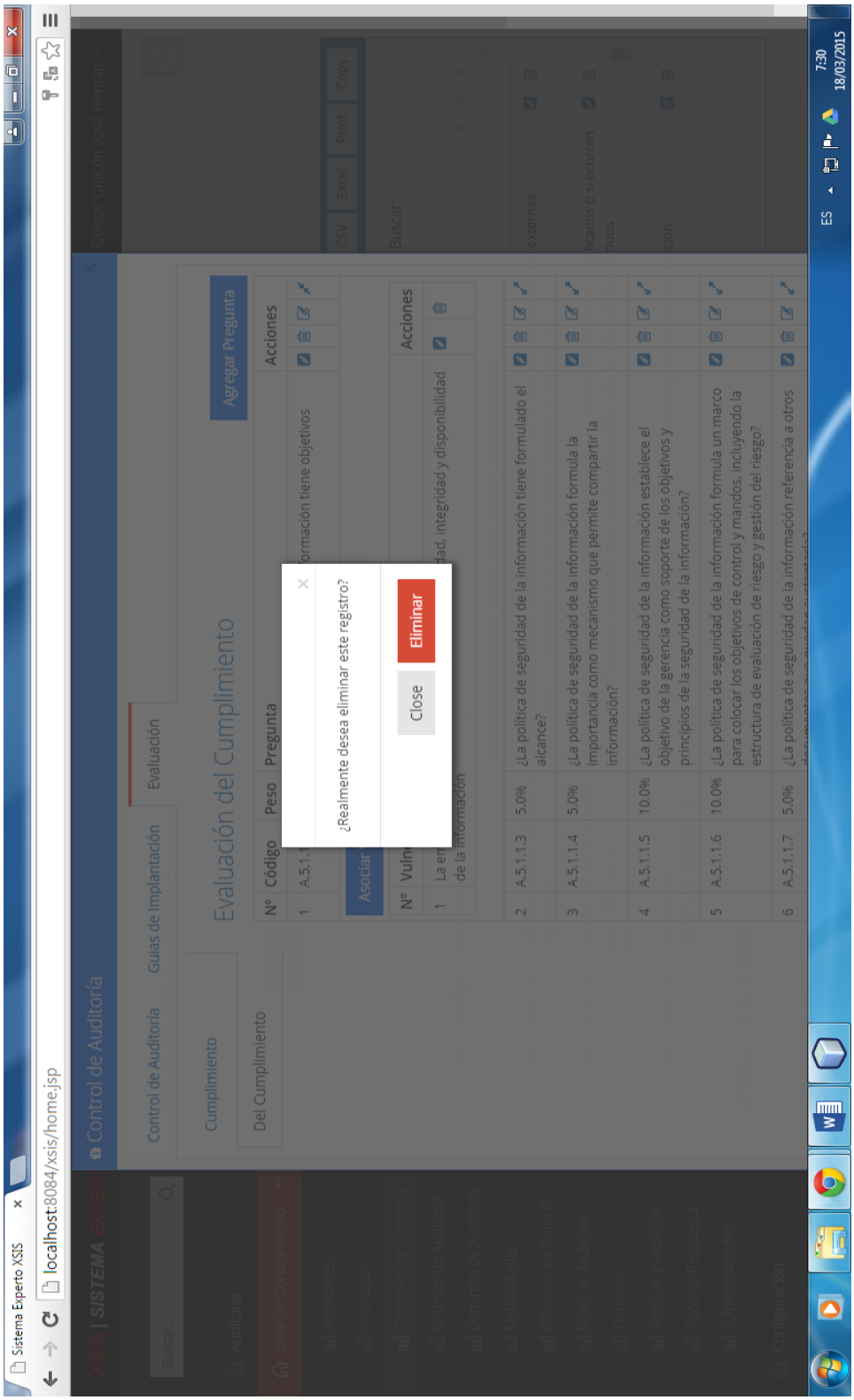
- **Asociar pregunta – vulnerabilidad**



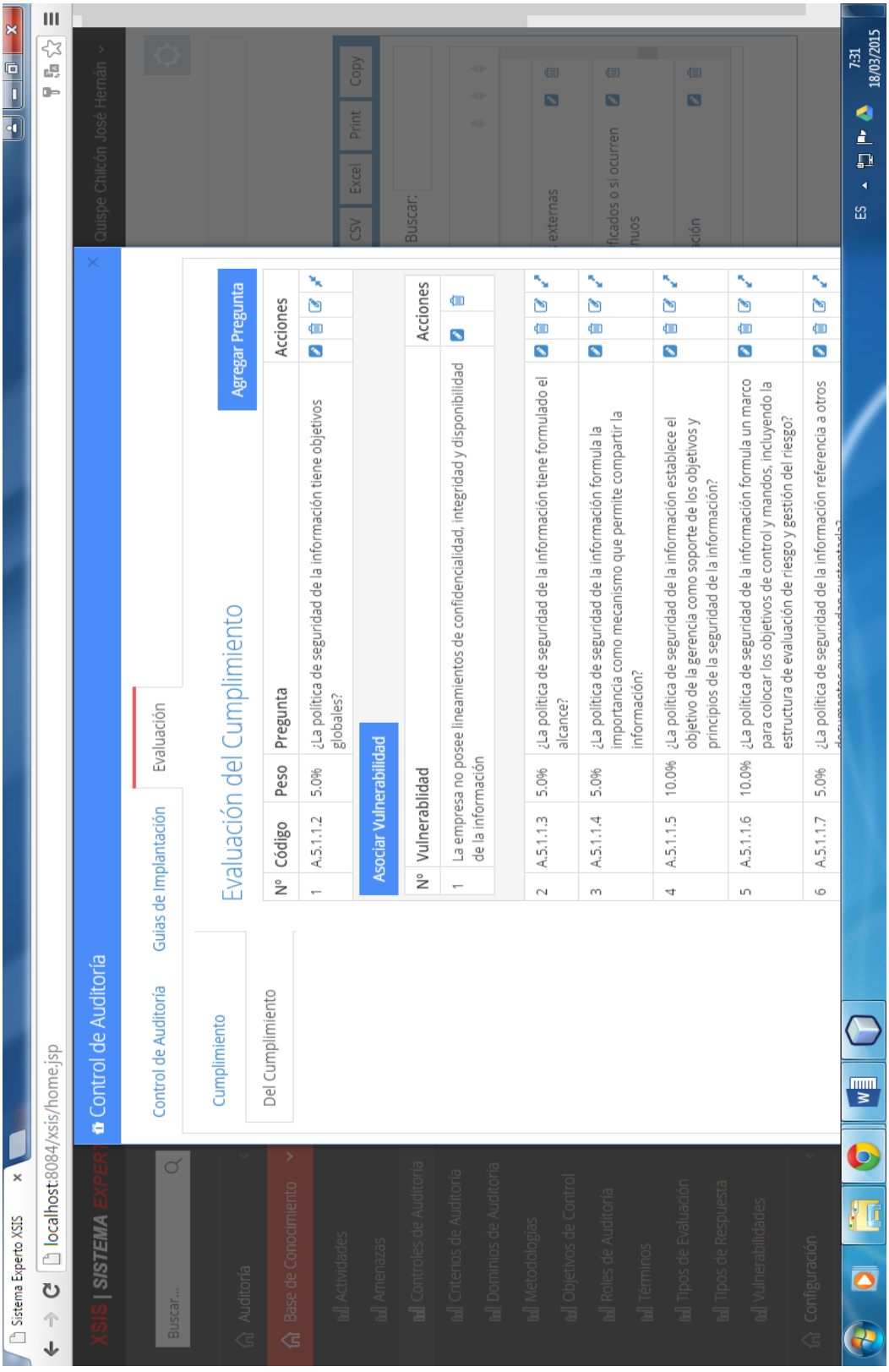
- **Modificar asociación pregunta – vulnerabilidad.**



- **Eliminar asociación pregunta – vulnerabilidad**

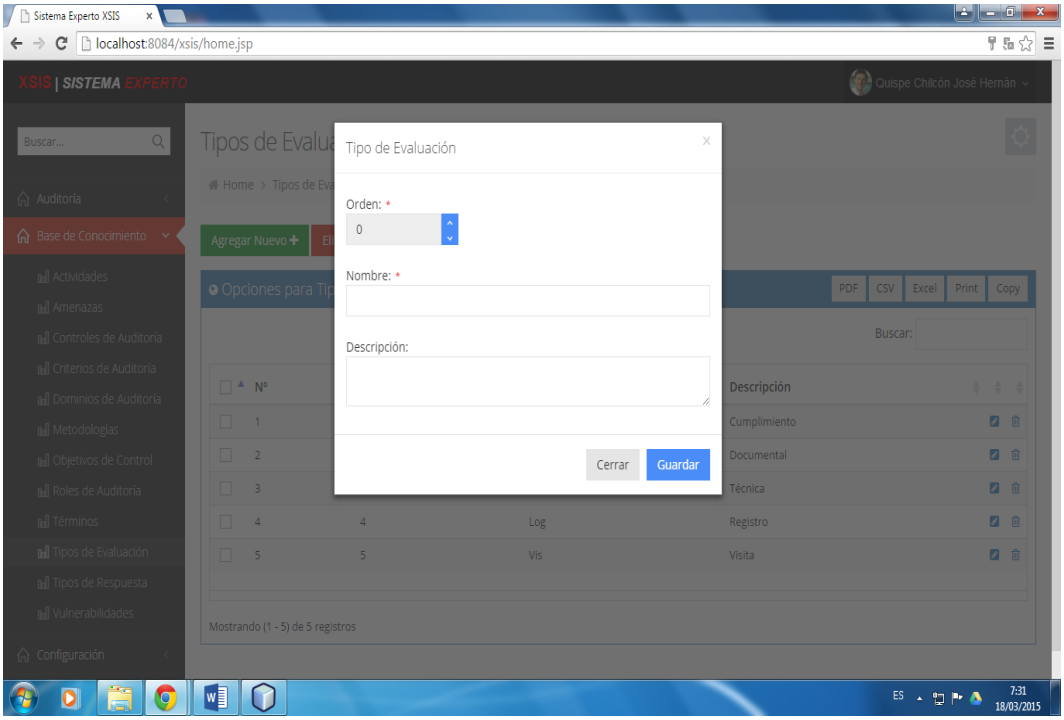


- **Listar vulnerabilidades – pregunta**

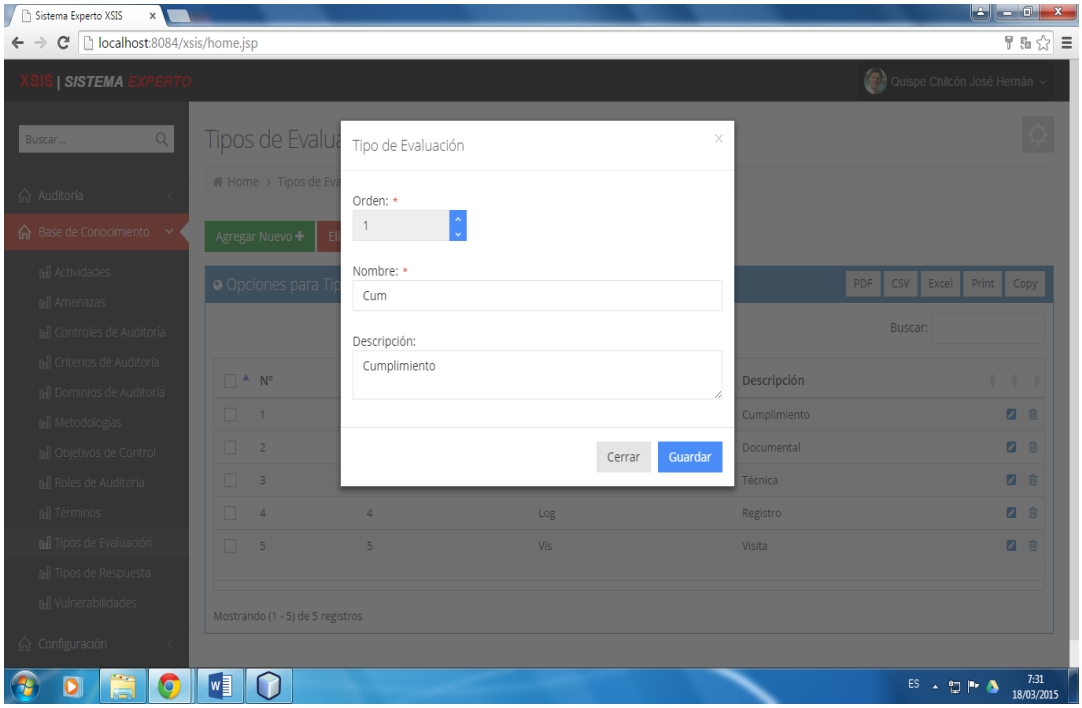


k. Tipos de Evaluación

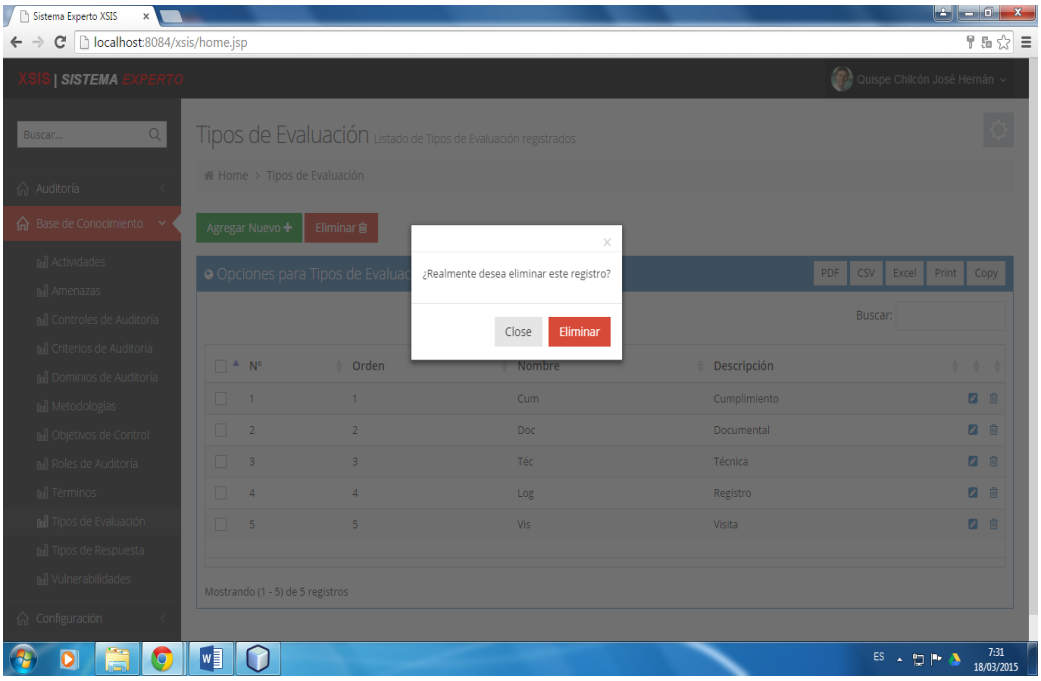
- Registrar tipo evaluación



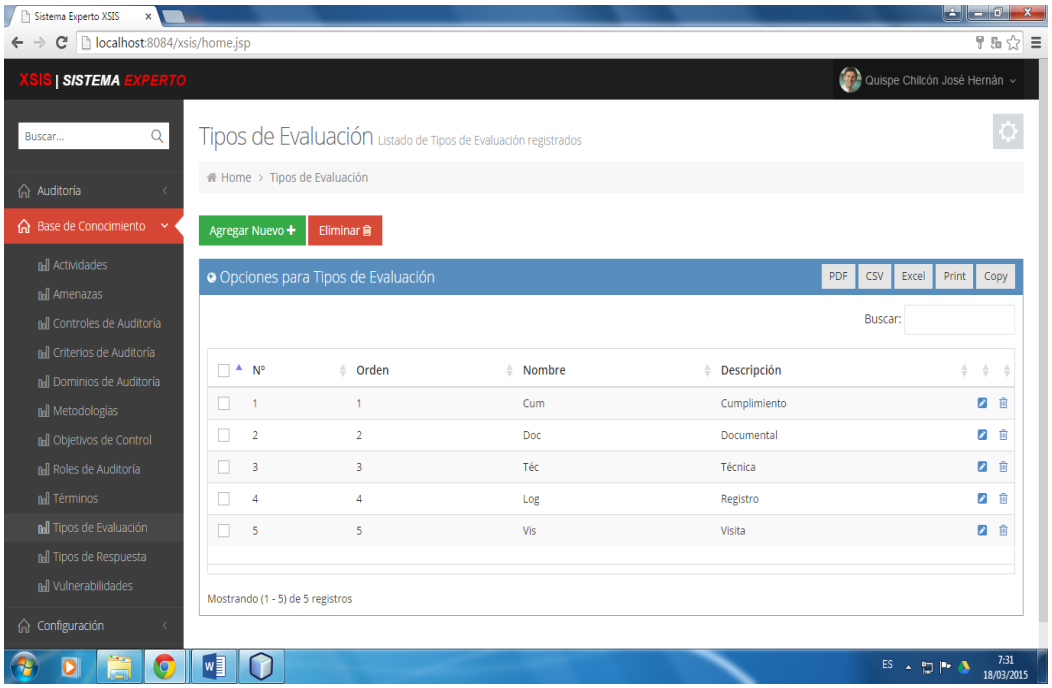
- Modificar tipo evaluación



- **Eliminar tipo evaluación**

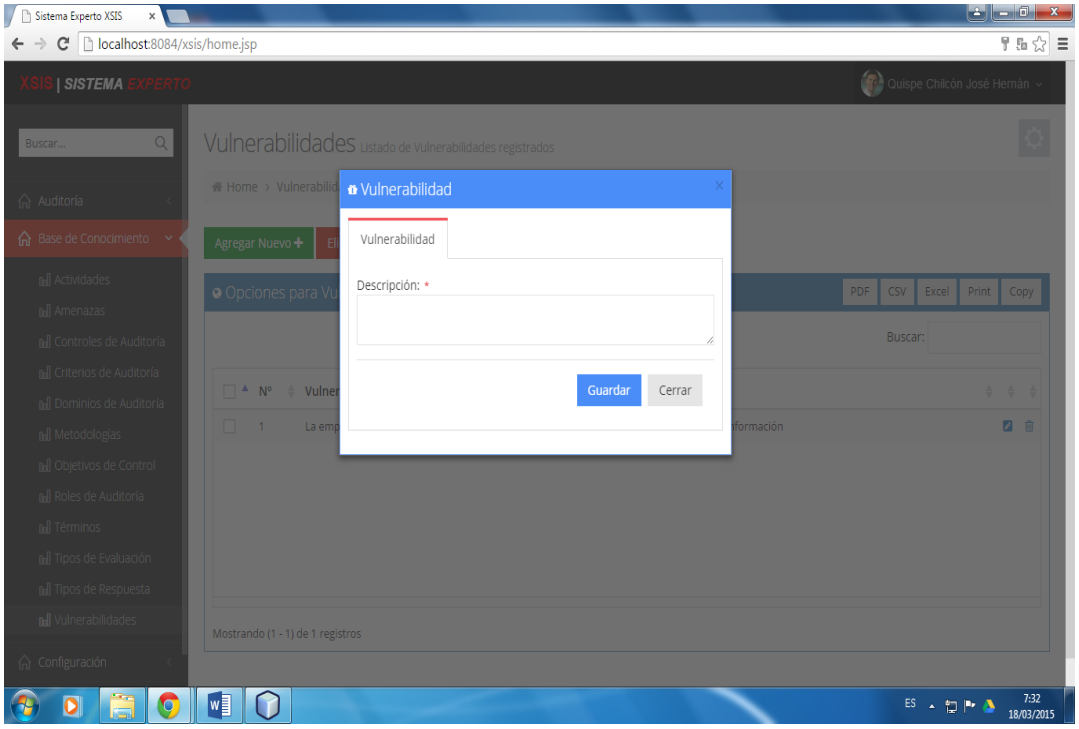


- **Listar tipos de evaluación**

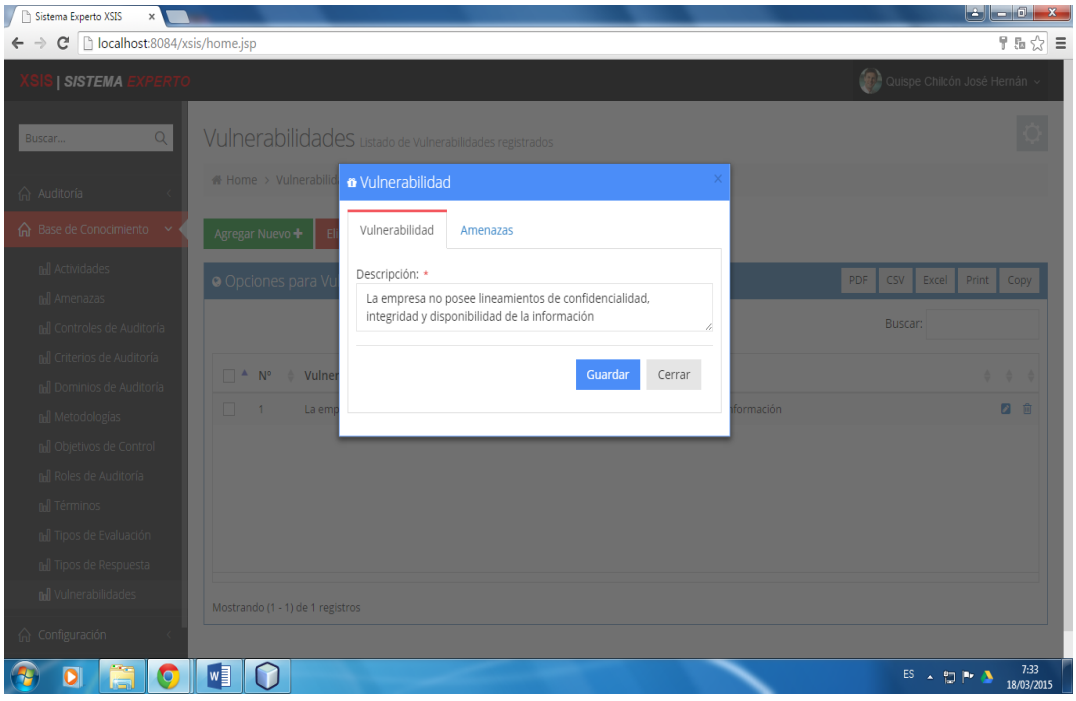


l. Vulnerabilidad

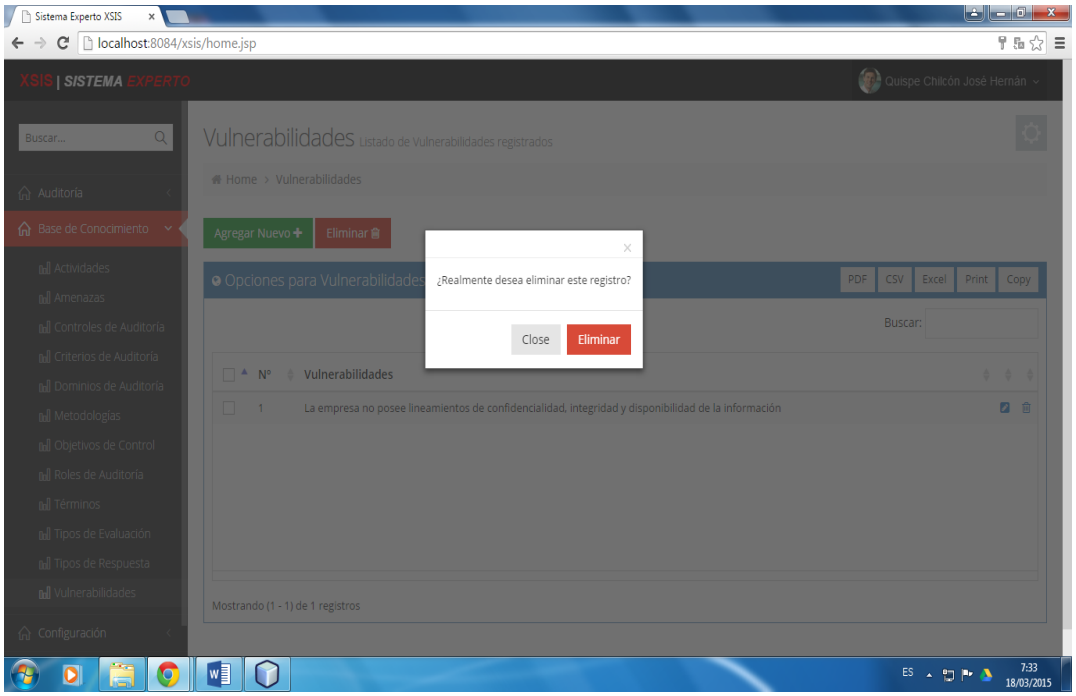
- Registrar vulnerabilidad



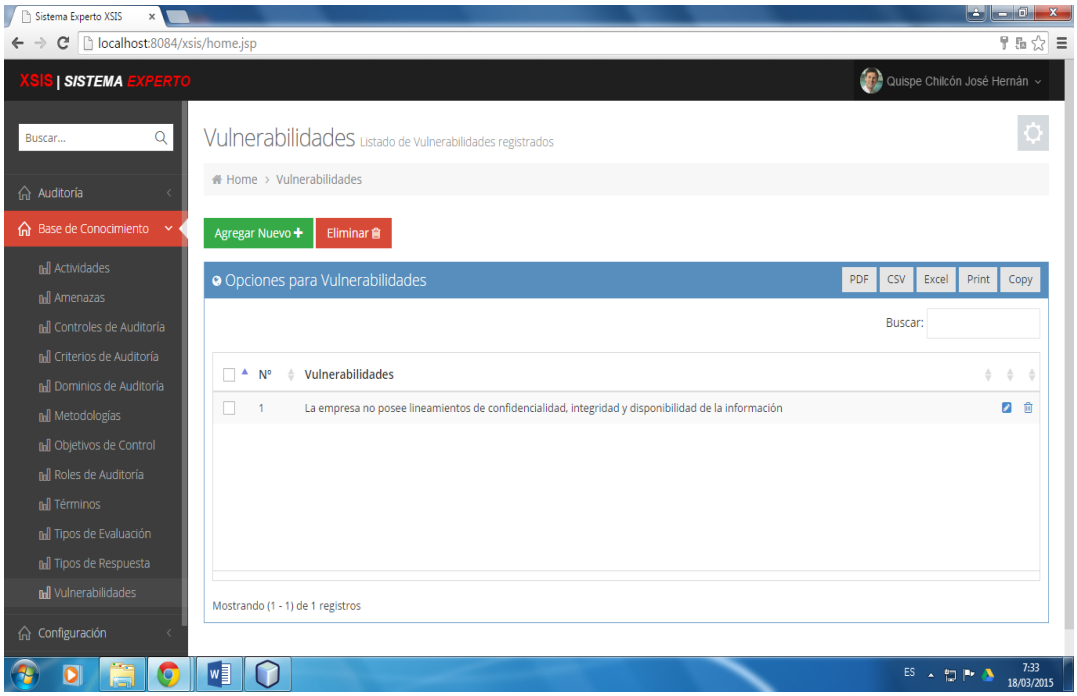
- Modificar vulnerabilidad



- **Eliminar vulnerabilidad**

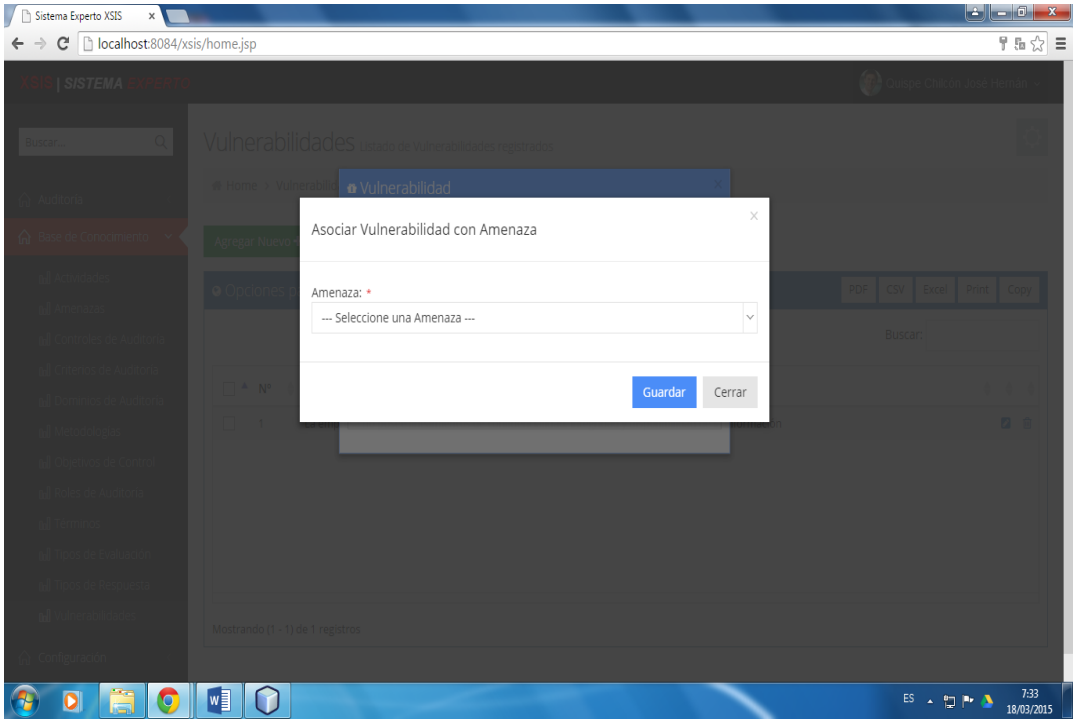


- **Listar vulnerabilidades**

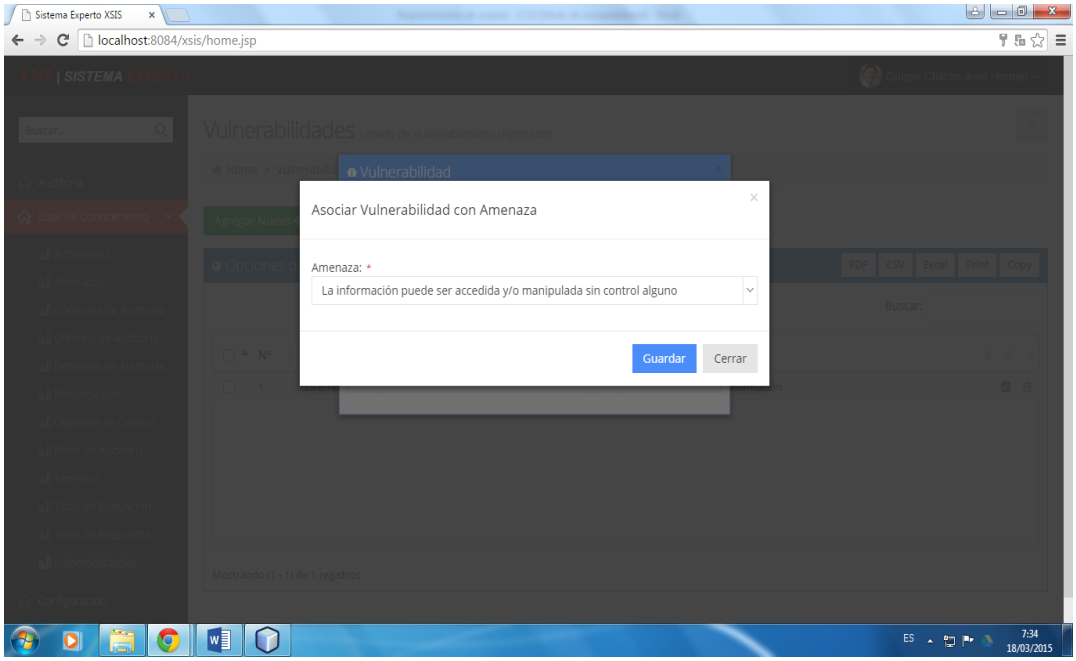


m. Vulnerabilidad - Amenaza

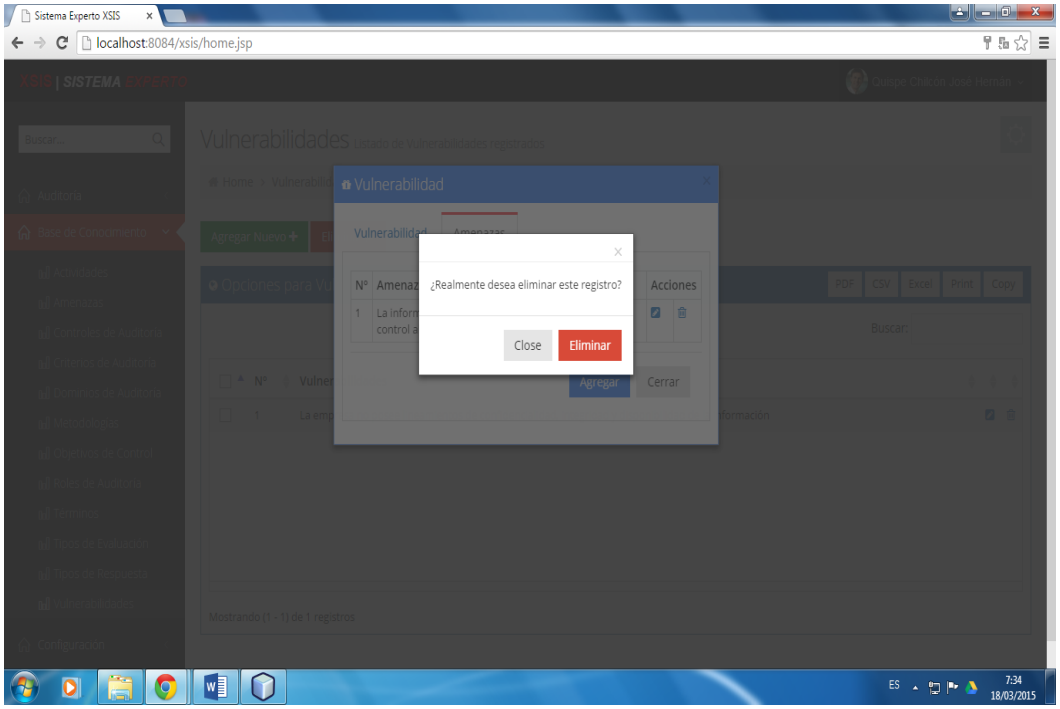
- **Asociar vulnerabilidad amenaza**



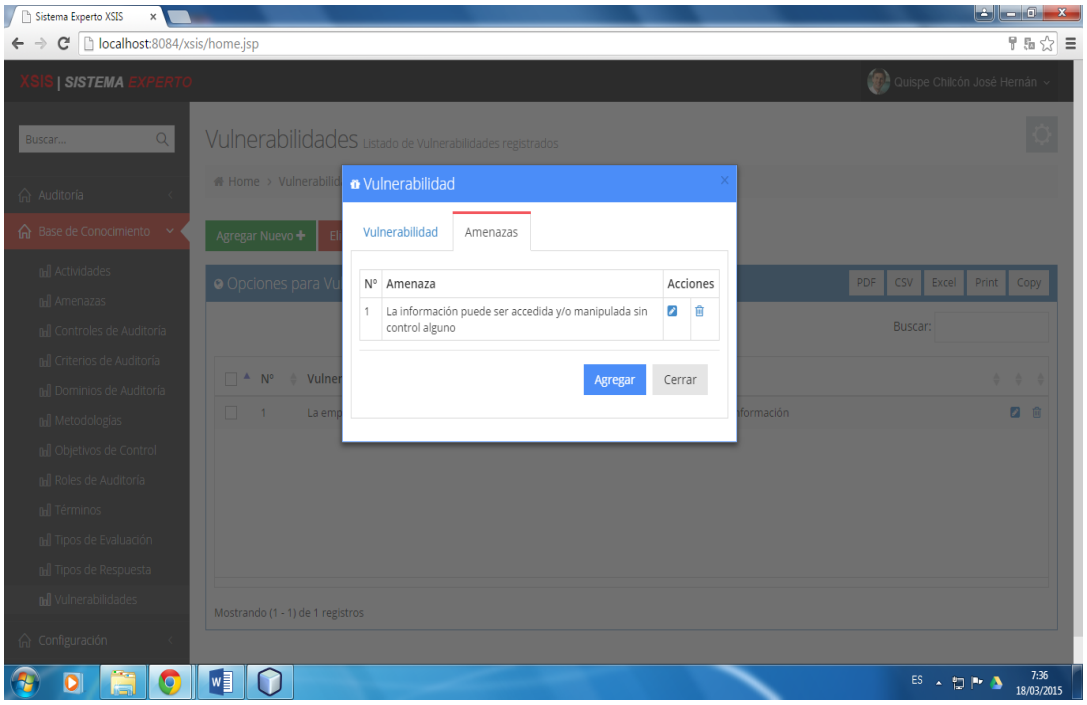
- **Modificar asociación vulnerabilidad – amenaza**



- **Eliminar asociación vulnerabilidad – amenaza**

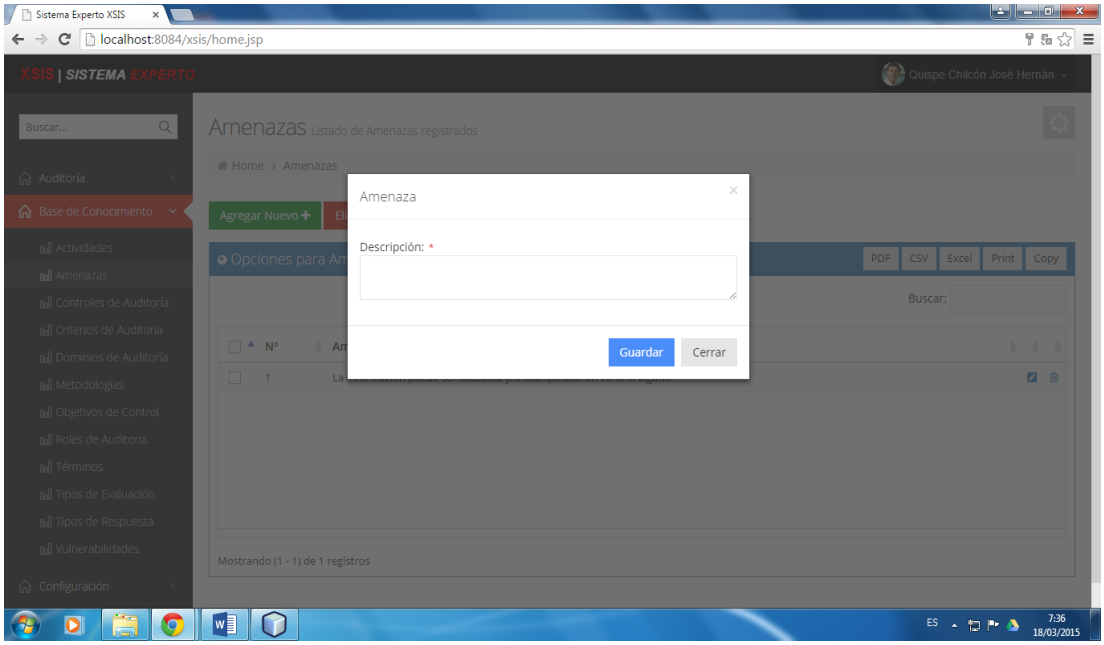


- **Listar vulnerabilidades – amenazas**

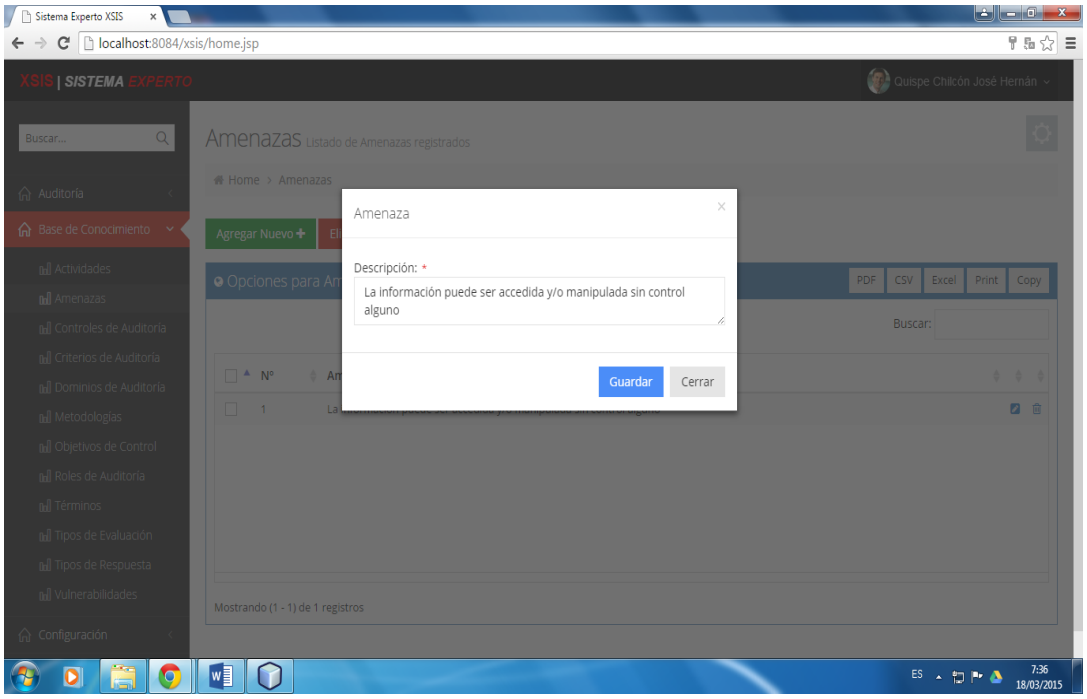


n. Amenazas

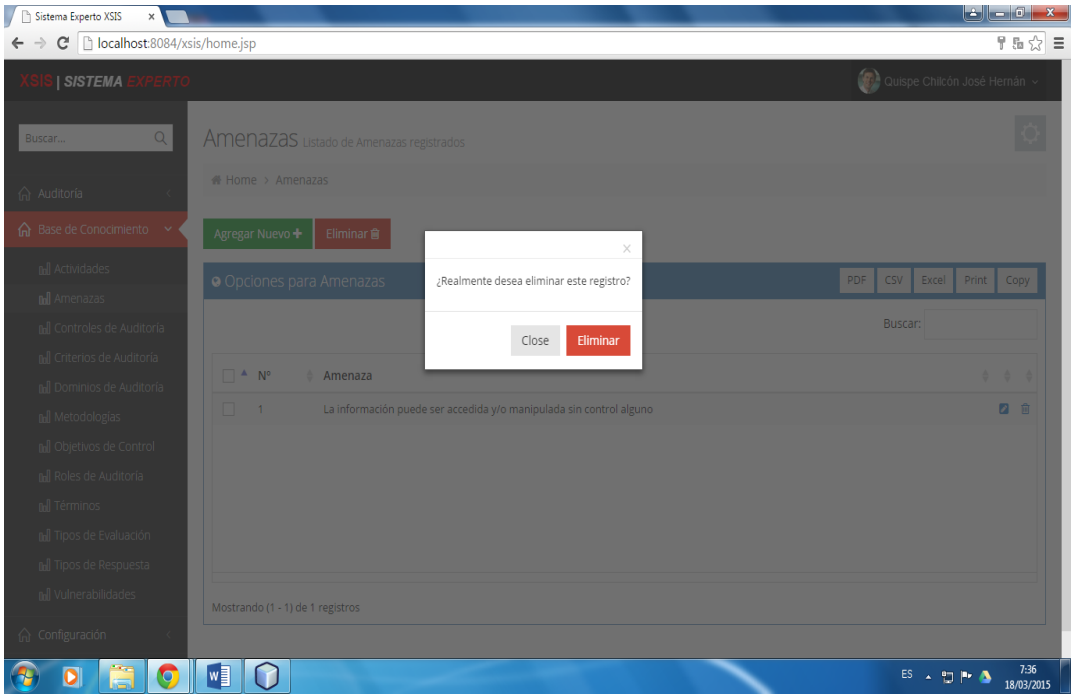
- Registrar amenaza



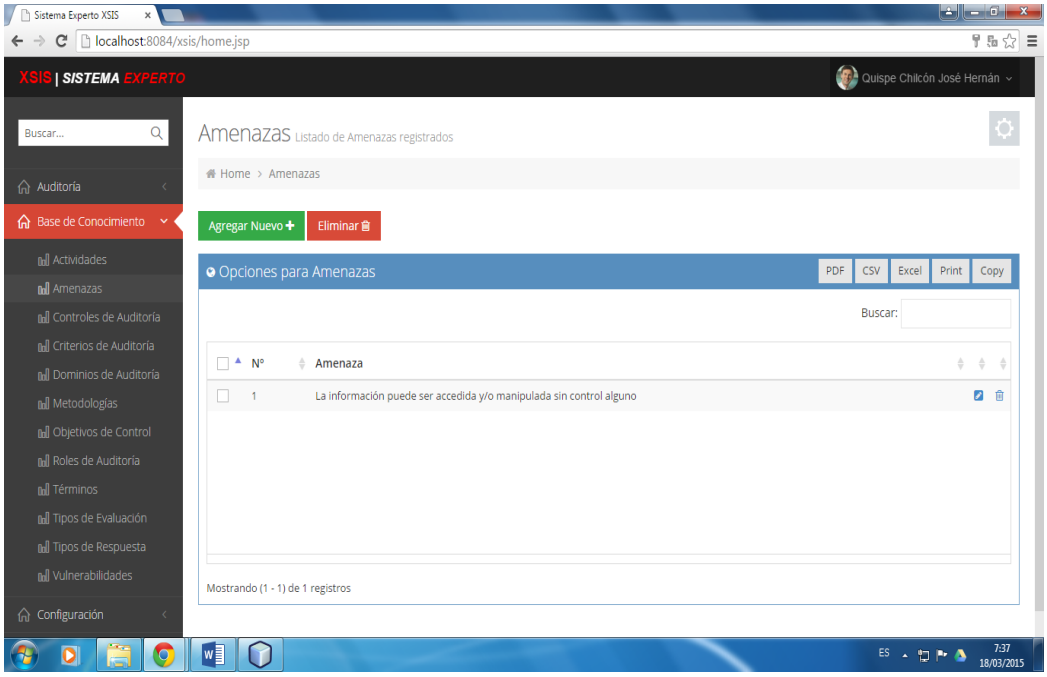
- Modificar amenaza



- **Eliminar amenaza**

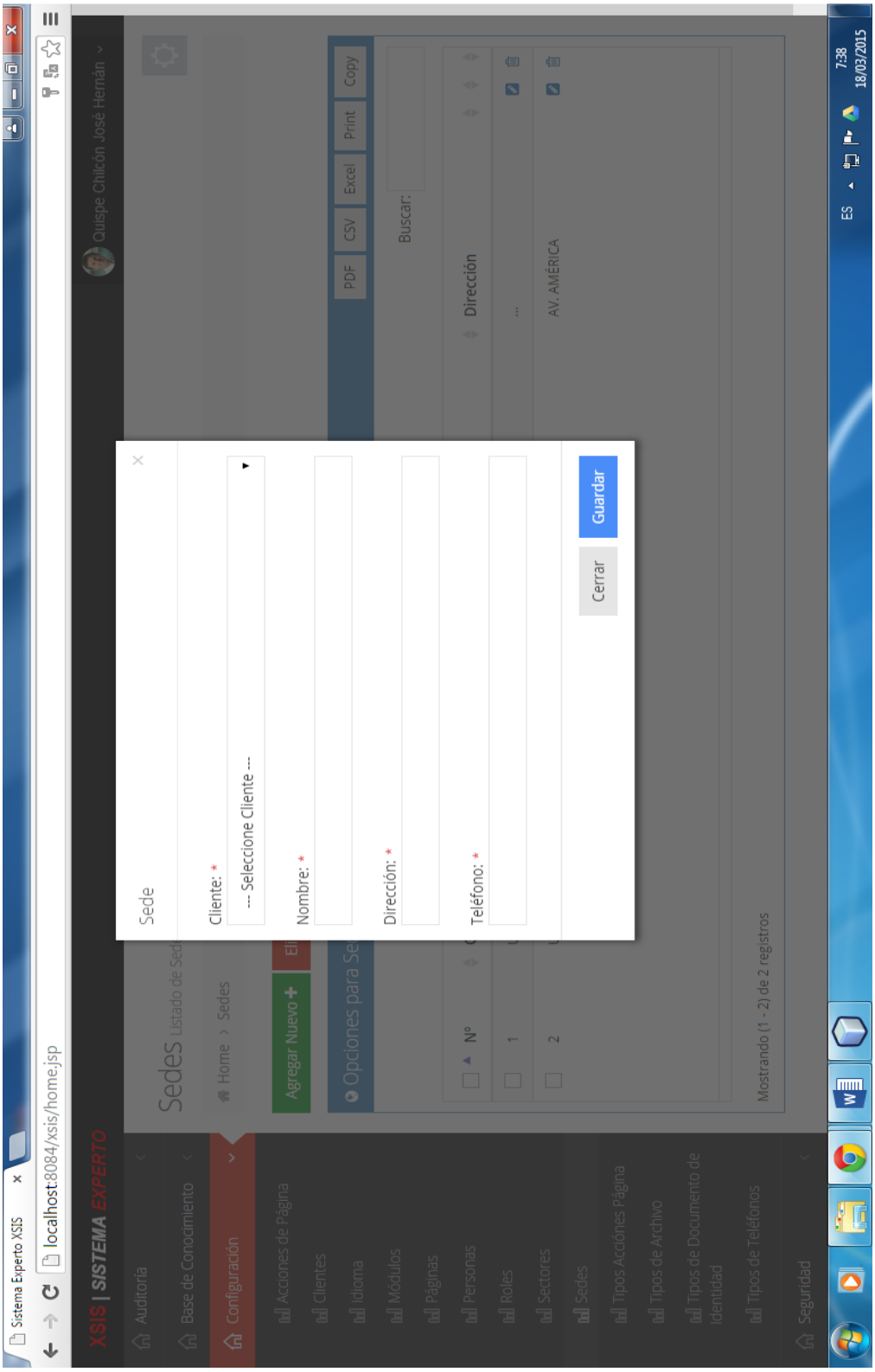


- **Listar amenazas**

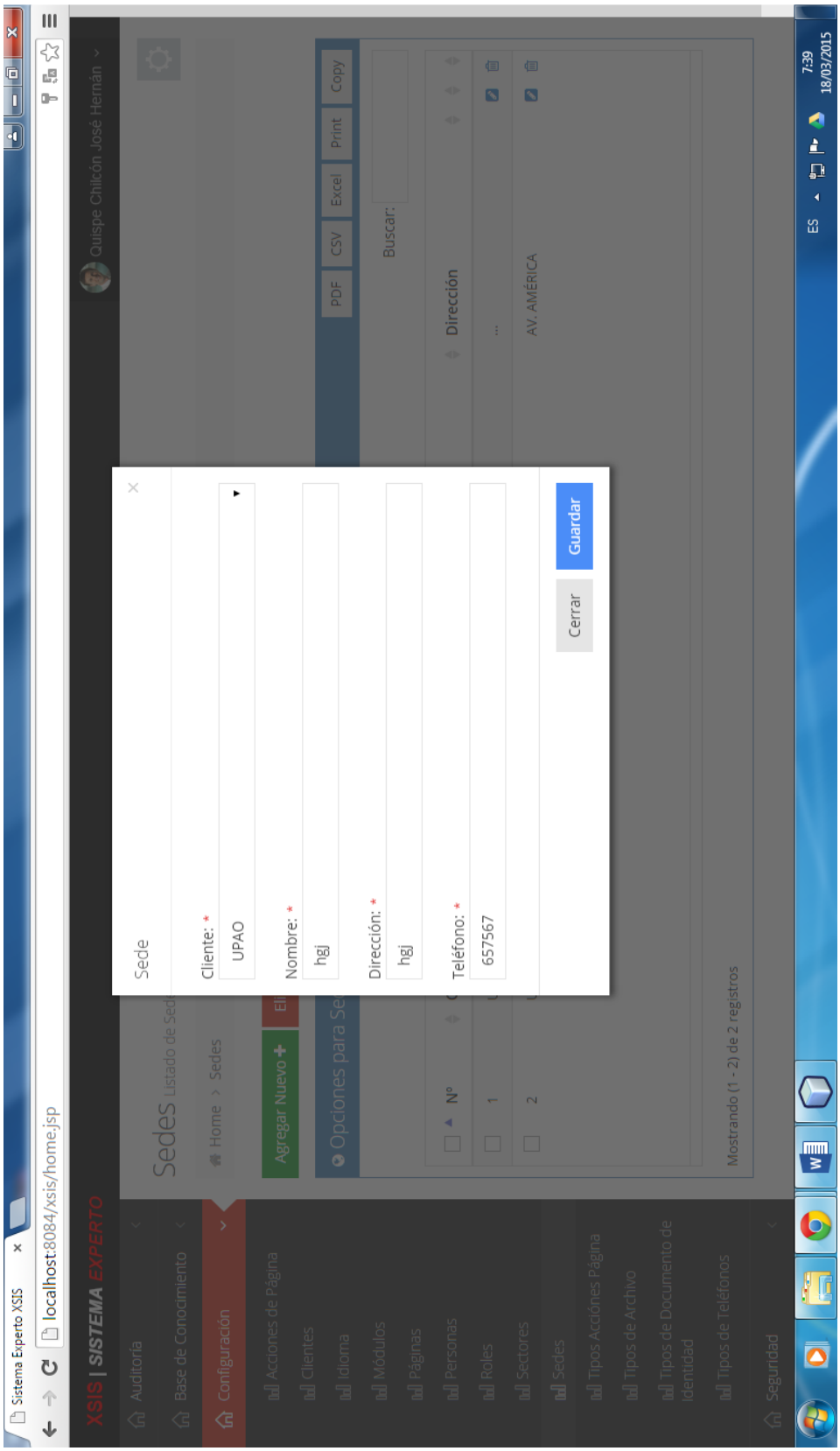


Módulo Auditoría

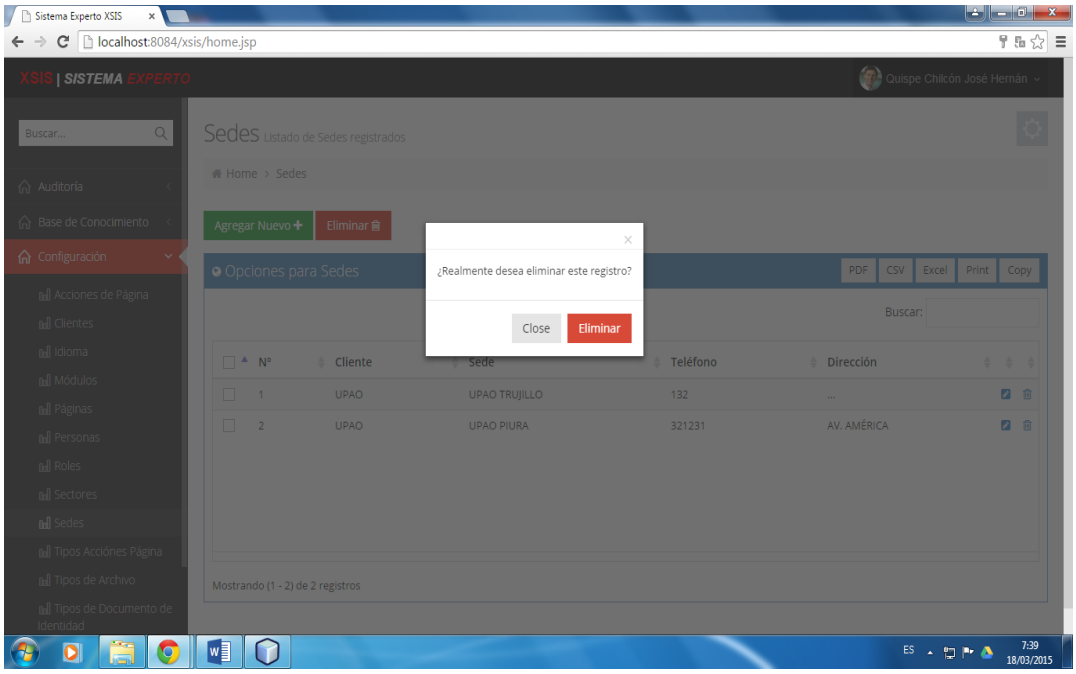
- **Registrar sedes**



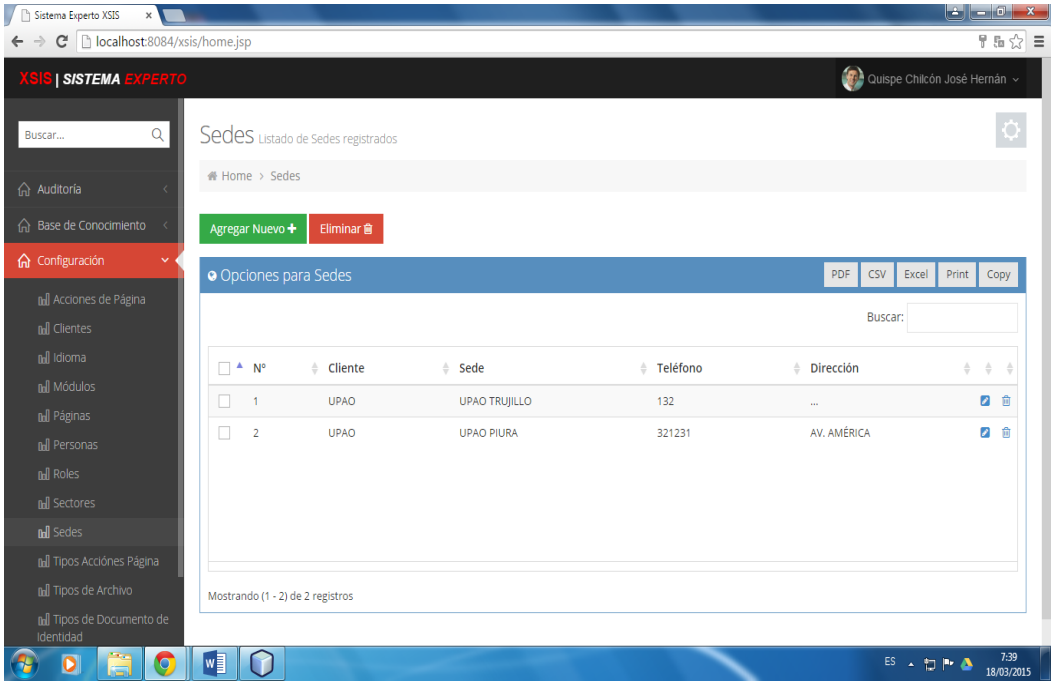
- **Modificar sede**



- **Eliminar sede**



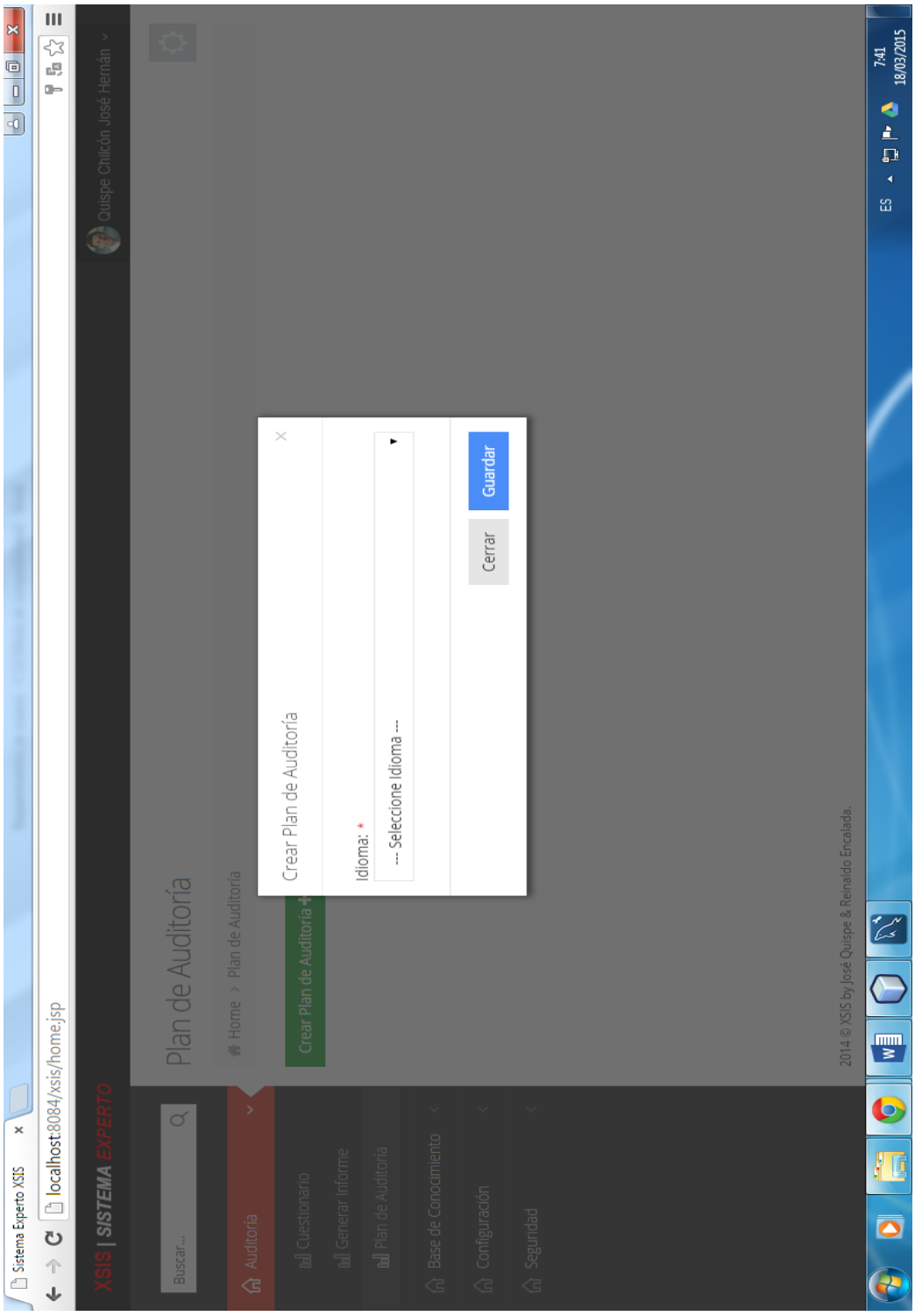
- **Listar sedes**



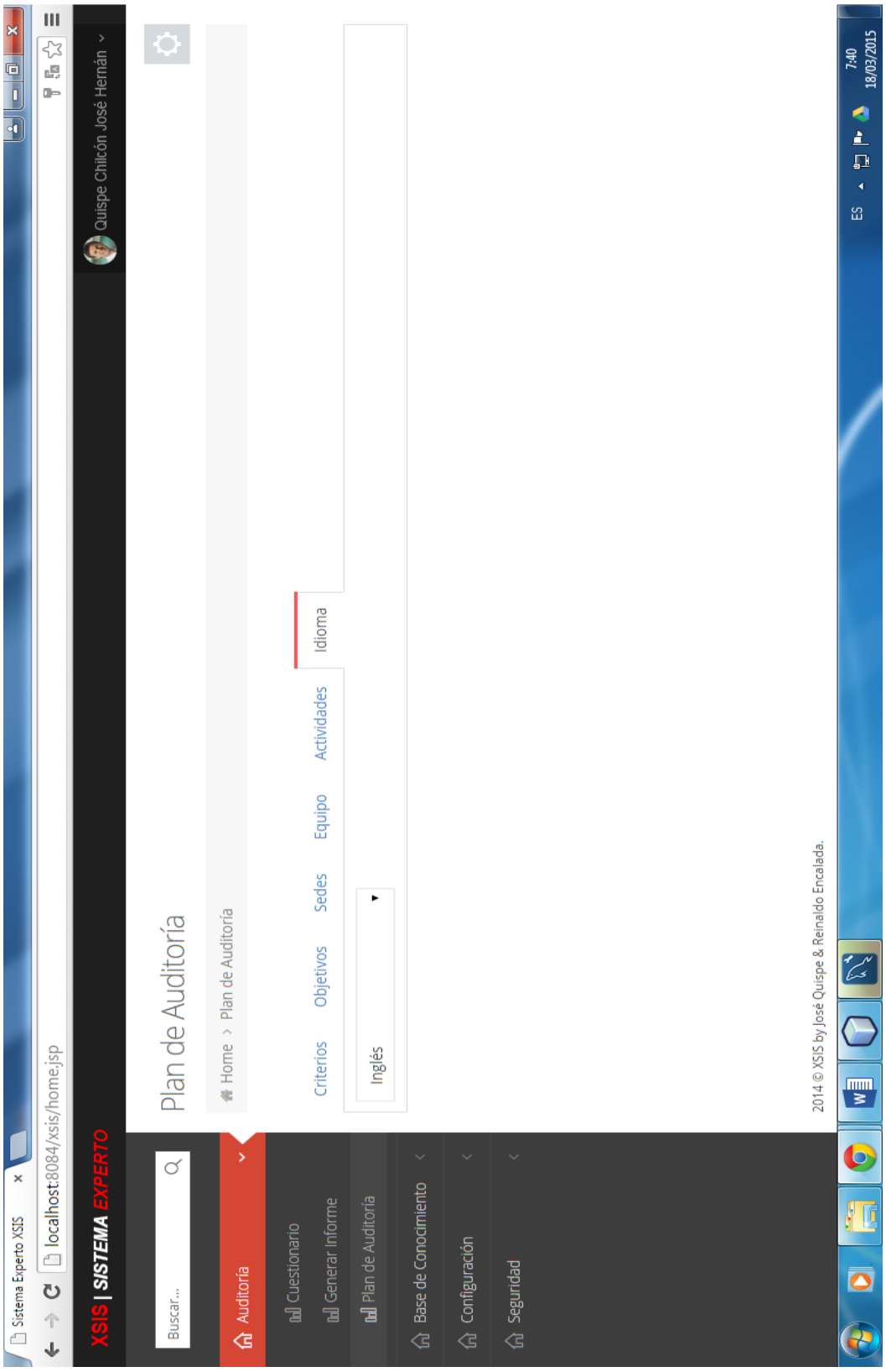
Módulo Auditoría

a. Plan auditoría

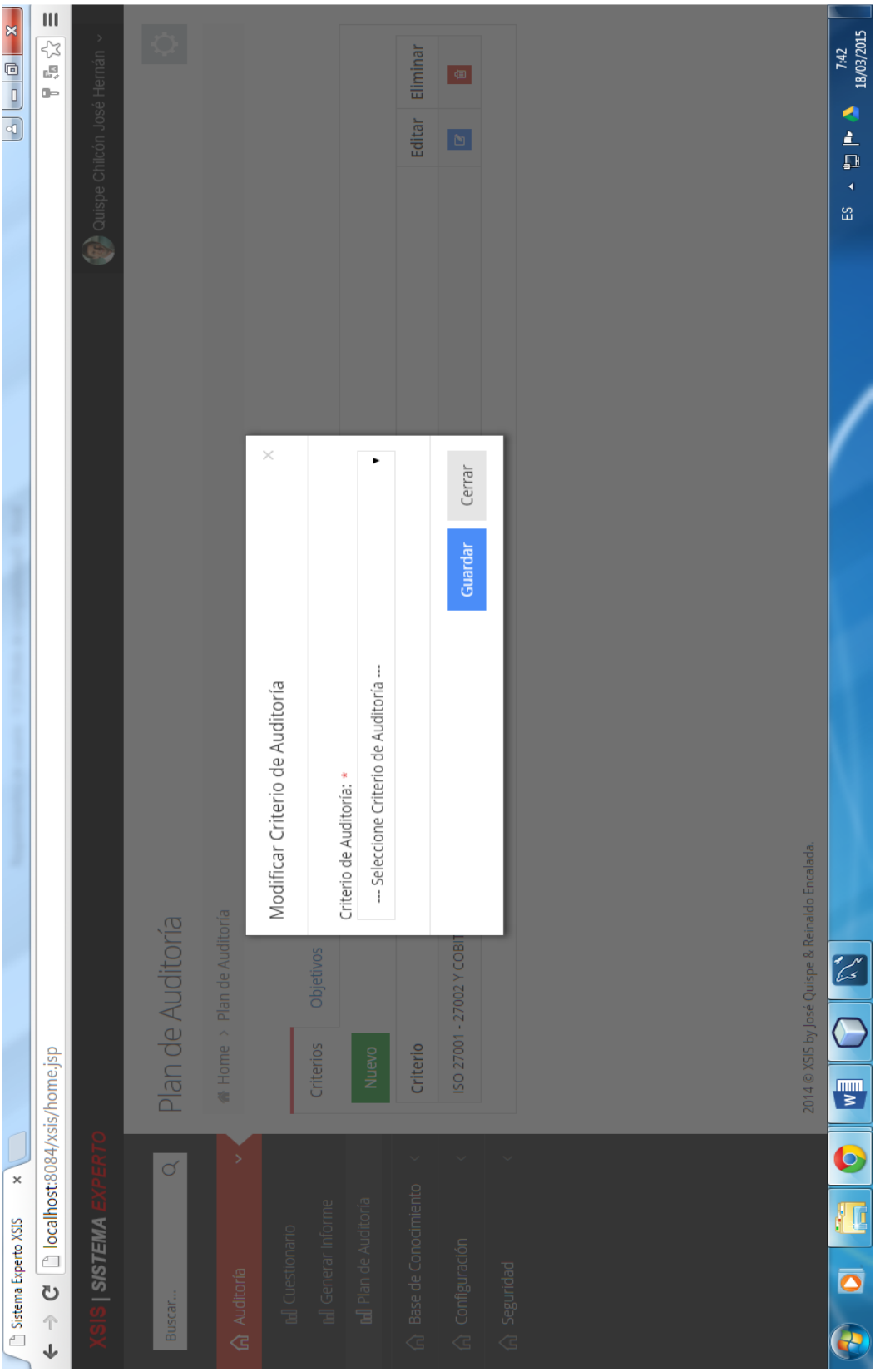
- **Crear plan auditoría**



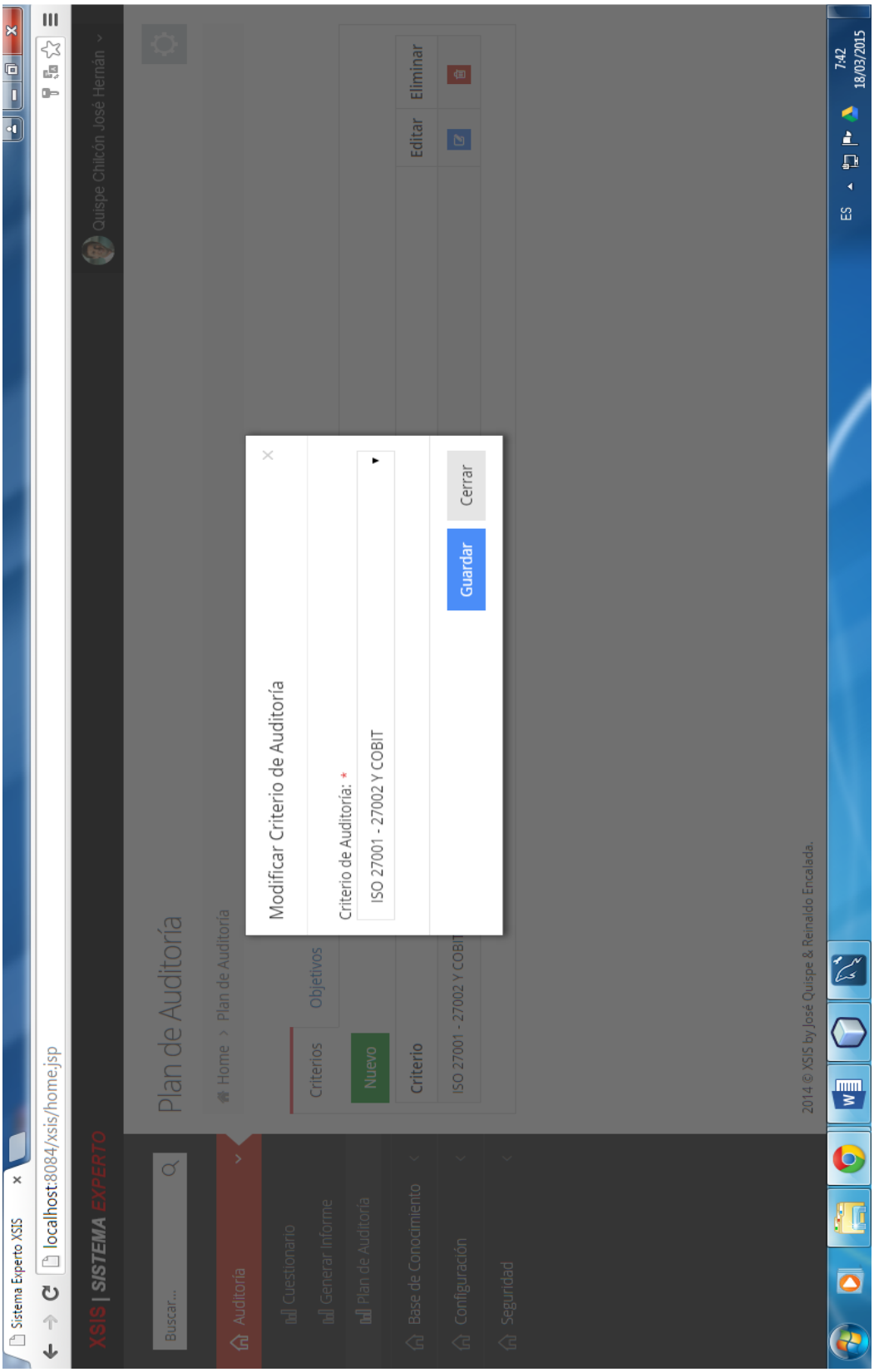
- **Modificar idioma plan auditoría**



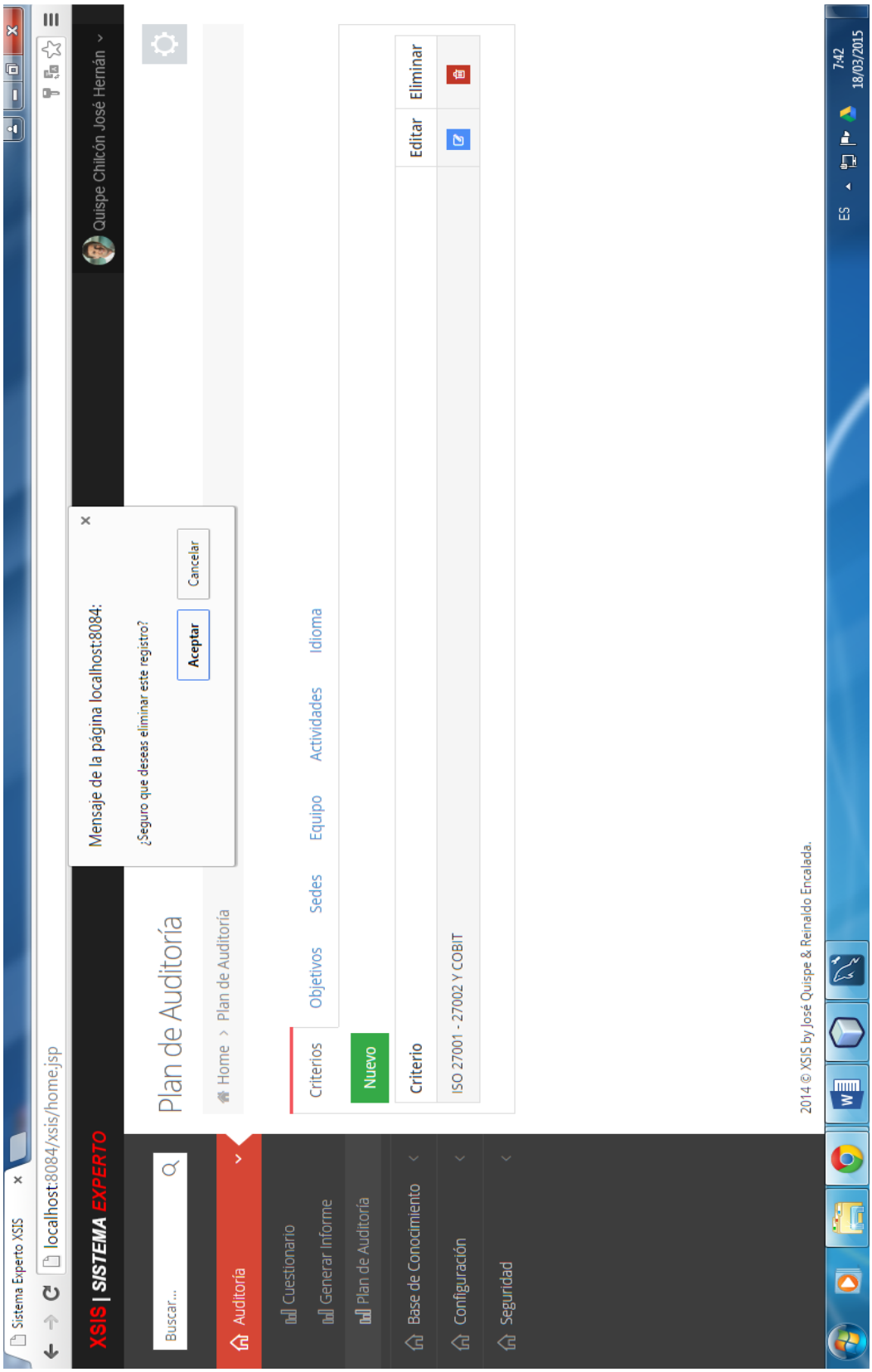
- **Registrar criterio - plan auditoría**



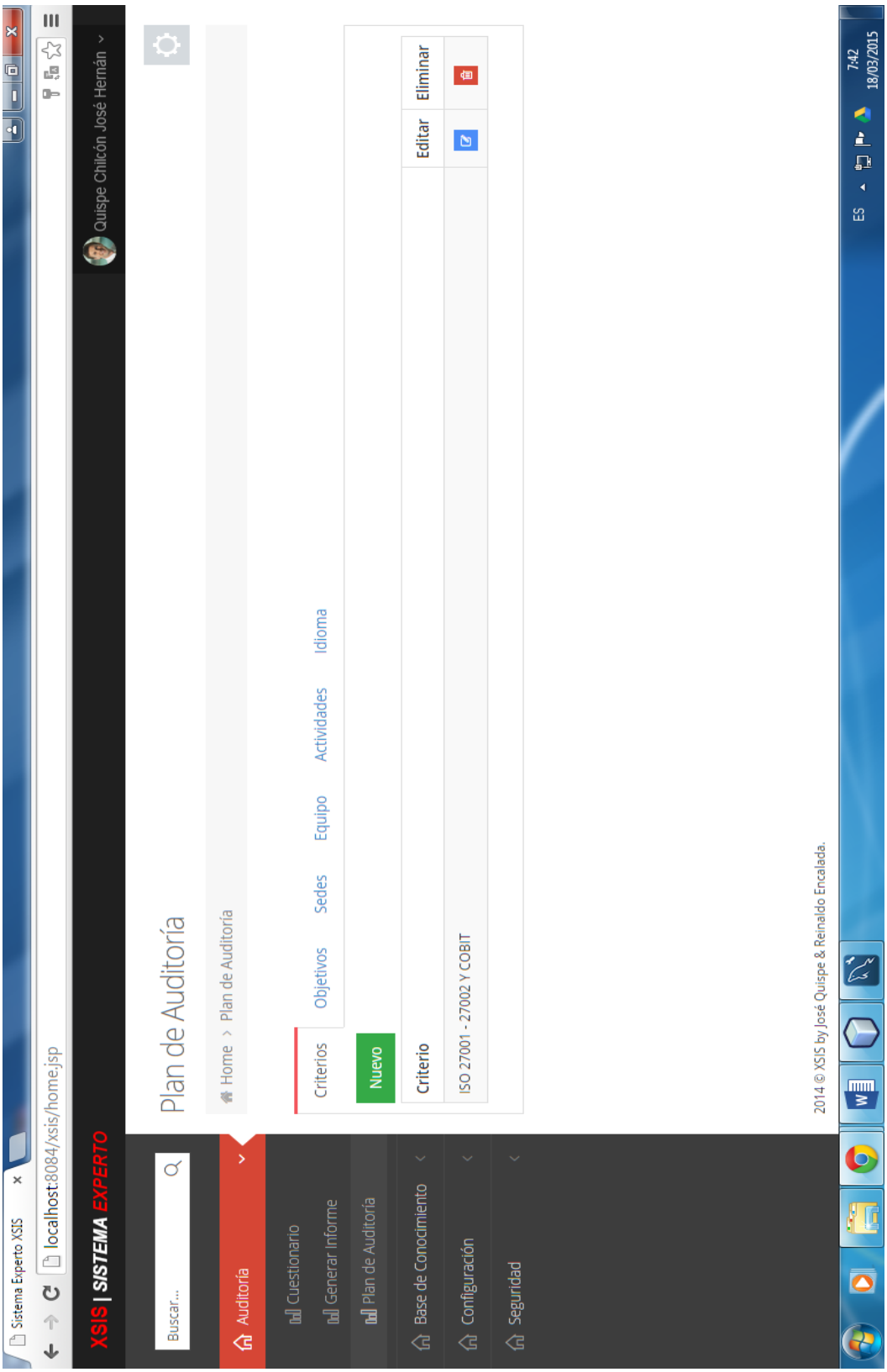
- **Modificar criterio – plan auditoría**



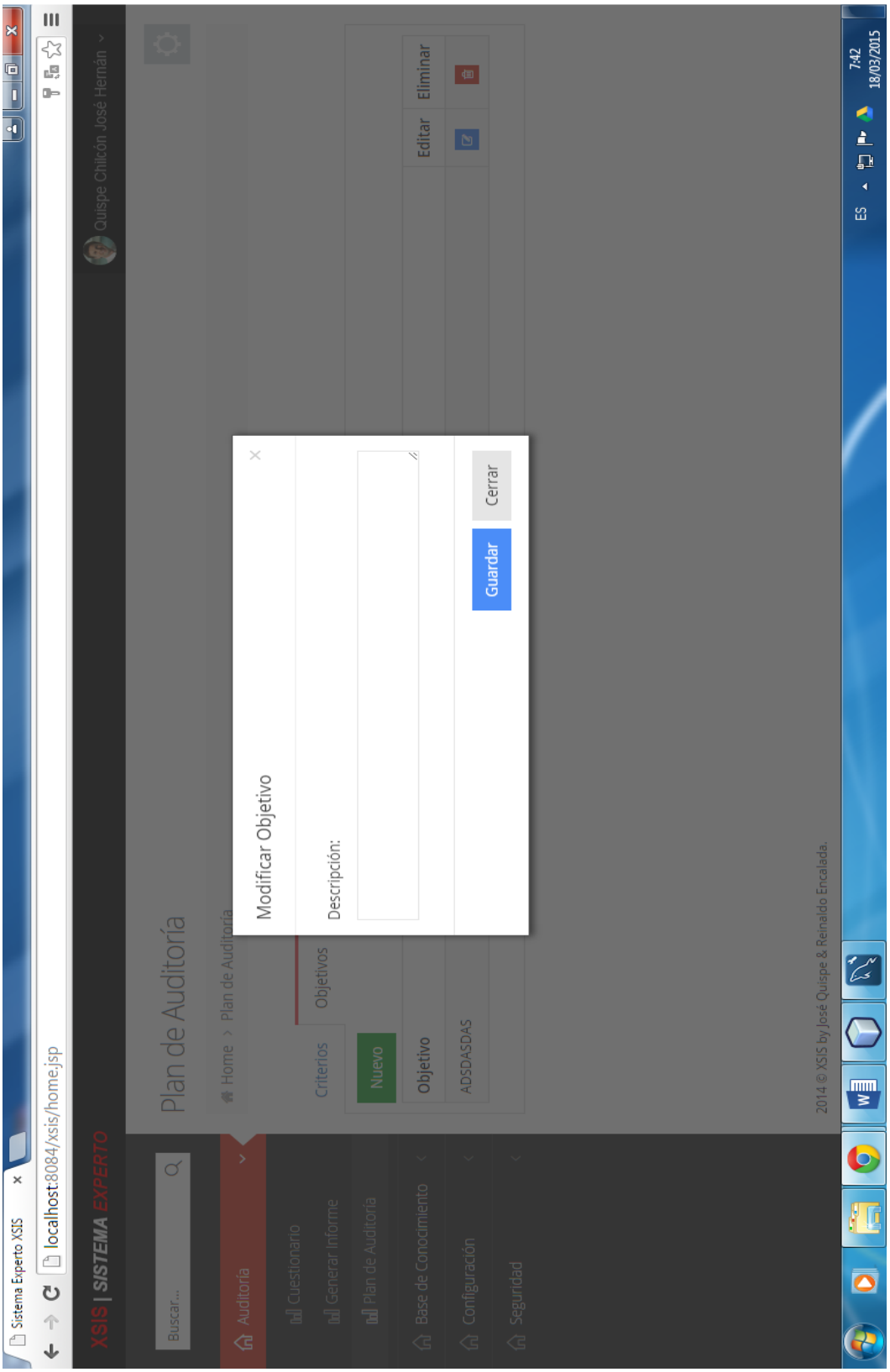
- **Eliminar criterio – plan auditoría**



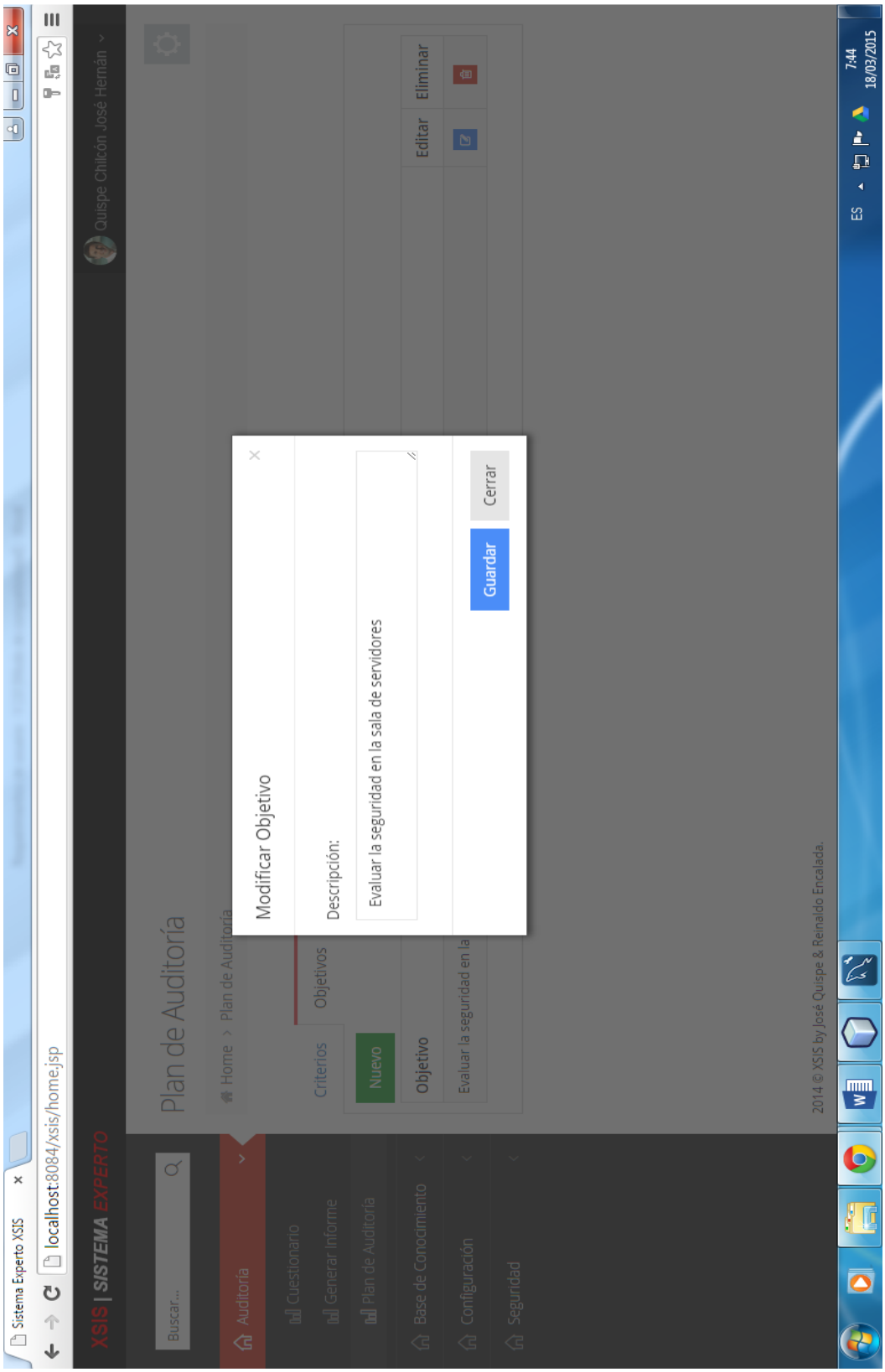
- **Listar criterios – plan auditoría**



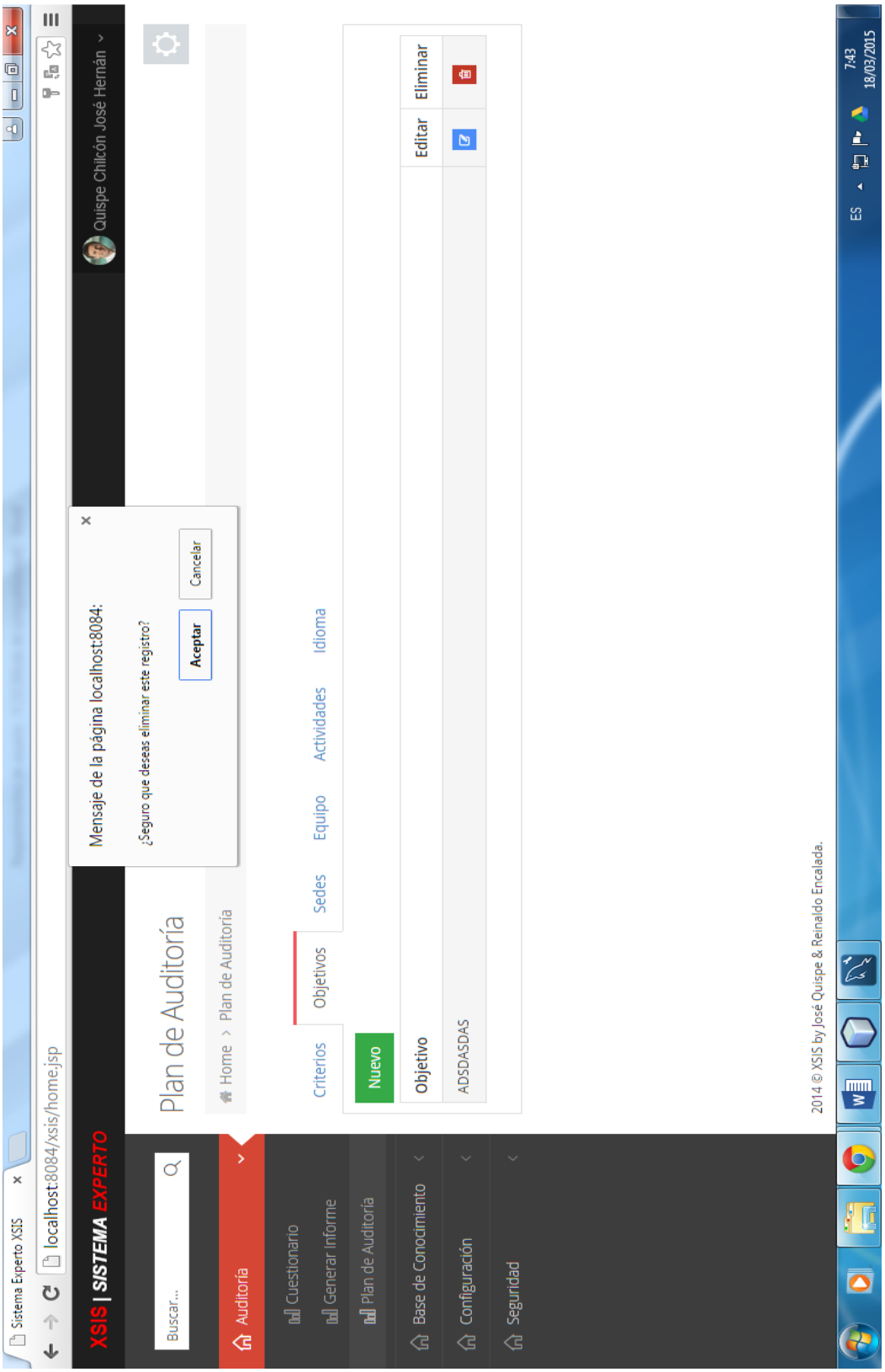
- **Registrar objetivo del plan auditoría**



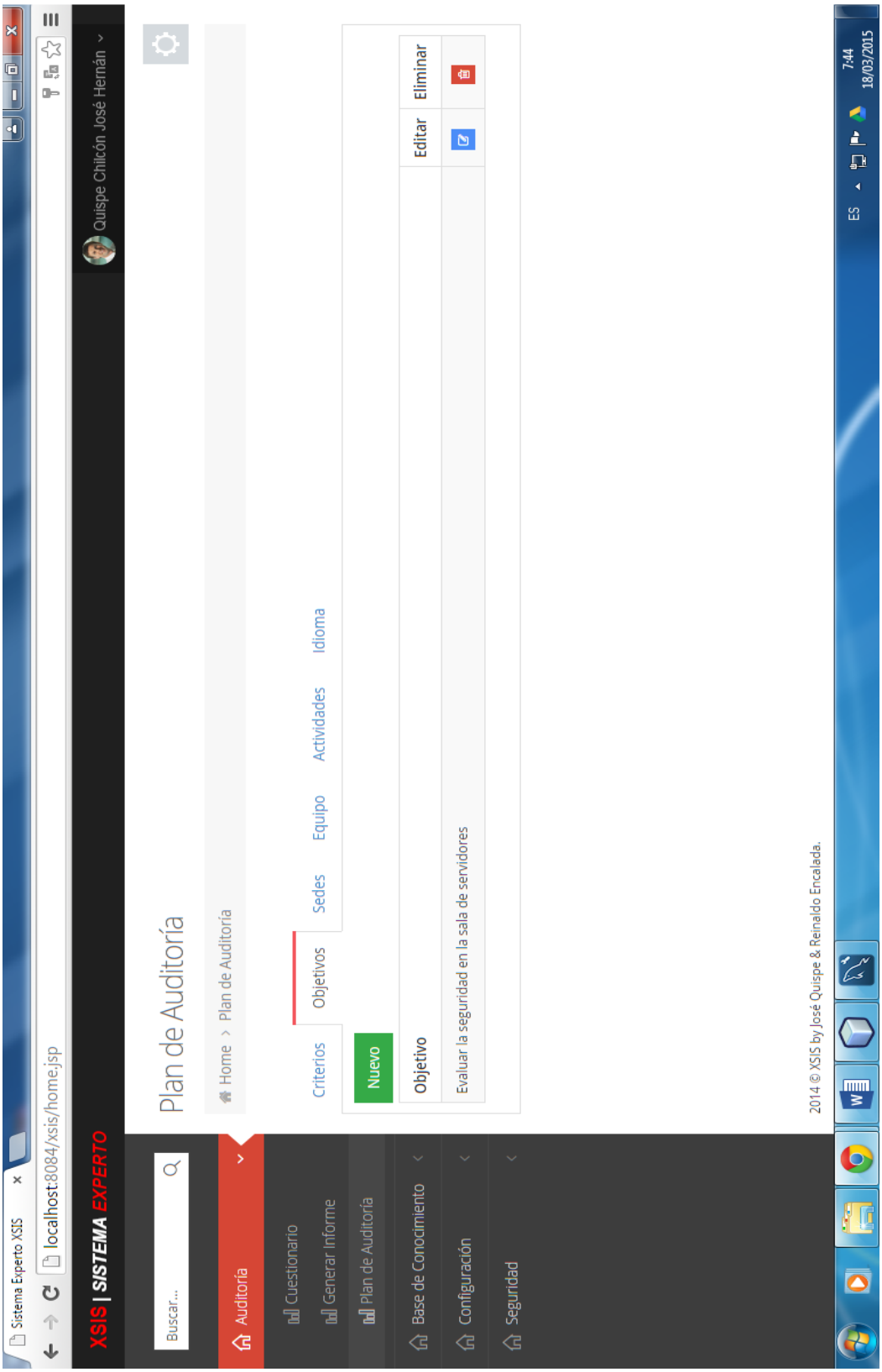
- **Modificar objetivo del plan auditoría**



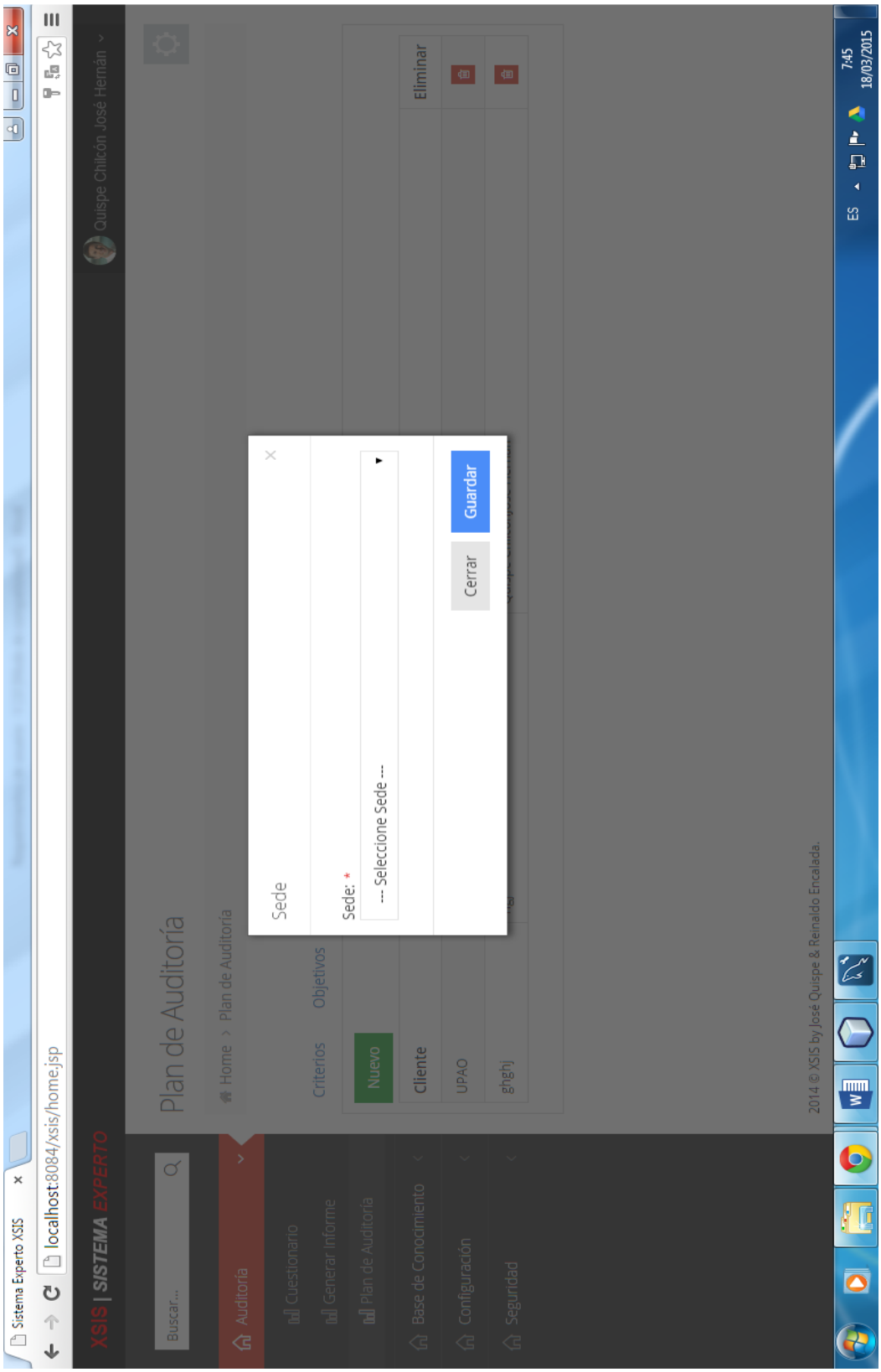
- **Eliminar objetivo del plan de auditoría**



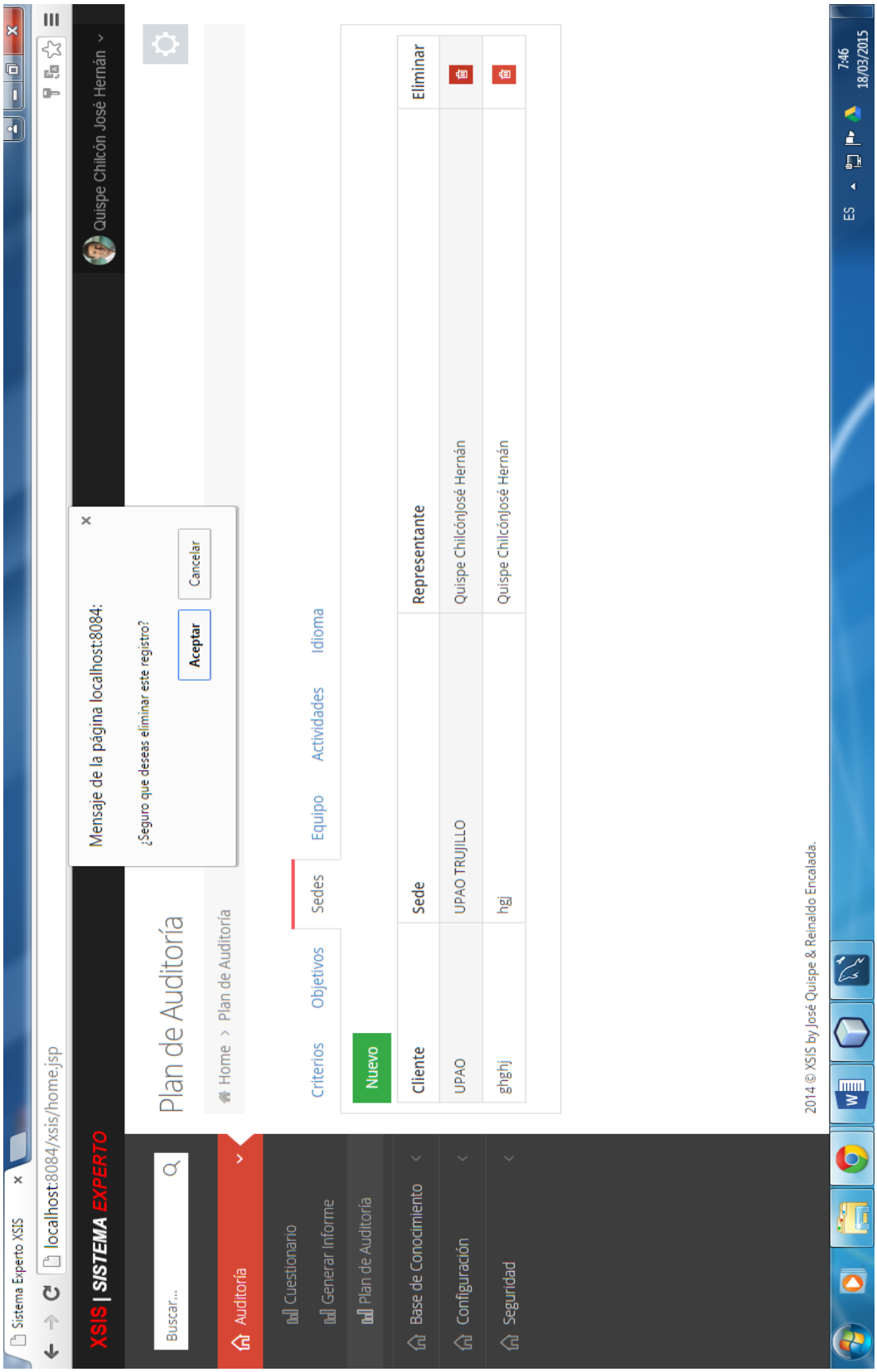
- **Listar objetivos del plan de auditoría**



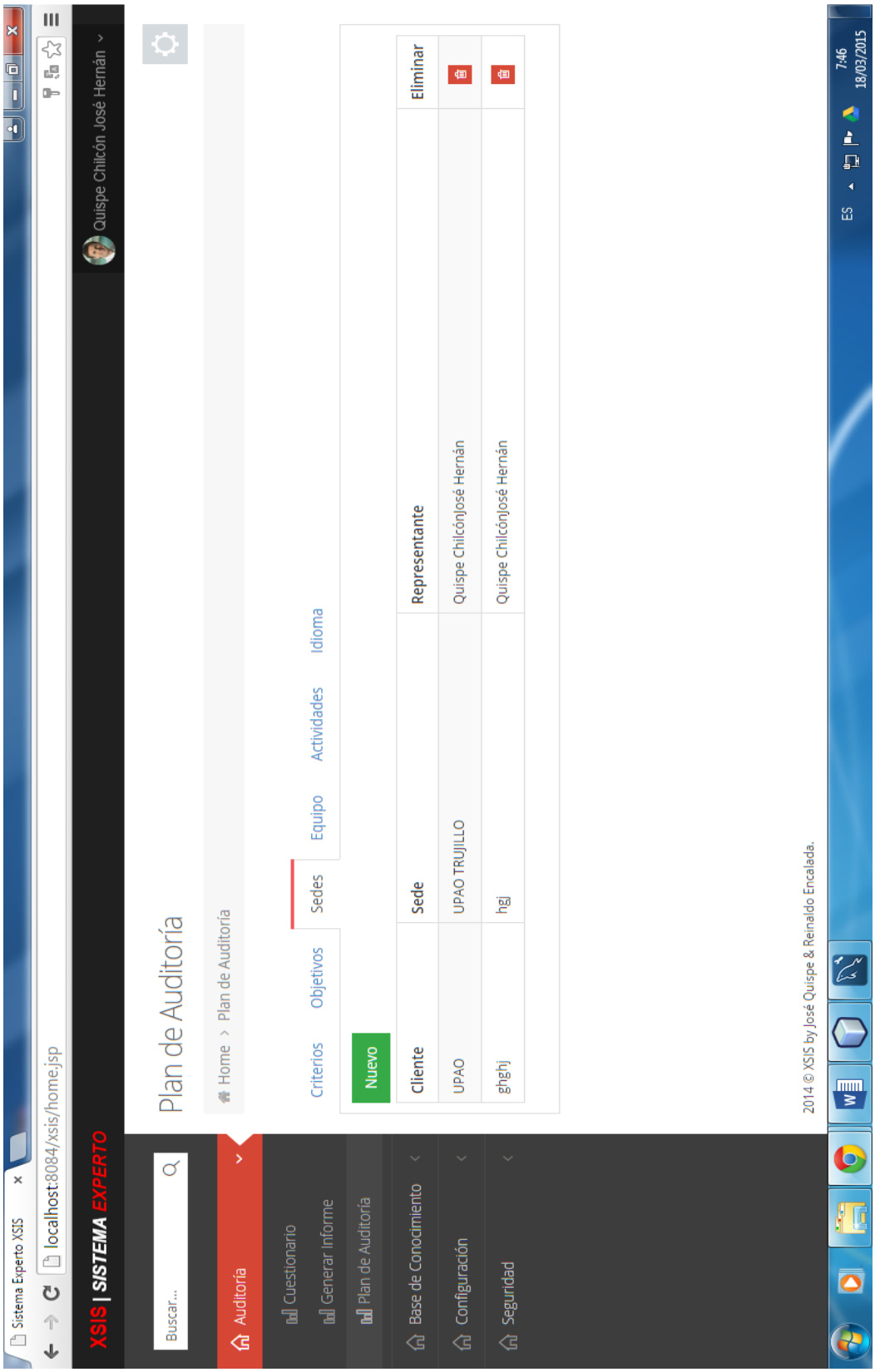
- **Registrar sede – plan auditoría**



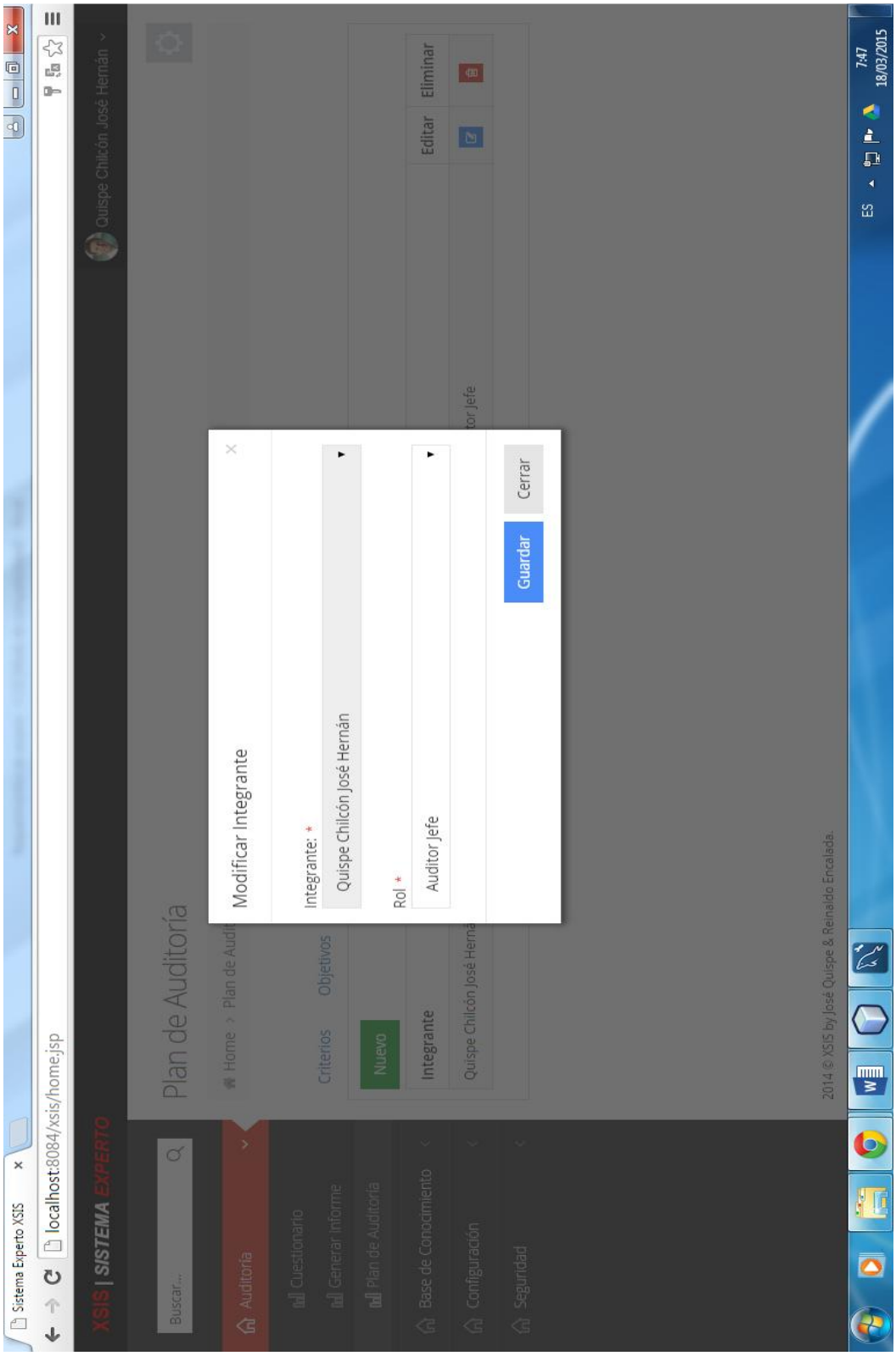
- **Eliminar sede – plan auditoría**



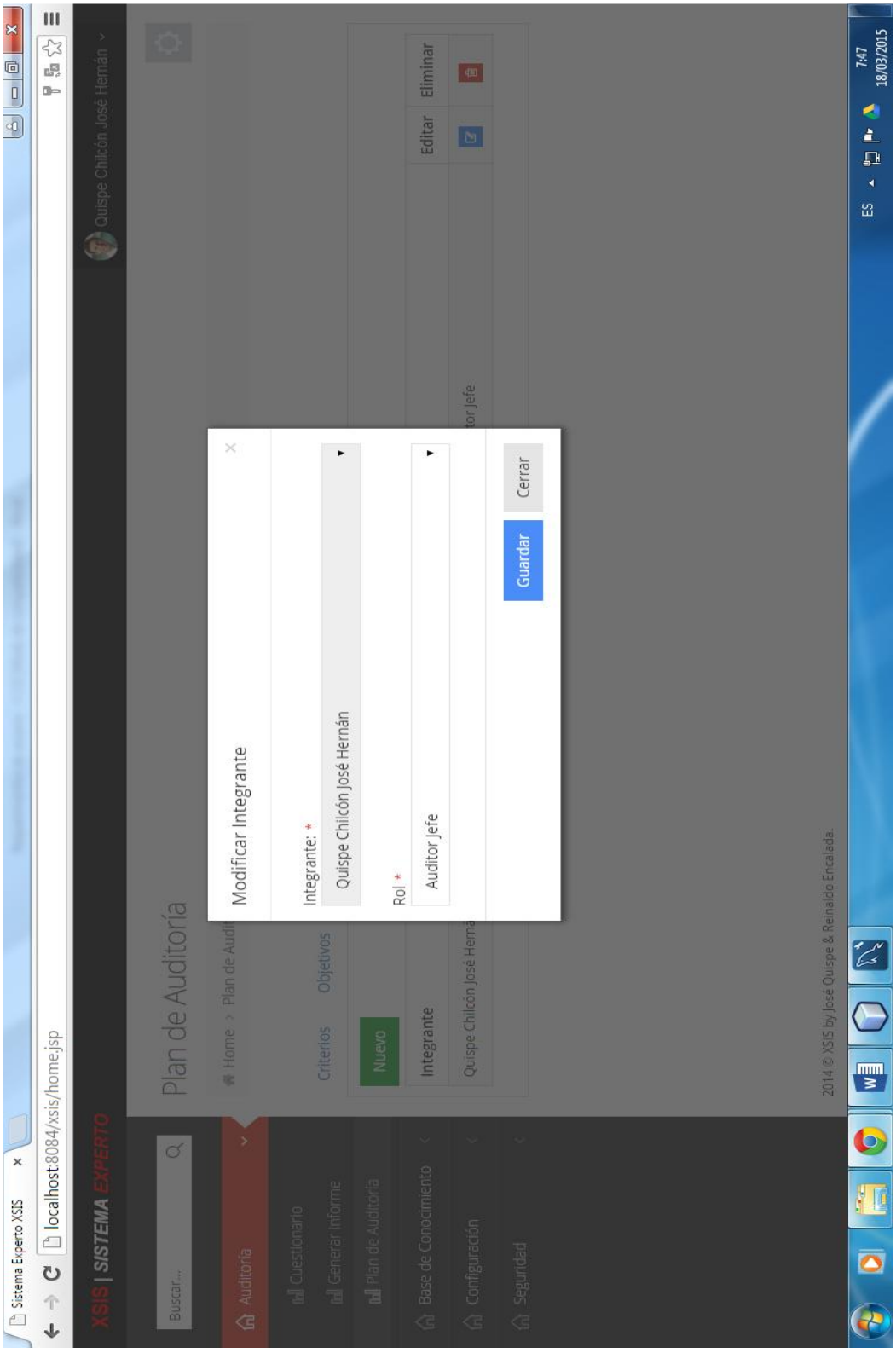
- **Listar sedes- plan auditoría**



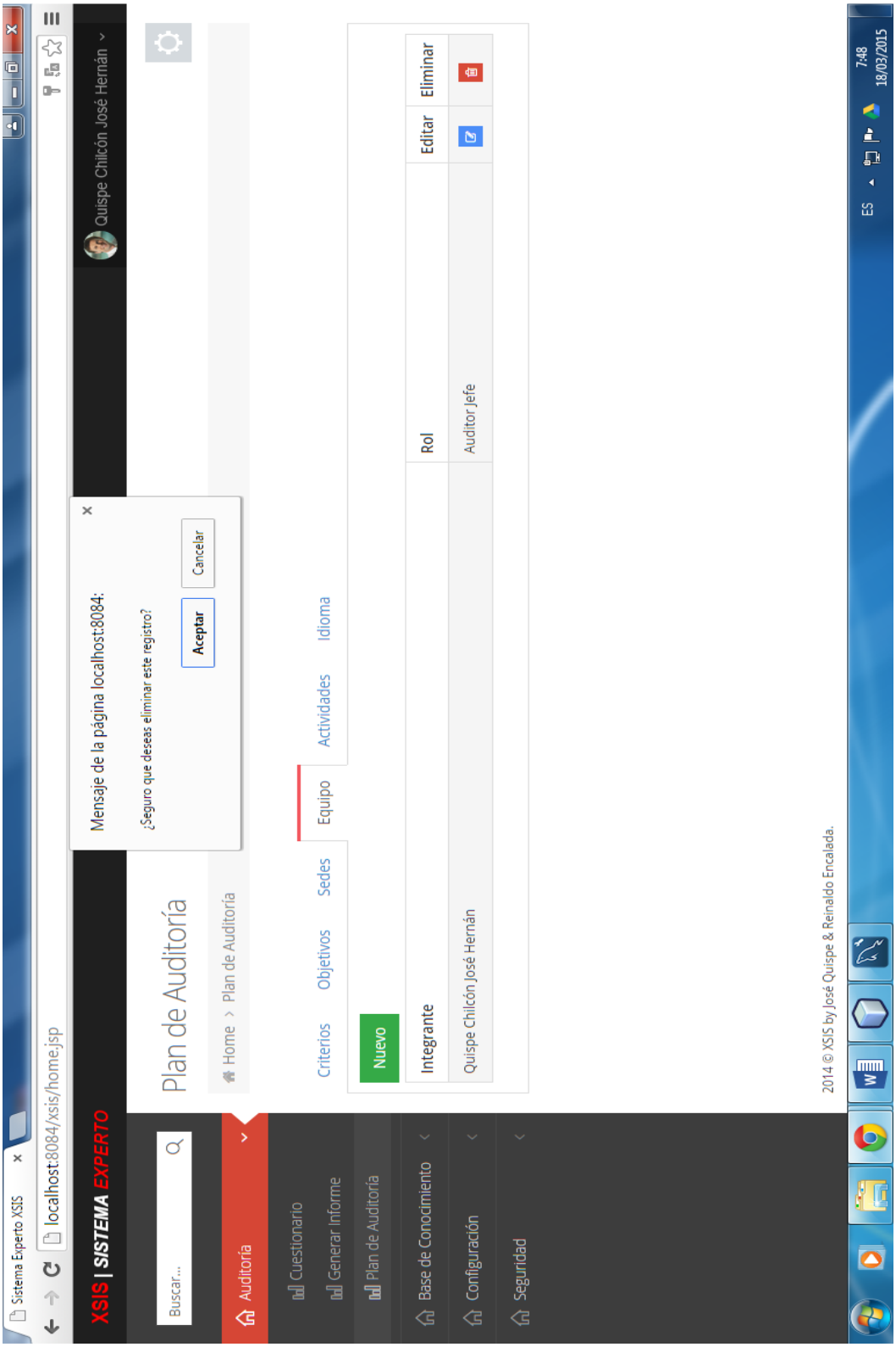
- **Registrar miembro equipo – plan auditoría**



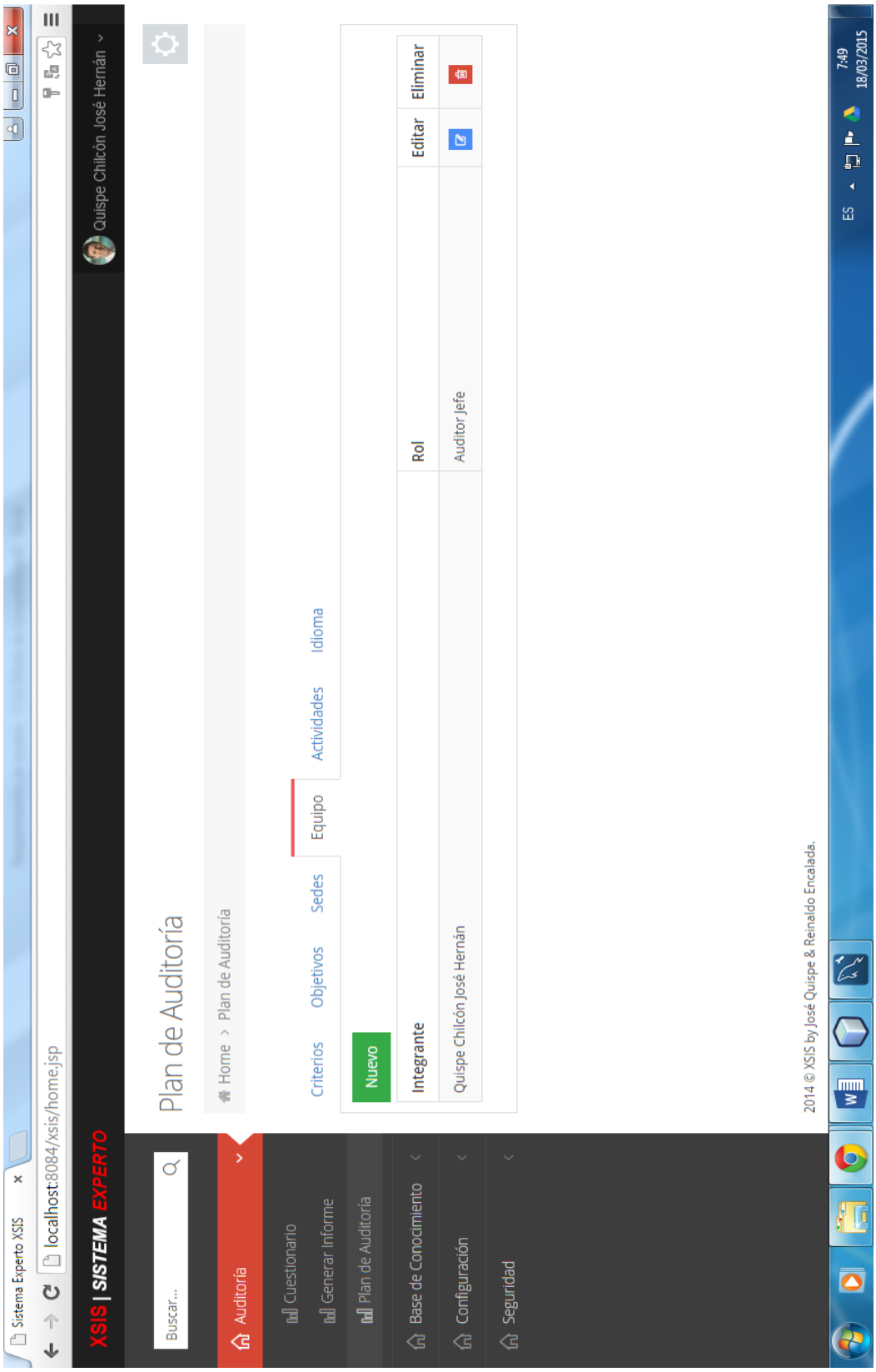
- **Modificar miembro equipo – plan auditoría**



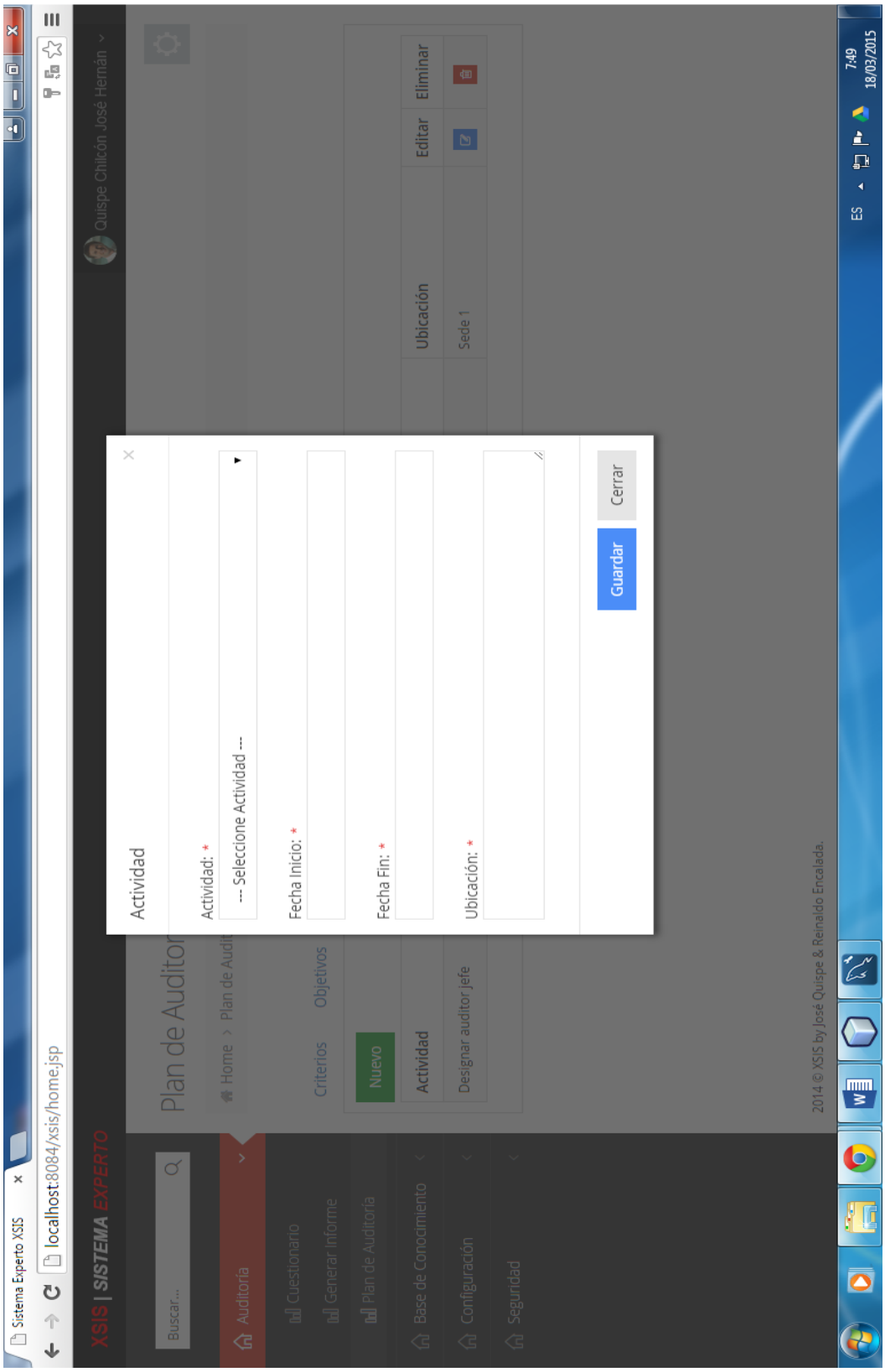
- **Eliminar miembro equipo – plan auditoría**



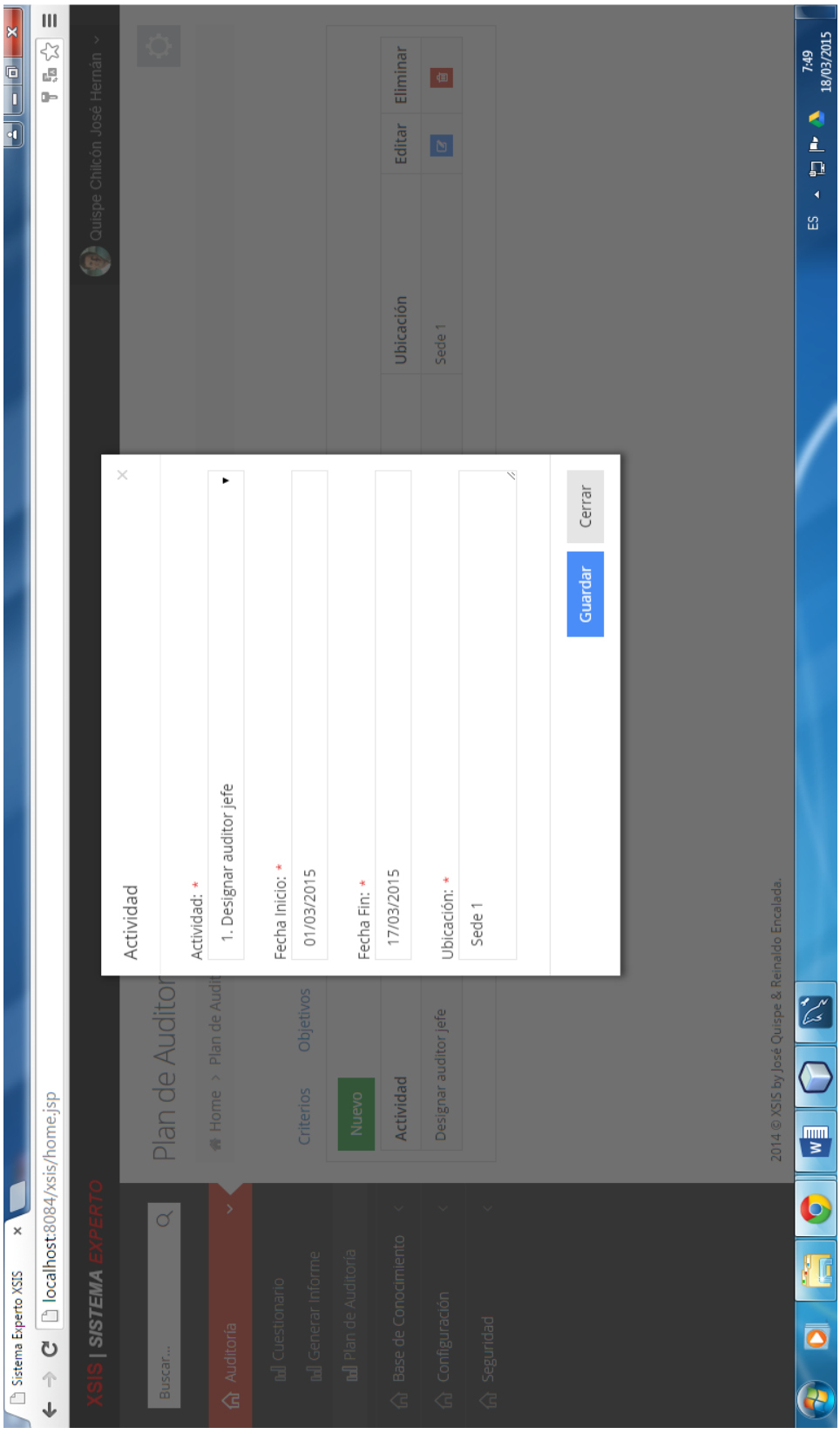
- **Listar equipo – plan auditoría**



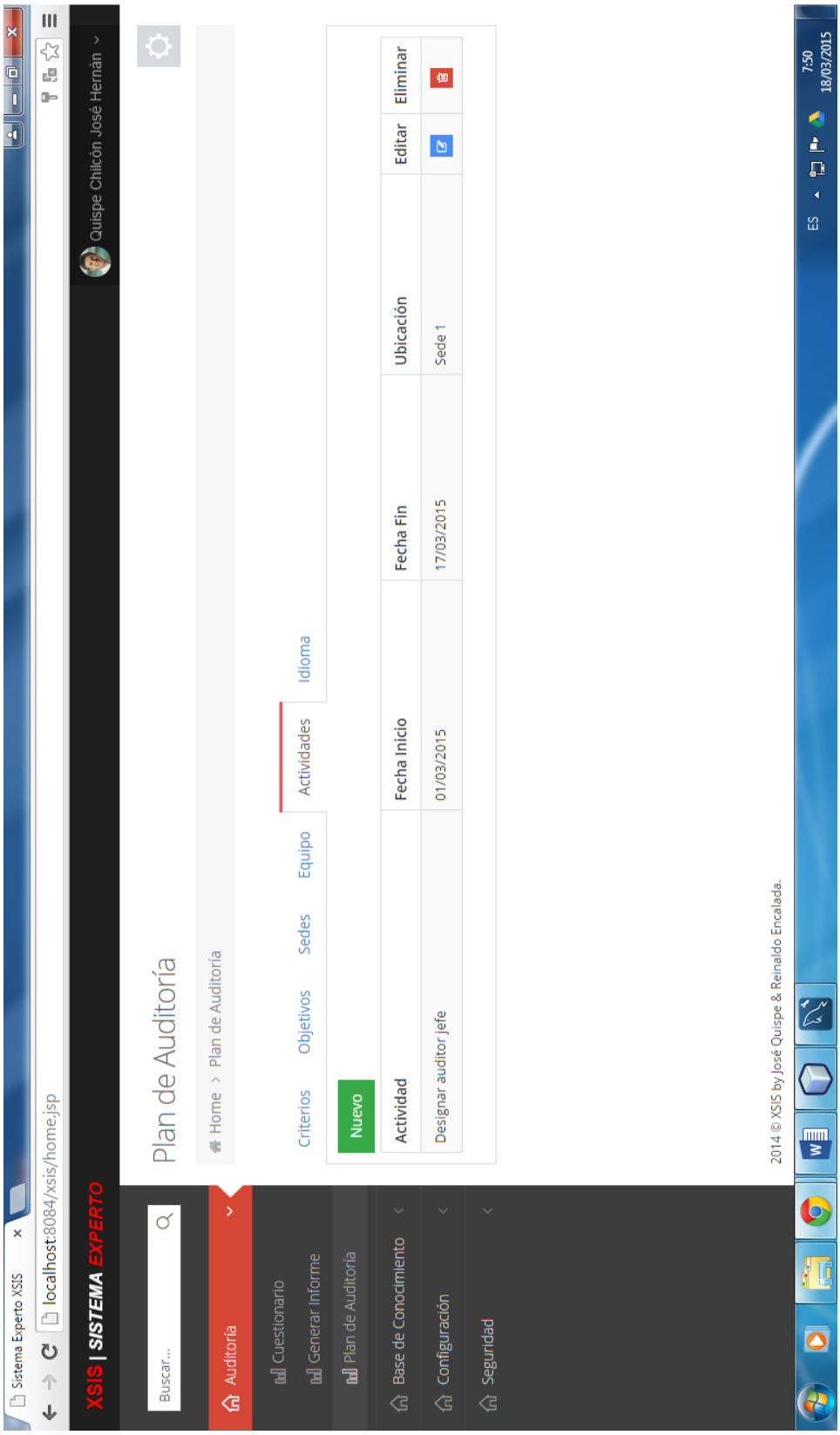
- **Registrar actividad – plan auditoría**



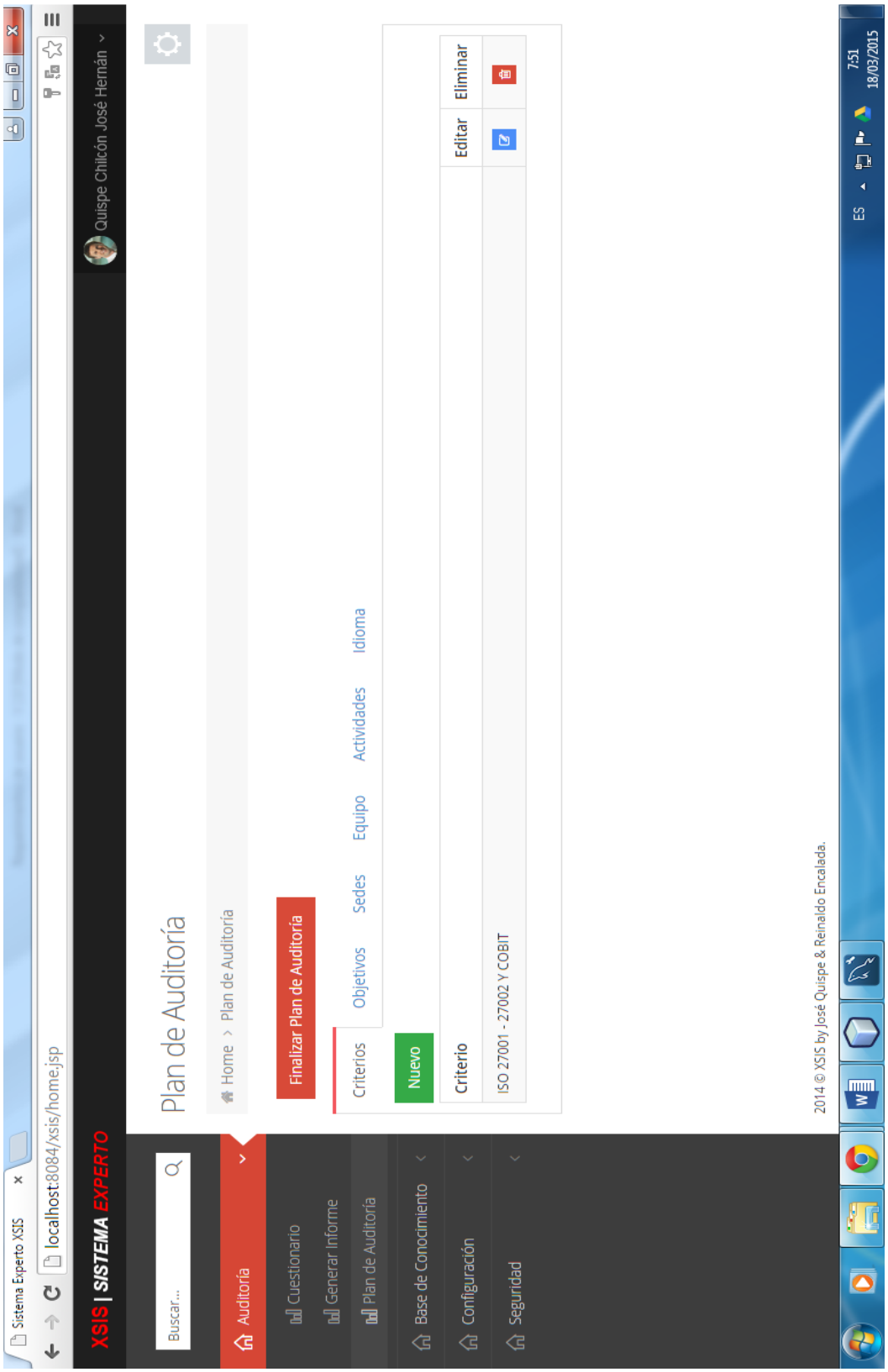
- **Modificar actividad – plan auditoría**



- **Listar actividades – plan auditoría**

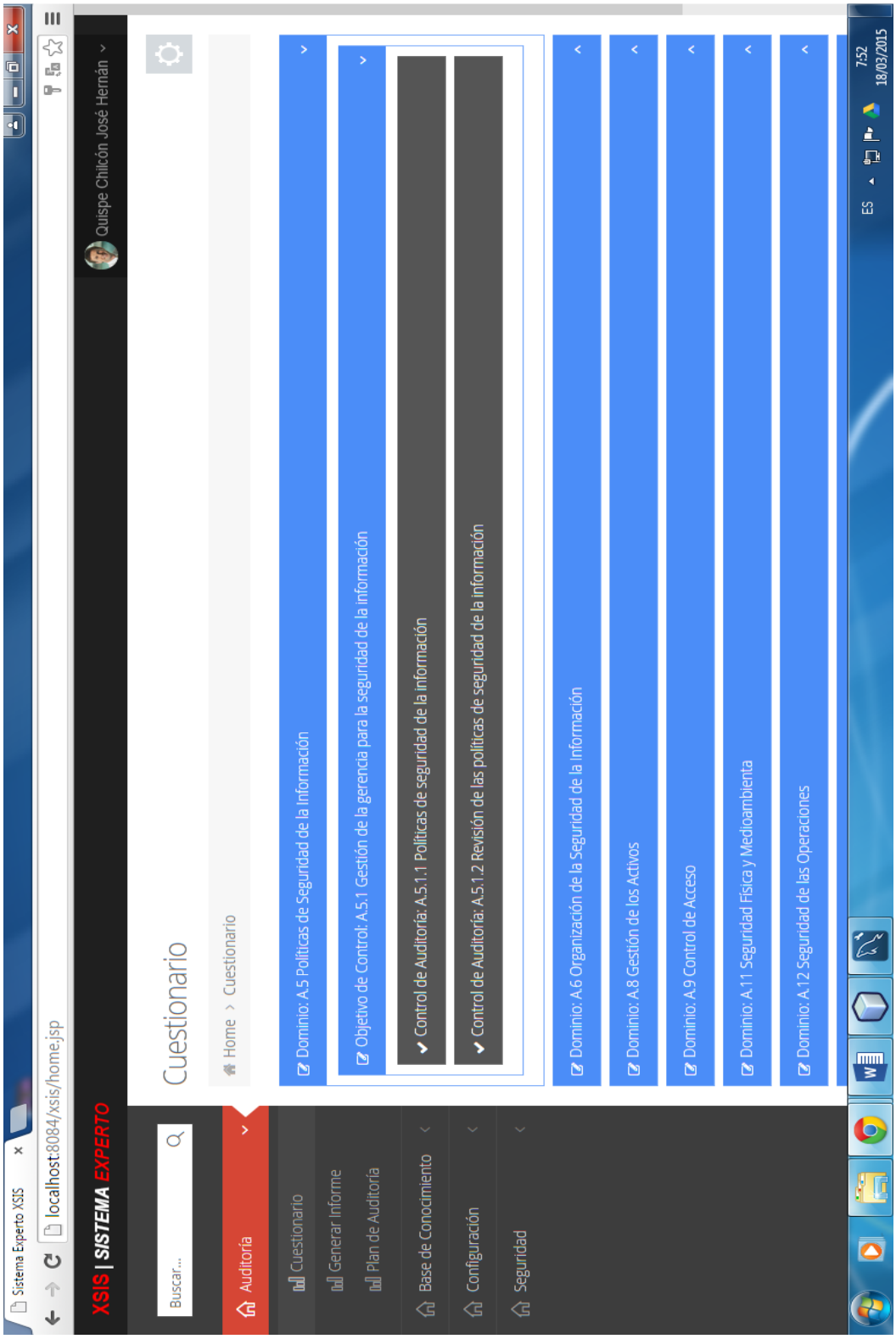


- **Finalizar plan auditoría**

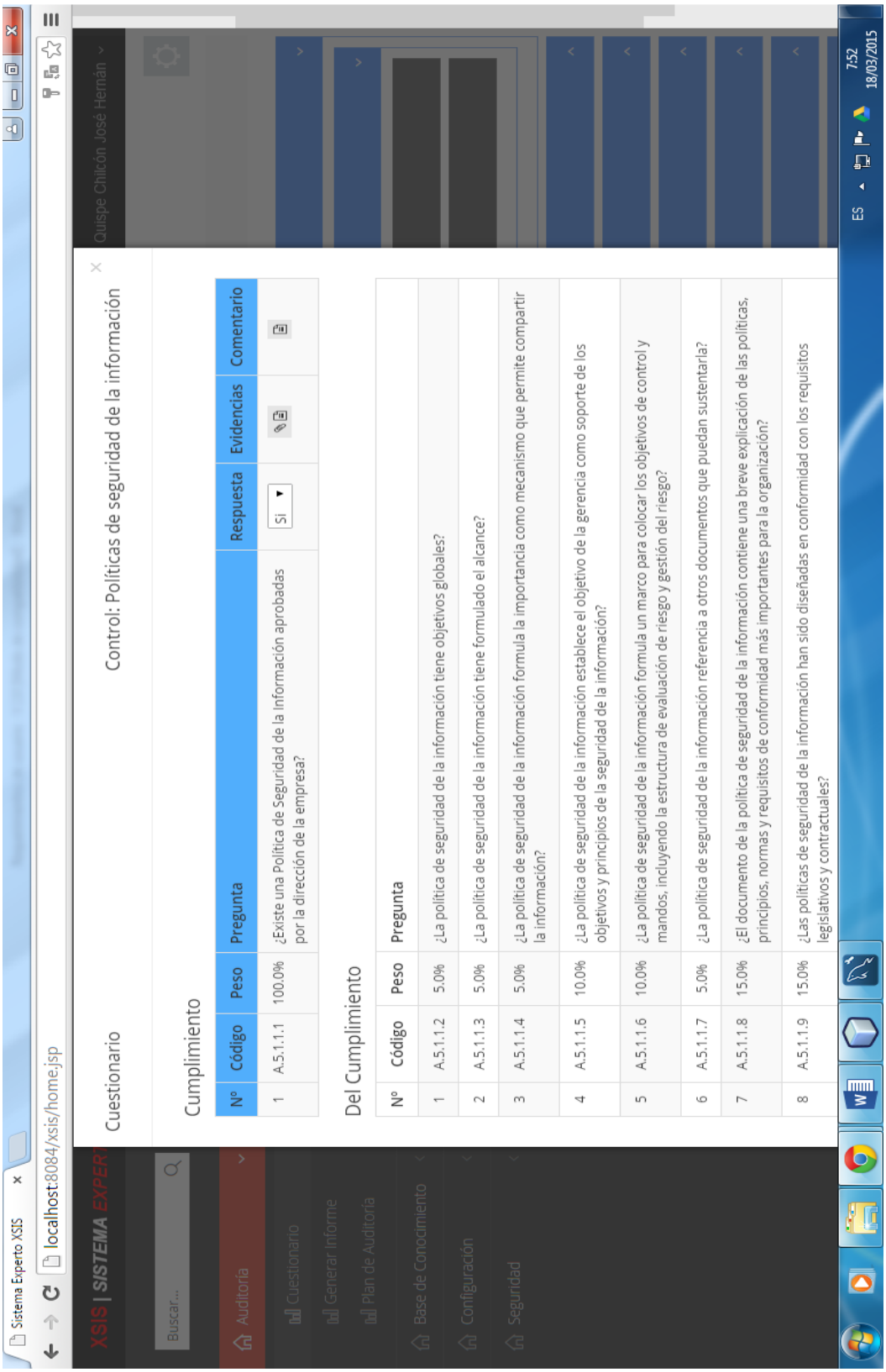


b. Cuestionario

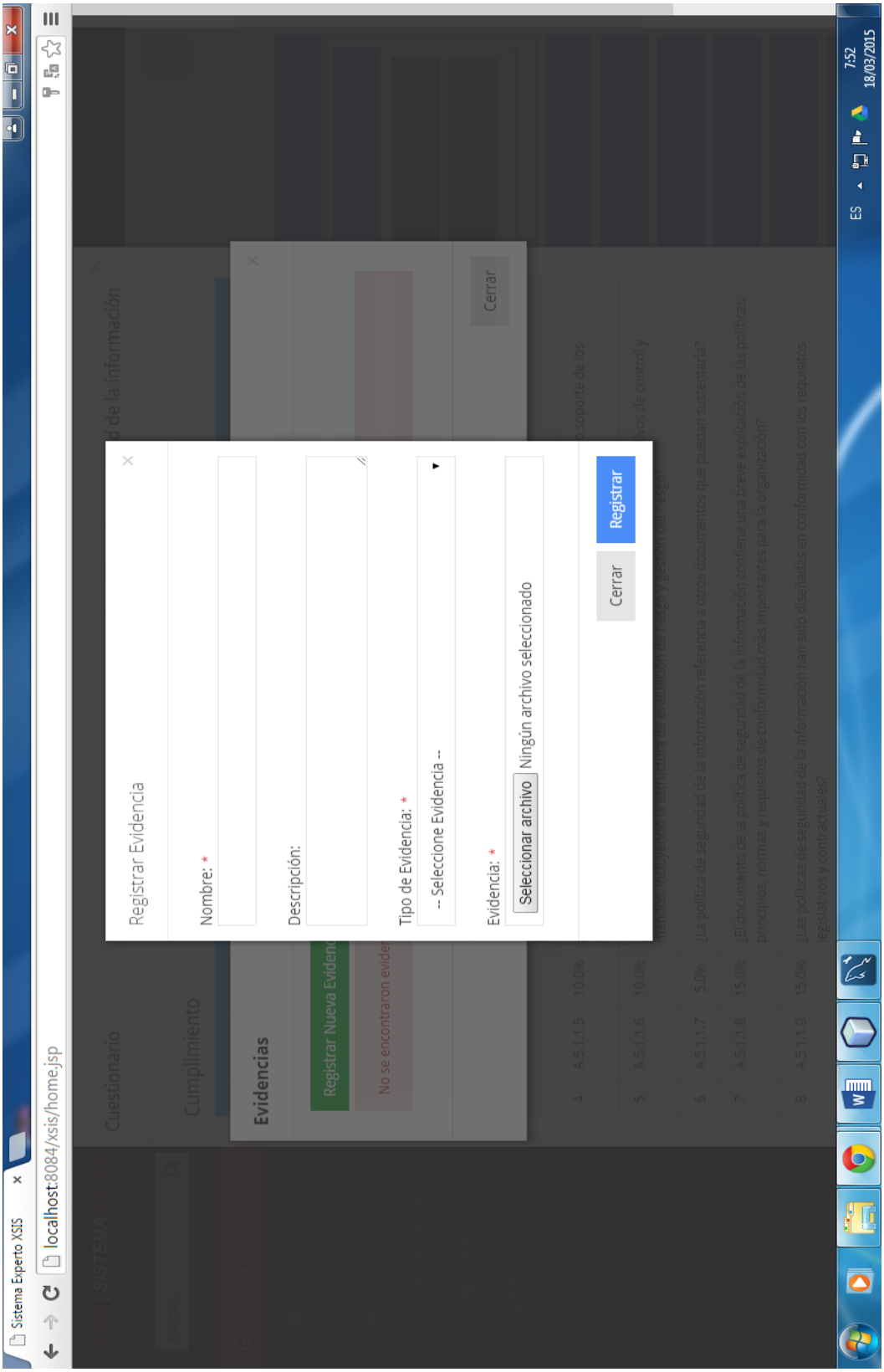
- **Listar controles cuestionario**



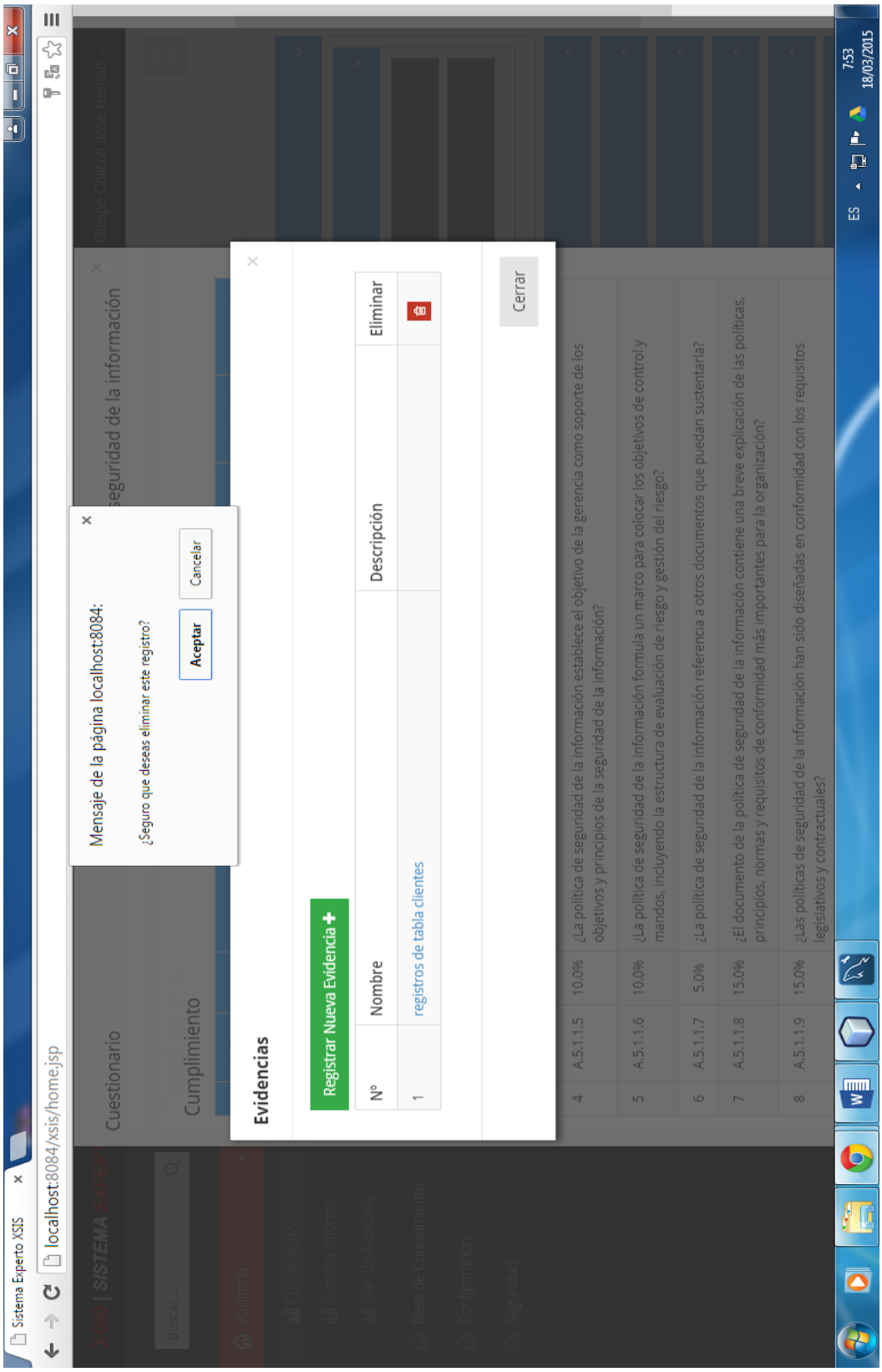
- **Completar cuestionario auditoría**



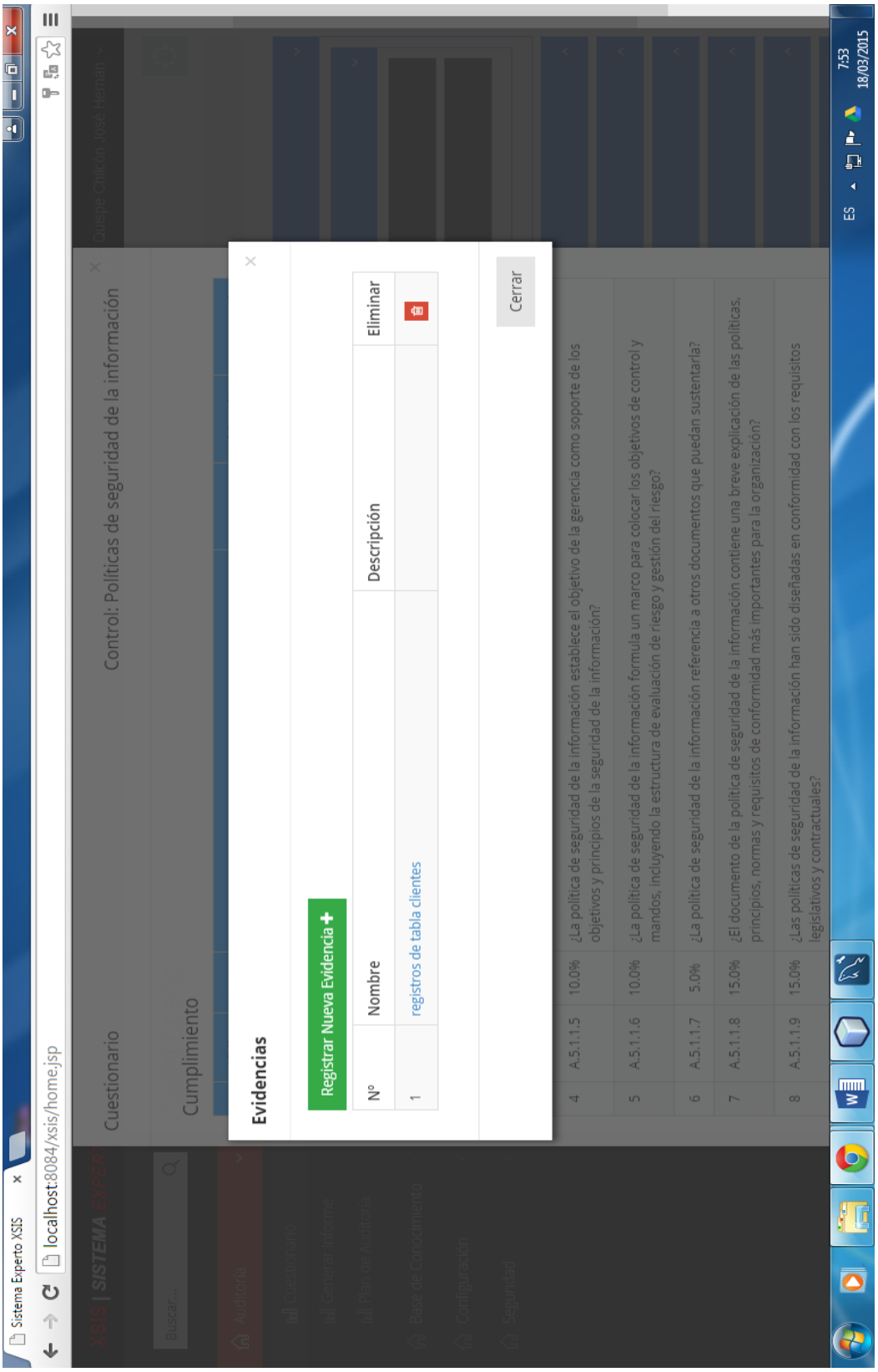
- **Adjuntar evidencia pregunta**



- **Eliminar evidencia pregunta**

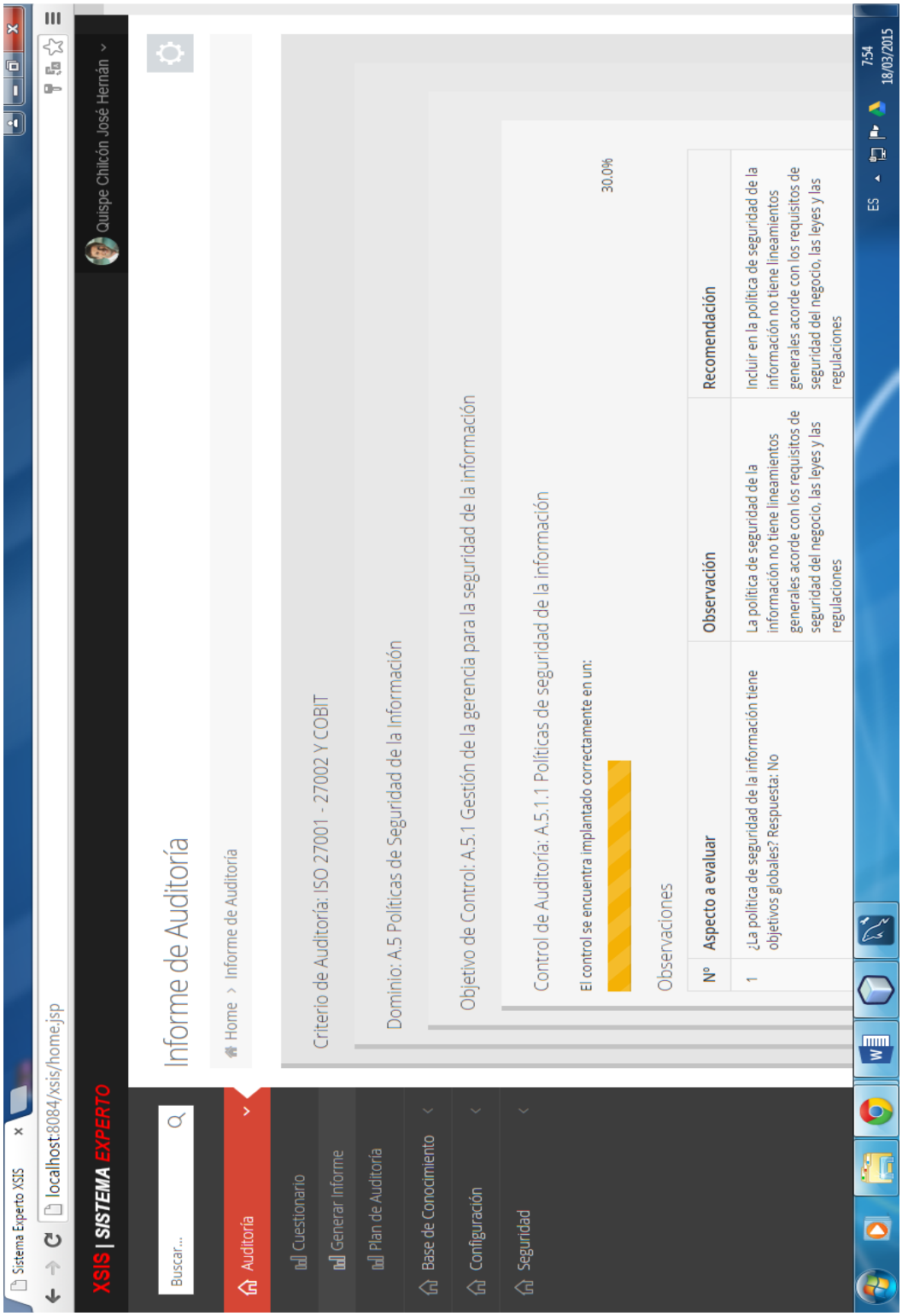


- **Listar evidencias pregunta**

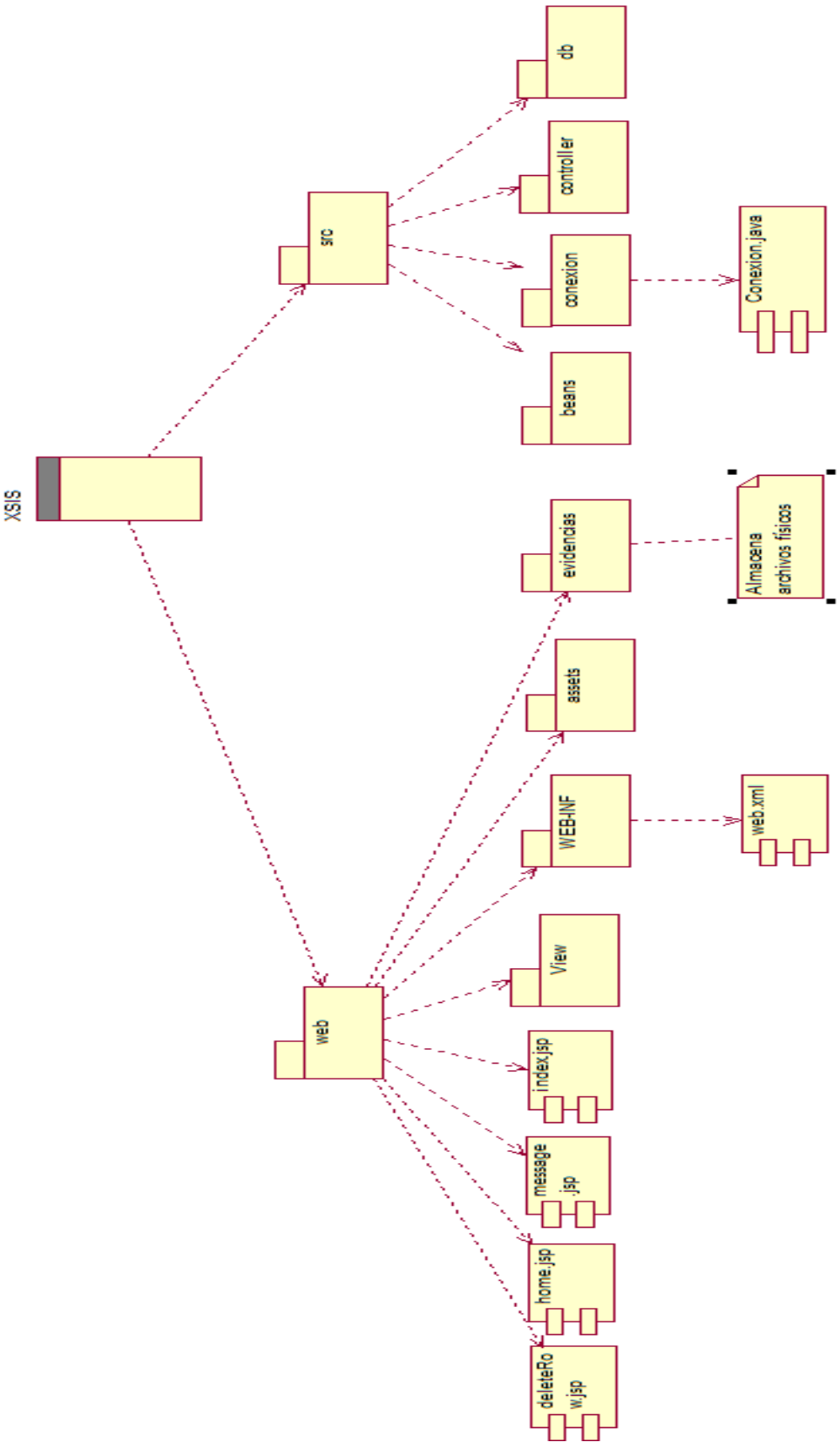


c. Informe auditoría

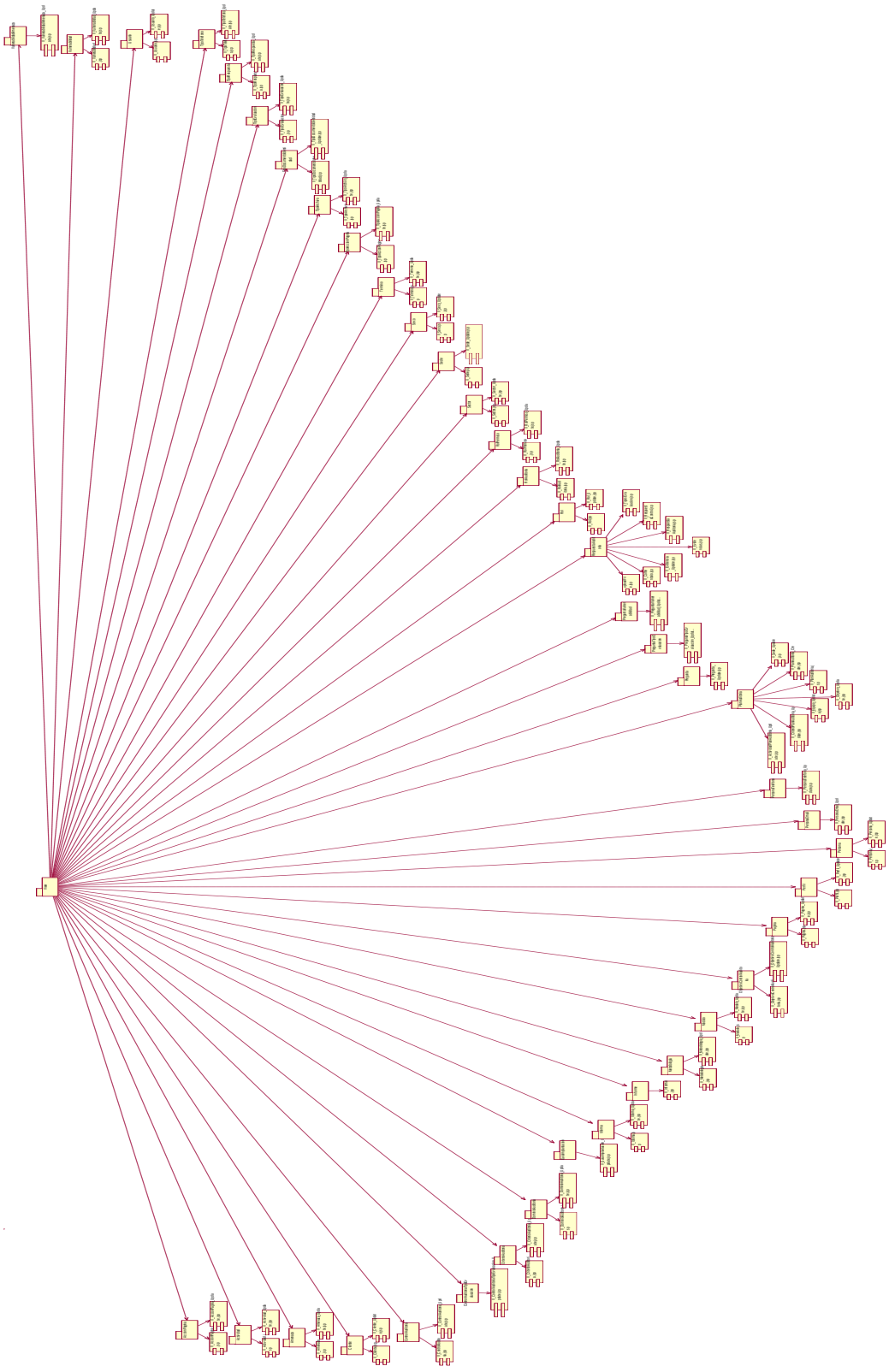
- **Generar informe de Auditoría**



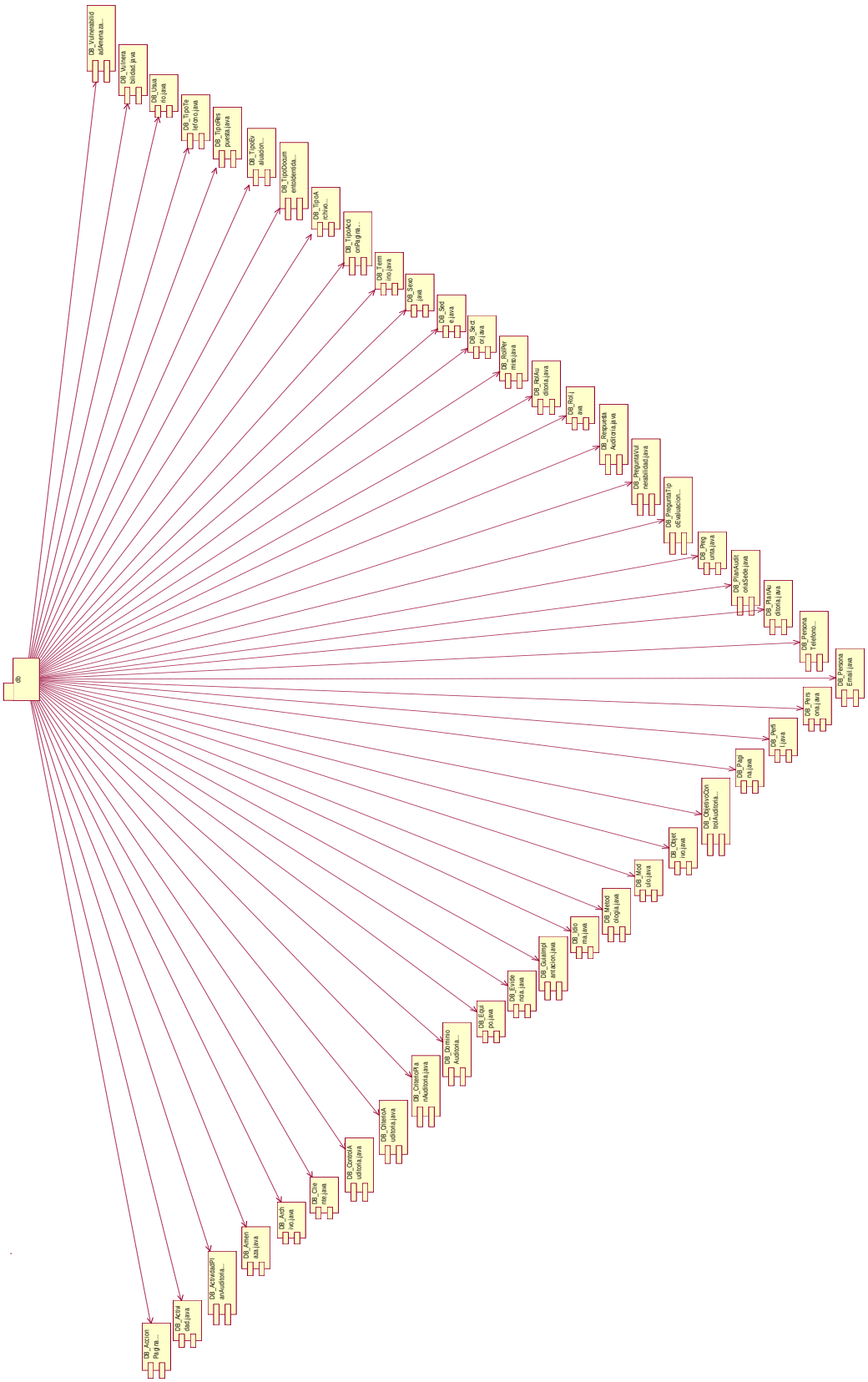
4.4.2 Diagrama de componentes



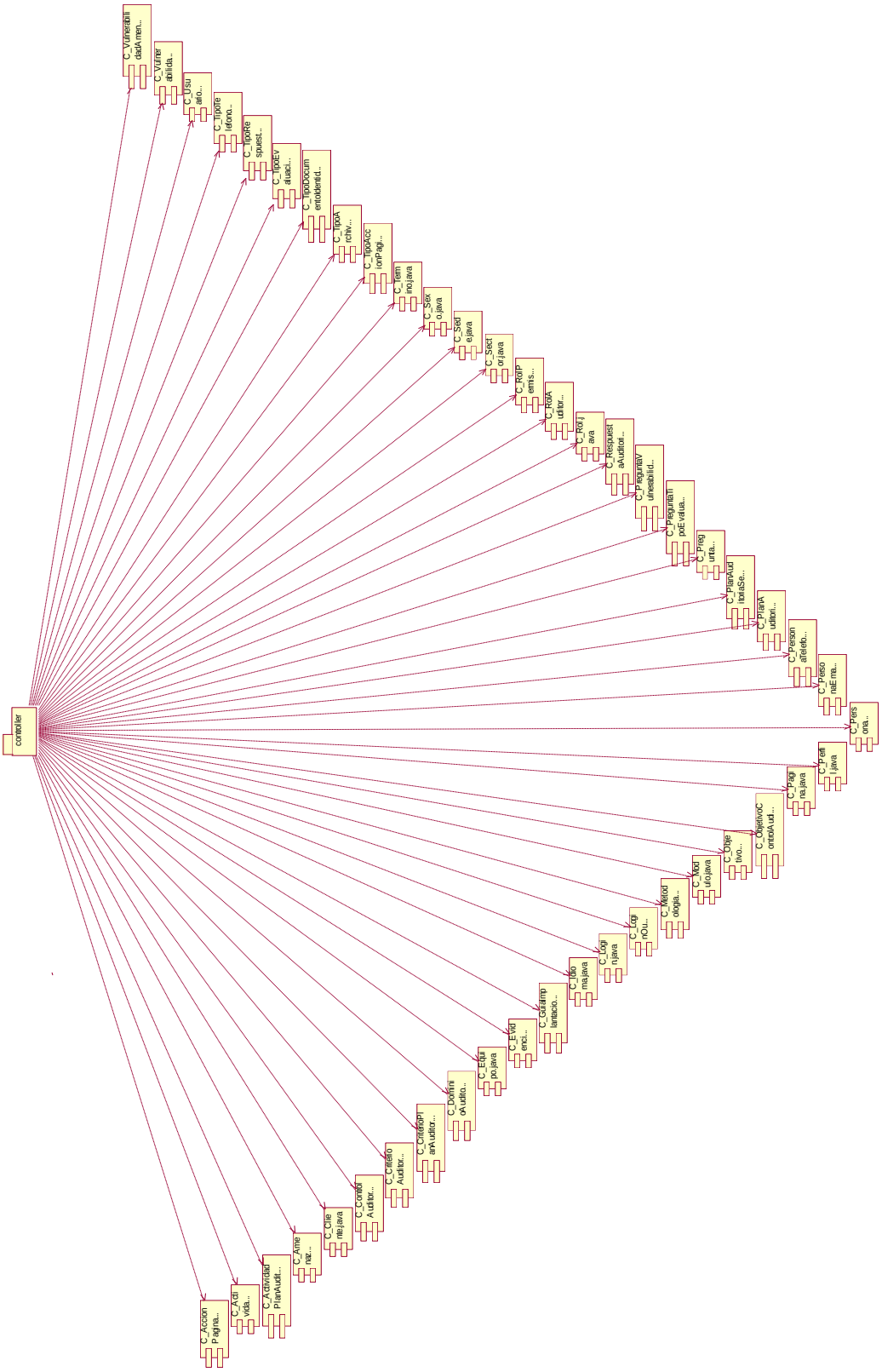
4.4.2.1 Diagrama de componentes (View)



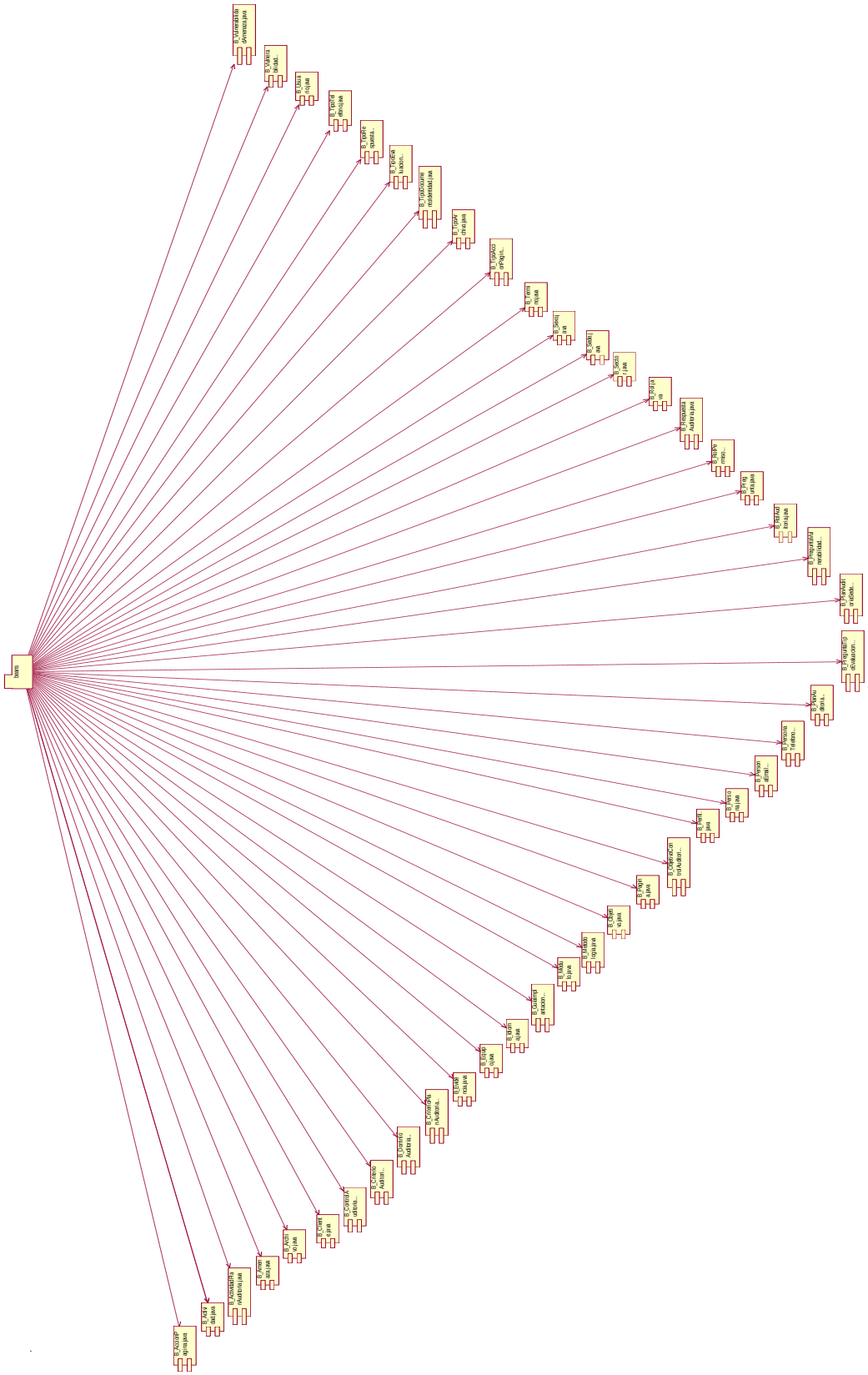
4.4.2.2 Diagrama de componentes (db)



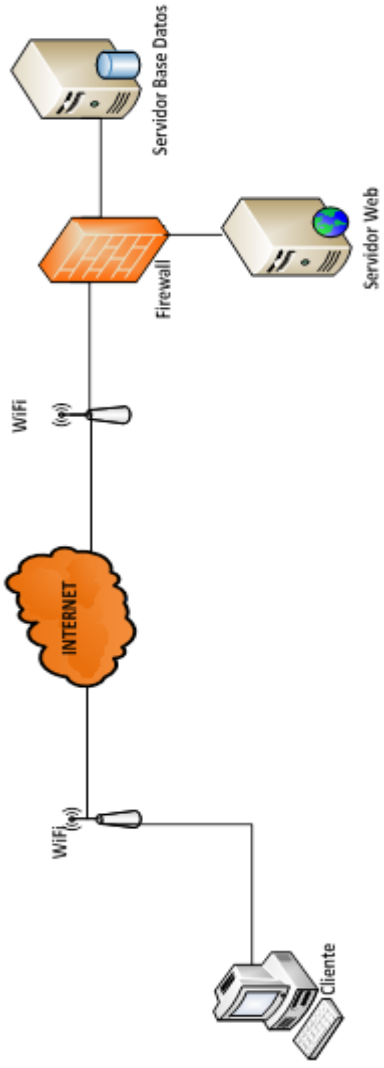
4.4.2.3 Diagrama de componentes (controller)



4.4.2.4 Diagrama de componentes (beans)



4.4.3 Diagrama de despliegue



4.4.4 Diagrama físico

4.5 Pruebas

El resultado de las pruebas del Sistema Experto se encuentran descrito en el Capítulo V: Discusión.

V. DISCUSIÓN

5.1. Contrastación de la Hipótesis

5.1.1. Identificación de Variables e Indicadores

El Método de Contrastación será: Post-Test, siendo las variables las siguientes:

Variable Independiente (VI)	Variable Dependiente (VD)
Sistema Experto en Auditoría de Seguridad de la Información	identificación de vulnerabilidades y amenazas de los activos informáticos

Tabla Nº 5.1: Variables

Los indicadores de la VD se muestran en la siguiente Tabla:

N°	INDICADOR	TIPO
1	Disponibilidad del Informe de Auditoría	Cualitativo
2	Integridad del Informe de Auditoría	Cualitativo
3	Confidencialidad del Informe de Auditoría	Cualitativo
4	Facilidad de uso del Sistema Experto	Cualitativo
5	Cantidad de vulnerabilidades identificadas	Cuantitativo
6	Cantidad de amenazas identificadas	Cuantitativo

Tabla Nº 5.2: Indicadores de la Variable Dependiente (VD)

5.1.2. Método de Análisis para los Indicadores Cualitativos

Para todos los Indicadores Cualitativos se aplicará la prueba estadística basada en la Distribución ***t de Student*** para CINCO (05) encuestados. Al buscar en las Tablas de Distribución de ***t de Student*** con Nivel de Significancia igual a 5% ($\alpha = 0.05$), Nivel de Confianza

igual a 95% (1-α = 0.95) y con n-1=5-1=4 grados de libertad, se obtiene

$$t_{(1-\alpha)(n-1)} = t_{(1-0.05)(5-1)} = 2.132 \quad \text{.....(5.1)}$$

Asimismo, para todas los Indicadores Cualitativos se procederá de la siguiente manera:

- Paso 1: Definición de la Variable a evaluar.
- Paso 2: Planteamiento de la Hipótesis Estadística.
- Paso 3: Formulación del Cuestionario aplicado.
- Paso 4: Procesamiento de los resultados utilizando las Tablas del Anexo 1 Subtítulo 1.
- Paso 5: Cálculo del Promedio Muestral, tomando los resultados del respectivo subtítulo del Anexo 1 se hacen uso de las expresiones:

$$\boldsymbol{PN_D} = \frac{\sum_{\mathbf{i=1}}^{\mathbf{n}} \boldsymbol{N_{Di}}}{\mathbf{n}} \quad \text{.....(5.2)}$$

Dónde:

- $\boldsymbol{n}$ = Número de Preguntas
- $\boldsymbol{PN_D}$ = Promedio después de la implementación del Sistema Experto
- $\boldsymbol{N_{Di}}$ = Puntaje Total de la Pregunta i – ésima.

- Paso 6: Cálculo de la Desviación Estándar Muestral, que es el promedio de todos los valores obtenidos antes y después del estímulo, usando las expresiones:

$$\boldsymbol{S^2_D} = \frac{\boldsymbol{n}\ \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{D^2} - \left(\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{D_i}\right)^{\mathbf{2}}}{\boldsymbol{n(n-1)}} \quad \text{.....(5.3)}$$

Dónde:

- $\boldsymbol{S^2_D}$ = Desviación Estándar
- $\boldsymbol{D}$ = Diferencia
- $\boldsymbol{D_i}$ = Diferencia de promedio de la pregunta i – ésima.

n = Número de Preguntas

- Paso 7: Cálculo del Valor Crítico de t, usando la expresión:

$$t_c = \frac{\bar{D}\sqrt{n}}{\sqrt{S_D^2}} \quad \text{.....(5.4)}$$

- Paso 8: Redacción de la Conclusión de la Prueba Estadística teniendo en cuenta que la región de rechazo se encuentran fuera del rango:

$$-2.132 < t_c < 2.132 \quad \text{.....(5.5)}$$

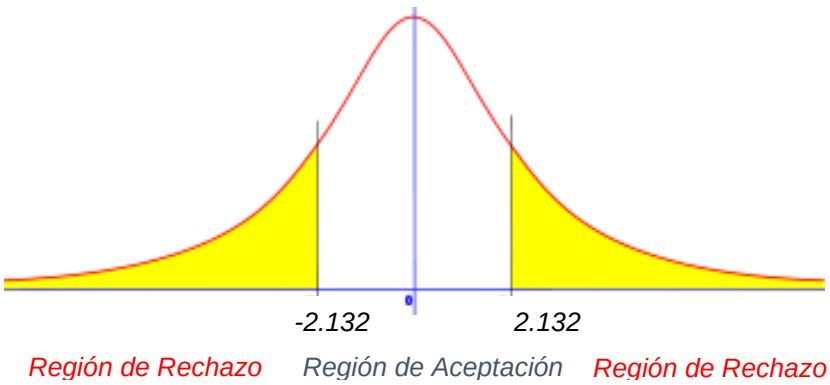


Figura Nº 5.1: Distribución t de Student indicando zona de aceptación y rechazo

5.1.3. Método de Análisis para los Indicadores Cuantitativos

Para todas los Indicadores Cuantitativos se procederá de la siguiente manera:

- Paso 1: Definición de la Variable a evaluar.
- Paso 2: Planteamiento de la Hipótesis Estadística.
- Paso 3: Definición del Nivel de Significancia, para todos será del 5%. Por lo tanto el Nivel de Confianza (1-α = 0.95) será del 95%.
- Paso 4: Definición del Tipo de Prueba Aplicada, para todos será la distribución es Normal Z para CINCO (05) encuestados.

- Paso 5: Tabulación de Valores obtenidos después de la implementación del Sistema Experto, se mostrarán solo los resumidos y/o trabajados y los originales en el Anexo 1.
- Paso 6: Cálculo del Promedio Muestral usando las expresiones,

$$\overline{X_D} = \frac{\sum_{i=1}^{n} X_{Di}}{n} \quad \text{.....(5.5)}$$

Se entiende que ***D*** significa ***Después*** de la implementación del Sistema Experto, aquí como en las siguientes expresiones.

- Paso 7: Cálculo de la Varianza Muestral, que es el promedio de todos los valores obtenidos antes y después del estímulo, usando las expresiones:

$$\sigma_D{}^2 = \frac{\sum_{i=1}^{n} (X_{Di} - \overline{X_D})^2}{n-1} \quad \text{.....(5.6)}$$

- Paso 8: Cálculo Estadístico de la Prueba, que es la diferencia al cuadrado de las diferencias obtenidas, entre el valor observado y la media, antes y después del estímulo, usando la expresión:

$$Z_c = \frac{-\overline{X_D}}{\sqrt{\left(\frac{\sigma_D^2}{n_D}\right)}} \quad \text{.....(5.7)}$$

- Paso 9: Búsqueda del Valor Critico de Z en las Tablas estadísticas de la Distribución Z.
- Paso 10: Redacción de la Conclusión de la Prueba Estadística.

5.2. Prueba de Hipótesis para el Indicadores Cualitativos

5.2.1. Indicador "Disponibilidad del Informe de Auditoría"

a. Definición de Variables

- D_A = 0, no existe un procedimiento que asegure la disponibilidad del Informe de Auditoría antes de la Implementación del Sistema Experto.
- D_D: Disponibilidad del Informe de Auditoría después de la Implementación del Sistema Experto.

b. Hipótesis Estadística

- Hipótesis H_o: La disponibilidad del Informe de Auditoría antes de la Implementación del Sistema Experto es mayor o igual a la disponibilidad del Informe de Auditoría después de la Implementación del Sistema Experto ($H_o \geq H_a$).
- Hipótesis H_a: La disponibilidad del Informe de Auditoría antes de la Implementación del Sistema Experto es menor a la disponibilidad del Informe de Auditoría después de la Implementación del Sistema Experto ($H_o < H_a$).

c. Cuestionario aplicado

Se proponen las siguientes preguntas:

1. ¿Cómo calificaría el acceso al Informe de Auditoría?
2. ¿El Informe de Auditoría puede ser accedido desde cualquier lugar?
3. ¿El Informe de Auditoría puede ser accedido a cualquier hora?
4. ¿El Informe de Auditoría puede ser exportado a un archivo local?

5. ¿El Informe de Auditoría puede ser requerido por correo electrónico?
6. ¿El Informe de Auditoría puede ser requerido de manera impresa?
7. ¿Se puede solicitar un detalle del Informe de Auditoría?

d. Valores Tabulados

Los valores obtenidos para este indicador se encuentran en el Anexo Nº 1 Subtítulo 2, aquí se muestran de manera consolidada.

Nº	Pregunta	Respuestas				Puntaje Pregunta (PP)	Puntaje Promedio Pregunta (PPP)
		MI	I	PI	NI		
		3	2	1	0		
1	¿Cómo calificaría el acceso al Informe de Auditoría?	3	2	0	0	13	2.17
2	¿El Informe de Auditoría puede ser accedido desde cualquier lugar?	3	2	0	0	13	2.17
3	¿El Informe de Auditoría puede ser accedido a cualquier hora?	4	1	0	0	14	2.33
4	¿El Informe de Auditoría puede ser exportado a un archivo local?	0	2	3	0	7	1.17
5	¿El Informe de Auditoría puede ser requerido por correo electrónico?	0	3	2	0	8	1.33
6	¿El Informe de Auditoría puede ser requerido de manera impresa?	0	1	3	1	5	0.83

Tabla Nº 5.3: Resultados consolidados del cuestionario aplicado respecto al Indicador "Disponibilidad del Informe de Auditoría" (Post-test)

Pregunta	Puntaje Promedio		D_i	D_i^2
	Pre-Prueba	Post-Prueba		
	PPP_{Ai}	PPP_{Di}		
1	0	2.17	-2.17	4.71
2	0	2.17	-2.17	4.71
3	0	2.33	-2.33	5.43
4	0	1.17	-1.17	1.37
5	0	1.33	-1.33	1.77
6	0	0.83	-0.83	0.69
Suma	**0**	**10.00**	**-10.00**	**18.68**
Promedio	**0**	**1.67**	**-1.67**	**3.11**

Tabla N° 5.4: Resultados estadísticos para el Indicador Cualitativo "Disponibilidad del Informe de Auditoría"

e. Cálculo de la Desviación Estándar Muestral

Valor	Antes	Después
Promedio Aritmético Muestral	$PN_A = 0$	$PN_D = \frac{10.00}{6} = 1.67$

Tabla Nº 5.5: Media y Varianza Muestral para Indicador "Disponibilidad del Informe de Auditoría"

f. Cálculo del Valor Crítico de t

Valor	Cálculo
Desviación Estándar Muestral	$S^2_D = \frac{6 \times 18.68 - (-10)^2}{6 \times (6-1)} = 0.403$
Cálculo Estadístico de la Prueba	$t_c = \frac{-1.67 \times \sqrt{6}}{\sqrt{0.403}} = -6.431$

Tabla Nº 5.6: Valor crítico de t para Indicador "Disponibilidad del Informe de Auditoría"

g. Conclusión

Puesto que t_c = -6.431 calculado es menor que $t_{0.05}$ = -2.132 y ***estando este valor dentro de la región de rechazo***, entonces ***se rechaza H_o y por consiguiente se acepta H_a.***

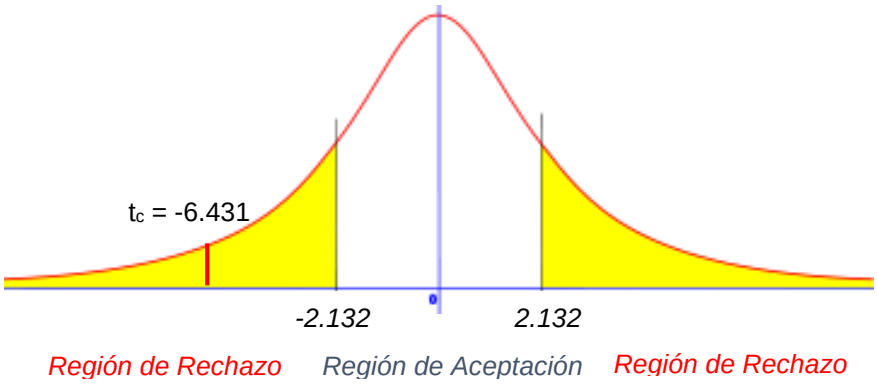


Figura Nº 5.2: Valor crítico de t para Indicador "Disponibilidad del Informe de Auditoría"

Se concluye que la Disponibilidad de la Información ***después*** de la implementación del Sistema Experto ***es mayor que antes*** de la implementación del Sistema Experto.

5.2.2. Indicador "Integridad del Informe de Auditoría"

a. Definición de Variables

- I_A = 0, no existe un procedimiento que asegure la Integridad del Informe de Auditoría antes de la Implementación del Sistema Experto.
- I_D: Integridad del Informe de Auditoría después de la Implementación del Sistema Experto.

b. Hipótesis Estadística

- Hipótesis H_o: La Integridad del Informe de Auditoría antes de la Implementación del Sistema Experto es mayor o igual

a la Integridad del Informe de Auditoría después de la Implementación del Sistema Experto ($H_o \geq H_a$).

- Hipótesis H_a: La Integridad del Informe de Auditoría antes de la Implementación del Sistema Experto es menor a la Integridad del Informe de Auditoría después de la Implementación del Sistema Experto ($H_o < H_a$).

c. Cuestionario aplicado

Se proponen las siguientes preguntas:

1. ¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?
2. ¿La información obtenida es la oficial?
3. ¿La información obtenida es certificada?
4. ¿La información obtenida puede ser validada posteriormente?
5. ¿La información obtenida puede ser verificada posteriormente?
6. ¿La información obtenida es actual (de reciente producción)?
7. ¿El Informe de Auditoría puede ser deducido de la información obtenida?

d. Valores Tabulados

Los valores obtenidos para este indicador se encuentran en el Anexo Nº 1 Subtítulo 3, aquí se muestran de manera consolidada.

Nº	Pregunta	Respuestas				Puntaje Pregunta (PP)	Puntaje Promedio Pregunta (PPP)
		MI	I	PI	NI		
		3	2	1	0		
1	¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?	1	4	0	0	11	1.83
2	¿La información obtenida es la oficial?	3	2	0	0	13	2.17
3	¿La información obtenida es certificada?	2	3	0	0	12	2.00
4	¿La información obtenida puede ser validada posteriormente?	0	2	3	0	7	1.17
5	¿La información obtenida puede ser verificada posteriormente?	0	3	2	0	8	1.33
6	¿La información obtenida es actual (de reciente producción)?	1	3	0	1	9	1.50
7	¿El Informe de Auditoría puede ser deducido de la información obtenida?	0	3	2	0	8	1.33

Tabla Nº 5.7: Resultados consolidados del cuestionario aplicado respecto al Indicador "Integridad del Informe de Auditoría" (Post-test)

Pregunta	Puntaje Promedio		D_i	D_i^2
	Pre-Prueba	Post-Prueba		
	PPP_{Ai}	PPP_{Di}		
1	0	1.83	-1.83	3.35
2	0	2.17	-2.17	4.71
3	0	2.00	-2.00	4.00
4	0	1.17	-1.17	1.37
5	0	1.33	-1.33	1.77
6	0	1.50	-1.50	2.25
7	0	1.33	-1.33	1.77

Pregunta	Puntaje Promedio		D_i	D_i^2
	Pre-Prueba	Post-Prueba		
	PPP_{Ai}	PPP_{Di}		
Suma	**0**	**10.00**	**-10.00**	**17.45**
Promedio	**0**	**1.67**	**-1.67**	**2.91**

Tabla N° 5.8: Resultados estadísticos para el Indicador Cualitativo "Integridad del Informe de Auditoría"

e. Cálculo de la Desviación Estándar Muestral

Valor	Antes	Después
Promedio Aritmético Muestral	$PN_A = 0$	$PN_D = \frac{10}{7} = 1.67$

Tabla Nº 5.9: Media y Varianza Muestral para Indicador "Integridad del Informe de Auditoría"

f. Cálculo del Valor Crítico de t

Valor	Cálculo
Desviación Estándar Muestral	$S^2_D = \frac{7 \times 17.45 - (-10)^2}{7 \times (7-1)} = 0.157$
Cálculo Estadístico de la Prueba	$t_c = \frac{-1.67 \times \sqrt{7}}{\sqrt{0.157}} = -10.303$

Tabla Nº 5.10: Valor Crítico de t para Indicador "Integridad del Informe de Auditoría"

g. Conclusión

Puesto que t_c = -10.303 calculado es menor que $t_{0.05}$ = -2.132 y ***estando este valor dentro de la región de rechazo***, entonces ***se rechaza H_o y por consiguiente se acepta H_a.***

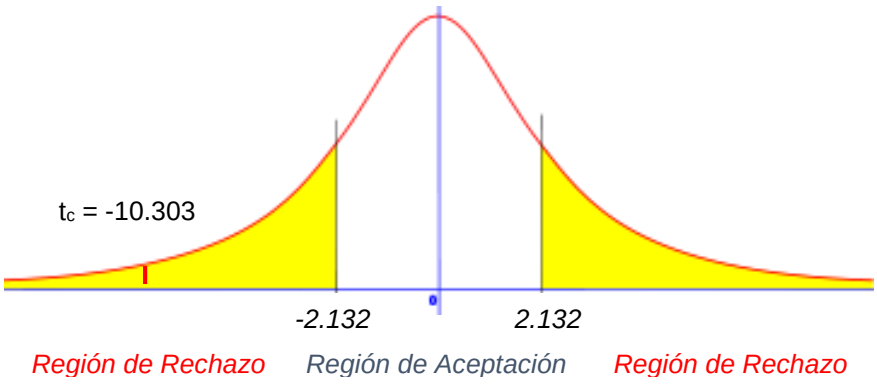


Figura Nº 5.3: Valor crítico de t para Indicador "Integridad del Informe de Auditoría"

Se concluye que la Integridad del Informe de Auditoría ***después*** de la implementación del Sistema Experto ***es mayor que antes*** de la implementación del Sistema Experto.

5.2.3. Indicador "Confidencialidad del Informe de Auditoría"

a. Definición de Variables

- C_A = 0, no existe un procedimiento que asegure la Confidencialidad del Informe de Auditoría antes de la Implementación del Sistema Experto.
- C_D: Confidencialidad del Informe de Auditoría después de la Implementación del Sistema Experto.

b. Hipótesis Estadística

- Hipótesis H_o: La Confidencialidad del Informe de Auditoría antes de la Implementación del Sistema Experto es menor o igual la Confidencialidad del Informe de Auditoría después de la Implementación del Sistema Experto ($H_o \geq H_a$).
- Hipótesis H_a: La Confidencialidad del Informe de Auditoría antes de la Implementación del Sistema Experto es mayor a

la Confidencialidad d del Informe de Auditoría después de la Implementación del Sistema Experto ($H_o < H_a$).

c. Cuestionario aplicado

Se proponen las siguientes preguntas:

1. ¿Existe un acuerdo de confidencialidad entre las partes intervinientes?
2. ¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?
3. ¿El Informe de Auditoría es distribuido solo a personal debidamente autorizado?
4. ¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?
5. ¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?

d. Valores Tabulados

Los valores obtenidos para este indicador se encuentran en el Anexo Nº 1 Subtítulo 4, aquí se muestran de manera consolidada.

Nº	**Pregunta**	**Respuestas**				**Puntaje Pregunta**	**Puntaje Promedio Pregunta**
		MI	**I**	**PI**	**NI**		
		3	**2**	**1**	**0**	**(PP)**	**(PPP)**
1	¿Existe un acuerdo de confidencialidad entre las partes intervinientes?	3	2	0	0	13	2.60
2	¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?	2	3	0	0	12	2.40
3	¿El Informe de Auditoría es distribuido solo a personal	1	4	0	0	11	2.20

Nº	Pregunta	Respuestas				Puntaje Pregunta (PP)	Puntaje Promedio Pregunta (PPP)
		MI	I	PI	NI		
		3	2	1	0		
	debidamente autorizado?						
4	¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?	2	3	0	0	12	2.40
5	¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?	3	2	0	0	13	2.60

Tabla Nº 5.11: Resultados consolidados del cuestionario aplicado respecto al Indicador "Confidencialidad del Informe de Auditoría" (Post-test)

Pregunta	Puntaje Promedio		D_i	D_i^2
	Pre-Prueba	Post-Prueba		
	PPP_{Ai}	PPP_{Di}		
1	0	2.60	-2.60	6.76
2	0	2.40	-2.40	5.76
3	0	2.20	-2.20	4.84
4	0	2.40	-2.40	5.76
5	0	2.60	-2.60	6.76
Suma	**0**	**12.20**	**-12.20**	**29.88**
Promedio	**0**	**2.44**	**-2.44**	**5.98**

Tabla N° 5.12: Resultados estadísticos para el Indicador Cualitativo "Confidencialidad del Informe de Auditoría"

e. Cálculo de la Desviación Estándar Muestral

Valor	Antes	Después
Promedio Aritmético Muestral	$PN_A = 0$	$PN_D = \frac{12.20}{5} = 2.44$

Tabla Nº 5.13: Media y Varianza Muestral para Indicador "Confidencialidad del Informe de Auditoría

f. Cálculo del Valor Crítico de t

Valor	Cálculo
Desviación Estándar Muestral	$S^2_D = \frac{5\times 29.88-(-12.20)^2}{5\times(5-1)} = 0.028$
Cálculo Estadístico de la Prueba	$t_c = \frac{-2.44\times\sqrt{5}}{\sqrt{0.028}} = -32.606$

Tabla Nº 5.14: Valor Crítico de t para Indicador "Confidencialidad del Informe de Auditoría"

g. Conclusión

Puesto que t_c = -32.606 calculado es menor que $t_{0.05}$ = -2.132 y ***estando este valor dentro de la región de rechazo***, entonces ***se rechaza H_o y por consiguiente se acepta H_a.***

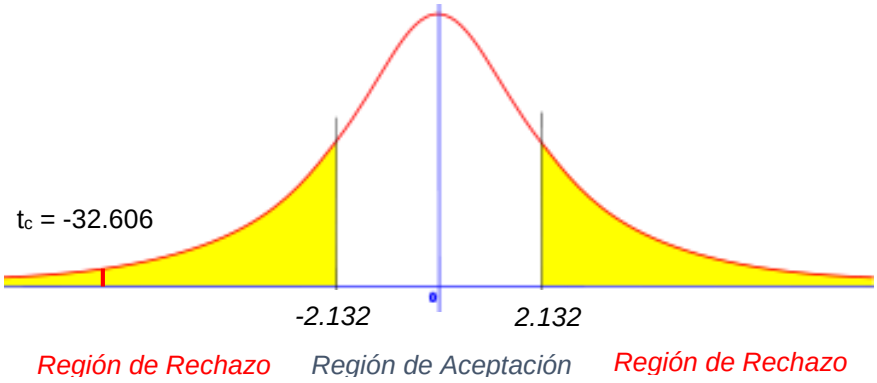


Figura Nº 5.4: Valor crítico de t para Indicador "Confidencialidad del Informe de Auditoría"

Se concluye que la Confidencialidad del Informe de Auditoría ***después*** de la implementación del Sistema Experto ***es mayor que antes*** de la implementación del Sistema Experto.

5.2.4. Indicador "Facilidad de Uso de la Aplicación"

a. Definición de Variables

- $D_A = 0$, no existe un Sistema Experto.
- D_D: Facilidad de Uso del Sistema Experto.

b. Hipótesis Estadística

- Hipótesis H_o: No es fácil usar el Sistema Experto ($H_o \geq H_a$).
- Hipótesis H_a: Es fácil usar el Sistema Experto ($H_o < H_a$).

c. Cuestionario aplicado

Se proponen las siguientes preguntas:

1. ¿El Sistema Experto usa un lenguaje entendible?
2. ¿El Sistema Experto emite mensajes entendibles?
3. ¿El Sistema Experto está divido en módulos?
4. ¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?
5. ¿El Sistema Experto permite emitir reportes de manera personalizada?

d. Valores Tabulados

Los valores obtenidos para este indicador se encuentran en el Anexo Nº 1 Subtítulo 5, aquí se muestran de manera consolidada.

Nº	**Pregunta**	**Respuestas**				**Puntaje Pregunta**	**Puntaje Promedio Pregunta**
		MI	**I**	**PI**	**NI**		
		3	**2**	**1**	**0**	**(PP)**	**(PPP)**
1	¿El Sistema Experto usa un lenguaje entendible?	3	2	0	0	13	2.60

Nº	Pregunta	Respuestas				Puntaje Pregunta (PP)	Puntaje Promedio Pregunta (PPP)
		MI	I	PI	NI		
		3	2	1	0		
2	¿El Sistema Experto emite mensajes entendibles?	2	1	2	0	10	2.00
3	¿El Sistema Experto está divido en módulos?	1	4	0	0	11	2.20
4	¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?	1	3	1	0	10	2.00
5	¿El Sistema Experto permite emitir reportes de manera personalizada?	1	1	3	0	8	1.60

Tabla Nº 5.11: Resultados consolidados del cuestionario aplicado respecto al Indicador "Facilidad de Uso de la Aplicación" (Post-test)

Pregunta	Puntaje Promedio		D_i	D_i^2
	Pre-Prueba	Post-Prueba		
	PPP_{Ai}	PPP_{Di}		
1	0	2.60	-2.60	6.76
2	0	2.00	-2.00	4.00
3	0	2.20	-2.20	4.84
4	0	2.00	-2.00	4.00
5	0	1.60	-1.60	2.56
Suma	**0**	**10.40**	**-10.40**	**22.16**
Promedio	**0**	**2.08**	**-2.08**	**4.43**

Tabla N° 5.12: Resultados estadísticos para el Indicador Cualitativo "Facilidad de Uso de la Aplicación"

e. Cálculo de la Desviación Estándar Muestral

Valor	Antes	Después
Promedio Aritmético Muestral	$PN_A = 0$	$PN_D = \frac{10.40}{5} = 2.08$

Tabla Nº 5.13: Media y Varianza Muestral para Indicador "Facilidad de Uso de la Aplicación"

f. Cálculo del Valor Crítico de t

Valor	Cálculo
Desviación Estándar Muestral	$S^2_D = \frac{8\times22.16-(-10.40)^2}{5\times(5-1)} = 0.132$
Cálculo Estadístico de la Prueba	$t_c = \frac{-10.40\times\sqrt{5}}{\sqrt{0.132}} = -12.802$

Tabla Nº 5.14: Valor Crítico de t para Indicador "Facilidad de Uso de la Aplicación"

g. Conclusión

Puesto que t_c = -12.802 calculado es menor que $t_{0.05}$ = -2.132 y ***estando este valor dentro de la región de rechazo***, entonces ***se rechaza H_o y por consiguiente se acepta H_a.***

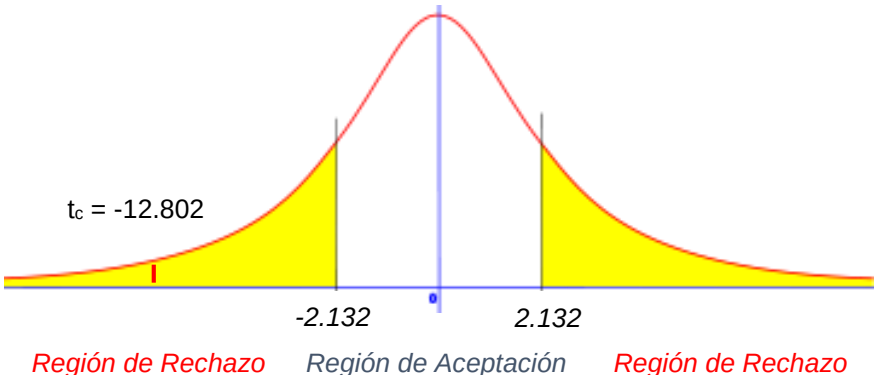


Figura Nº 5.5: Valor crítico de t para Indicador "Facilidad de uso del sistema experto"

Se concluye que ***es fácil usar*** el Sistema Experto.

5.3. Prueba de Hipótesis para el Indicadores Cuantitativos

5.3.1. Indicador "Cantidad de vulnerabilidades identificadas"

a. Definición de Variables

- V_A = 0, no existe un procedimiento que identifique la cantidad de vulnerabilidades antes de la Implementación del Sistema Experto.
- V_D: Cantidad de vulnerabilidades identificadas después de la Implementación del Sistema Experto.

b. Hipótesis Estadística

- Hipótesis H_0: La cantidad de vulnerabilidades identificadas antes de la Implementación del Sistema Experto es mayor o igual a la cantidad de vulnerabilidades identificadas después de la Implementación del Sistema Experto ($H_0 \geq H_a$).
- Hipótesis H_a: La cantidad de vulnerabilidades identificadas antes de la Implementación del Sistema Experto es menor a la cantidad de vulnerabilidades identificadas después de la Implementación del Sistema Experto ($H_0 < H_a$).

c. Valores Tabulados

Los valores obtenidos para este indicador se encuentran en el Anexo Nº 3 Subtítulo 1.

d. Cálculo Estadístico de la Prueba

Valor	Antes	Después
Media Aritmética Muestral	$\overline{X_A} = 0$	$\overline{X_D} = \frac{189}{5} = 37.8$
Varianza Muestral	$\sigma_A^2 = 0$	$\sigma_D^2 = \frac{1038.8}{(5-1)} = 259.70$

Tabla Nº 5.15: Media y Varianza Muestral para Indicador 6

Valor	Valor
Cálculo Estadístico de la Prueba	$Z_c = \frac{(0-37.8)}{\sqrt{\left[\frac{0}{5}+\frac{259.7}{5}\right]}} = \frac{-37.8}{\sqrt{51.94}} = -5.24$
Valor Critico de Z (En Tablas)	$Z_{(\alpha)} = Z_{(0.05)} = Z_{(0.95)} = 1.65$

Tabla Nº 5.16: Comparación de Z para Indicador 6

e. Conclusión

Puesto que $Z_c = -5.24$ calculado es menor que $Z_\alpha = 1.65$ y estando dentro de la región de aceptación, entonces *se rechaza H_0 y por consiguiente se acepta H_a.*

Se concluye entonces que la cantidad de vulnerabilidades identificadas después de la implementación del Sistemas Experto es mayor que la cantidad de vulnerabilidades identificadas antes de la implementación del Sistema Experto.

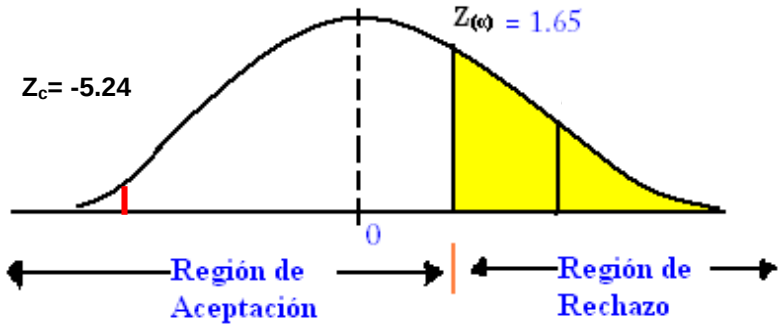


Figura Nº 5.6: Región de Aceptación y Rechazo para la Prueba de Hipótesis del Indicador 5

5.3.2. Indicador "Cantidad de amenazas identificadas"

a. Definición de Variables

- A_A = 0, no existe un procedimiento que identifique la cantidad de amenazas antes de la implementación del Sistema Experto.
- A_D: Cantidad de amenazas identificadas después de la Implementación del Sistema Experto.

b. Hipótesis Estadística

- Hipótesis H_0: La cantidad de amenazas identificadas antes de la Implementación del Sistema Experto es mayor o igual la cantidad de amenazas identificadas después de la Implementación del Sistema Experto ($H_0 \geq H_a$).
- Hipótesis H_a: La cantidad de amenazas identificadas antes de la Implementación del Sistema Experto es menor la cantidad de amenazas identificadas después de la Implementación del Sistema Experto ($H_0 < H_a$).

c. Valores Tabulados

Los valores obtenidos para este indicador se encuentran en el Anexo Nº 3 Subtítulo 2.

d. Resultados de la Hipótesis

Valor	Antes	Después
Media Aritmética Muestral	$\overline{X_A} = 0$	$\overline{X_D} = \frac{189}{5} = 37.8$
Varianza Muestral	$\sigma_A^2 = 0$	$\sigma_D^2 = \frac{2113.4}{(5-1)} = 528.35$

Tabla Nº 5.17: Media y Varianza Muestral para Indicador 6

Valor	Valor
Cálculo Estadístico de la Prueba	$Z_c = \frac{(0-37.8)}{\sqrt{\left[\frac{0}{5}+\frac{528.25}{5}\right]}} = \frac{-37.8}{\sqrt{185.67}} = -3.68$
Valor Critico de Z (En Tablas)	$Z_{(\alpha)} = Z_{(0.05)} = Z_{(0.95)} = 1.65$

Tabla Nº 5.18: Comparación de Z para Indicador 6

e. Conclusión

Puesto que Z_c = -3.68 calculado es menor que Z_α = 1.65 y estando este valor dentro de la región de aceptación, entonces se rechaza H_0 y por consiguiente se acepta H_a se concluye entonces que la cantidad de amenazas identificadas después de la implementación del Sistema Experto es mayor a la cantidad de amenazas identificadas antes de la implementación del Sistema Experto.

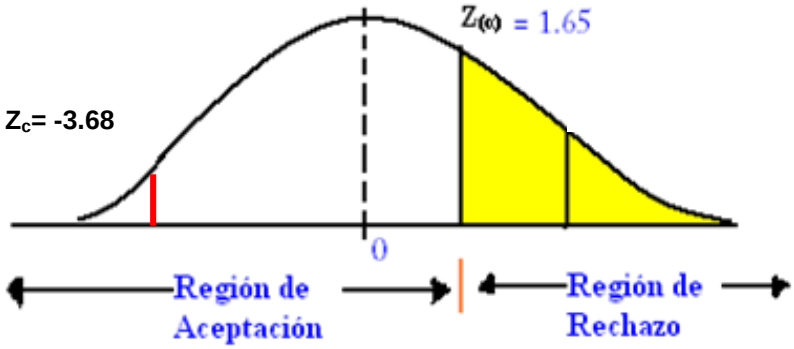


Figura Nº 5.7: Región de Aceptación y Rechazo para la Prueba de Hipótesis del Indicador 6

5.4. Discusión de Resultados

Como puede apreciarse en las Tablas N° 5.19 y 5.20, todos los indicadores han demostrado un aumento significativo:

	Antes		Después		Nivel de Impacto		Resultado del
Indicadores Cualitativos	**Puntaje (0-3)**	**Porcentaje**	**Puntaje (0-3)**	**Porcentaje**	**Diferencia**	**Porcentaje**	**Experimento**
Disponibilidad del Informe de Auditoría	0.00	0.00%	1.67	55.56%	1.67	55.56%	Aumentó
Integridad del Informe de Auditoría	0.00	0.00%	1.67	55.56%	1.67	55.56%	Aumentó
Confidencialidad del Informe de Auditoría	0.00	0.00%	2.44	81.33%	2.44	81.33%	Aumentó
Facilidad de uso del Sistema Experto	0.00	0.00%	2.08	69.33%	2.08	69.33%	Aumentó

Tabla Nº 5.19: Resultados de los Indicadores Cualitativos

	Cantidad		Nivel de Impacto		Resultado del
Indicadores Cuantitativos	**Antes**	**Después**	**Diferencia**	**Porcentaje**	**Experimento**
Cantidad de vulnerabilidades identificadas	0.00	189.00	189.00	189.00%	Aumentó
Cantidad de amenazas identificadas	0.00	88.00	88.00	88.00%	Aumentó

Tabla Nº 5.20: Resultados de los Indicadores Cuantitativos

Se deduce entonces que la implementación del Sistema Experto para la Auditoría de Seguridad de la Información mejora significativamente la identificación de amenazas y vulnerabilidades de los activos de información.

VI. CONCLUSIONES

6.1 Las metodologías investigadas convergen en un esquema de desarrollo de tres etapas: (1) Adquisición del conocimiento, (2) Representación del conocimiento y (3) Programación simbólica, cada una de ellas plantea el desarrollo del sistema con un ciclo de vida dividido en fases, validación de resultados, establecimiento de hitos de control, entre otros; algunos de los lineamientos para su evaluación fueron la calidad y disponibilidad de la información bibliográfica, sin embargo lo importante fue identificar cuál de ellas era más adaptable a los objetivos y tiempos del proyecto.

6.2 Las fuentes consideradas para formar la base de conocimiento del Sistema Experto fueron los criterios de auditoría mayor usados para auditorías en seguridad de la información, tanto para entidades públicas como privadas y los lineamientos del ámbito legal peruano para seguridad de la información, por lo cual se seleccionaron los siguiente criterios de auditoría: NTP ISO 27001:2013, NTP ISO 27002:2013 y COBIT 5, y el conocimiento propio de los expertos en Auditoría de Seguridad de la Información: Ing. Jaime Eduardo Díaz Sánchez, Ing. Juan Carlos Miranda Robles y Lic. Bruno Barbieri Gambini.

6.3 La determinación de la viabilidad del desarrollo del Sistema Experto estuvo basada en la evaluación de la disponibilidad, cantidad y calidad de las fuentes de conocimiento, tiempo para el desarrollo del proyecto, beneficios y costos de implementación, resultado: viabilidad del proyecto y desarrollo de tesis.

6.4 La metodología de John Durkin obtuvo mayor puntaje en la evaluación de lineamientos para el desarrollo de Sistemas Expertos (Capítulo IV 4.1.4. Adaptar una Metodología para el desarrollo del SE), por lo cual se tomó como metodología base para el desarrollo, asimismo se agregaron y/o

modificaron algunas etapas, actividades y artefactos de la metodología de desarrollo ICONIX.

6.5 Se concluye que la evaluación de la aplicación del Sistema Experto en una Auditoría de Seguridad de la Información, mejora significativamente la identificación de amenazas y vulnerabilidades de los activos de información.

VII. RECOMENDACIONES

7.1 Evaluar nuevas fuentes de conocimiento que mejoren la evaluación de Seguridad de la Información y revisar la base de conocimiento actual en busca de mejorar la calidad actual de la información y de representación del conocimiento.

7.2 Revisar el nivel de detalle en la evaluación de seguridad de la información, el modelo actual revisa aspectos de seguridad basado en controles de los criterios de auditoría, la propuesta es evaluar la seguridad de la información por activo de información lo cual permitirá al Sistema Experto procesar información específica que mejore la toma decisiones y reportes.

7.3 Plantear el rediseño del motor de inferencia en caso que la estructura de la información cambie o así lo requiera, sin dejar de lado la participación del personal experto en auditorías; el modelo actual de procesamiento del sistema no requiere de un motor robusto por el diseño y estructura de la representación del conocimiento y sus formatos de evaluación.

7.4 Si bien la forma de evaluación del sistema está basada en listas de verificación de aspectos de seguridad, es conveniente que la persona que cumpla el rol de Auditor dentro del Sistema Experto no descuide la verificación y validación de la información proporcionado por los auditados, siempre que sea pertinente y si la pregunta lo amerite.

7.5 Ingresar la mayor cantidad de información posible al momento de responder una pregunta de auditoría, tales como el método usado para su resolución (respecto a lo que se esté evaluando) y las formas de verificación y validación del mismo, estos datos permitirán alimentar al sistema experto de información que luego podrá convertirse en conocimiento.

VIII. REFERENCIAS

- Alonso, F. J. (1996). *Software engineering and knowledge engineering: Towards a common life cycle. Journal of Systems and Software.*
- Angele, J. F. (1993). Model-based and Incremental Knowledge Engineering: The MIKE Approach. *IFIP TC12 Workshop on Artificial Intelligence from the Information Processing Perspective* (págs. 139-168). Madrid: Elsevier.
- Badaró, S., Javier Ibañez, L., & Agüero, M. (2013). *Sistemas Expertos: Fundamentos, Metodologías y Aplicaciones.* Argentina.
- Brulé, J. & Bount, A. (1989). *Knowledge Acquisition.* New York: Mc. Graw - Hill.
- Buchanan, B.G.; , Barstow, R.; , Betchal, R.; , Bennet, J.; , Clancey, W.; , Kulikowski, C. (1983). Constructing an expert system. *Building Expert, 50*, 127-167.
- Durkin, J. (1994). *Expert Systems: Design and Development.* Maxwell: Macmillan.
- Escrig, M., Pacheco, J., & Toledo, F. (2001). *El Lenguaje de Programación Prolog.*
- González, A. &. (1993). *The Engineering of Knowledge based systems: Theory and Practice.* USA: Prentice – Hall.
- Grover, M. (1983). A Pragmatic Knowledge Acquisition Methodology. *VIII International Joint Conference On Artificial Intelligence*, (págs. 436 – 438). Germany.
- INDECOPI, C. d. (2013). *Norma Técnica Peruana NTP-ISO/IEC 27001 2013.* Lima.
- INDECOPI, C. d. (2013). *Norma Técnica Peruana NTP-ISO/IEC 27002 2013.* Lima, Perú.
- ISACA, (. S. (2012). *Cobit 5 Objetivos de Control para la Información y las Tecnologías Relacionadas.*
- Kendall, J., & Kendall, M. (2011). *Análisis y diseño de Sistemas.* México D.F.: Pearson Education.

- Martínez, R. G. (1992). *Construcción de Sistemas Expertos.* Argentina: Imprenta del CEI-UBA.
- Pazos, J. (1996). *Introducción a la Ingeniería del Conocimiento.*
- Piattini Velthuis, D. P. (2001). *Auditoría Informática: Un enfoque práctico* (Segunda ed.). Alfa Omega.
- Salazar Say, G. (2005). *Utilización de las Técnicas de Auditoría Asistida por Computadora.* Guatemala.
- Schreiber, G. A. (1999). *Knowledge Engineering and Management: The CommonKADS Methodology.* USA: MIT Press.
- Weiss, S. &. (1984). *Sistemas Expertos.* Prentice – Hall.

IX. ANEXOS

9.1 ANEXO Nº 1

9.1.1 Respuestas Entrevistado 1, Indicador 1, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Cómo calificaría el acceso al Informe de Auditoría?	1			
2	¿El Informe de Auditoría puede ser accedido desde cualquier lugar?	1			
3	¿El Informe de Auditoría puede ser accedido a cualquier hora?		1		
4	¿El Informe de Auditoría puede ser exportado a un archivo local?			1	
5	¿El Informe de Auditoría puede ser requerido por correo electrónico?		1		
6	¿El Informe de Auditoría puede ser requerido de manera impresa?				1

9.1.2 Respuestas Entrevistado 2, Indicador 1, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Cómo calificaría el acceso al Informe de Auditoría?	1			
2	¿El Informe de Auditoría puede ser accedido desde cualquier lugar?		1		
3	¿El Informe de Auditoría puede ser accedido a cualquier hora?	1			

4	¿El Informe de Auditoría puede ser exportado a un archivo local?		1		
5	¿El Informe de Auditoría puede ser requerido por correo electrónico?			1	
6	¿El Informe de Auditoría puede ser requerido de manera impresa?			1	

9.1.3 Respuestas Entrevistado 3, Indicador 1, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Cómo calificaría el acceso al Informe de Auditoría?	1			
2	¿El Informe de Auditoría puede ser accedido desde cualquier lugar?	1			
3	¿El Informe de Auditoría puede ser accedido a cualquier hora?	1			
4	¿El Informe de Auditoría puede ser exportado a un archivo local?		1		
5	¿El Informe de Auditoría puede ser requerido por correo electrónico?		1		
6	¿El Informe de Auditoría puede ser requerido de manera impresa?		1		

9.1.4 Respuestas Entrevistado 4, Indicador 1, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Cómo calificaría el acceso al Informe de Auditoría?		1		
2	¿El Informe de Auditoría puede ser accedido desde cualquier lugar?	1			
3	¿El Informe de Auditoría puede ser accedido a cualquier hora?	1			
4	¿El Informe de Auditoría puede ser exportado a un archivo local?			1	
5	¿El Informe de Auditoría puede ser requerido por correo electrónico?		1		
6	¿El Informe de Auditoría puede ser requerido de manera impresa?			1	

9.1.5 Respuestas Entrevistado 5, Indicador 1, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Cómo calificaría el acceso al Informe de Auditoría?		1		
2	¿El Informe de Auditoría puede ser accedido desde cualquier lugar?		1		
3	¿El Informe de Auditoría puede ser accedido a cualquier hora?	1			
4	¿El Informe de Auditoría puede ser exportado a un archivo local?			1	
5	¿El Informe de Auditoría puede ser requerido por correo electrónico?			1	
6	¿El Informe de Auditoría puede ser requerido de manera impresa?			1	

9.1.6 Respuestas Entrevistado 1, Indicador 2, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?		1		
2	¿La información obtenida es la oficial?	1			
3	¿La información obtenida es certificada?	1			
4	¿La información obtenida puede ser validada posteriormente?		1		
5	¿La información obtenida puede ser verificada posteriormente?		1		
6	¿La información obtenida es actual (de reciente producción)?	1			
7	¿El Informe de Auditoría puede ser deducido de la información obtenida?		1		

9.1.7 Respuestas Entrevistado 2, Indicador 2, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?	1			
2	¿La información obtenida es la oficial?		1		
3	¿La información obtenida es certificada?		1		
4	¿La información obtenida puede ser validada posteriormente?		1		
5	¿La información obtenida puede ser verificada posteriormente?		1		
6	¿La información obtenida es actual (de reciente producción)?		1		
7	¿El Informe de Auditoría puede ser deducido de la información obtenida?			1	

9.1.8 Respuestas Entrevistado 3, Indicador 2, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?		1		
2	¿La información obtenida es la oficial?	1			
3	¿La información obtenida es certificada?	1			
4	¿La información obtenida puede ser validada posteriormente?			1	
5	¿La información obtenida puede ser verificada posteriormente?			1	
6	¿La información obtenida es actual (de reciente producción)?		1		
7	¿El Informe de Auditoría puede ser deducido de la información obtenida?		1		

9.1.9 Respuestas Entrevistado 4, Indicador 2, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?		1		
2	¿La información obtenida es la oficial?	1			
3	¿La información obtenida es certificada?		1		
4	¿La información obtenida puede ser validada posteriormente?			1	
5	¿La información obtenida puede ser verificada posteriormente?		1		
6	¿La información obtenida es actual (de reciente producción)?		1		
7	¿El Informe de Auditoría puede ser deducido de la información obtenida?			1	

9.1.10 Respuestas Entrevistado 5, Indicador 2, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Informe de Auditoría se basa en fuentes confiables (personas y documentos)?		1		
2	¿La información obtenida es la oficial?		1		
3	¿La información obtenida es certificada?		1		
4	¿La información obtenida puede ser validada posteriormente?			1	
5	¿La información obtenida puede ser verificada posteriormente?			1	
6	¿La información obtenida es actual (de reciente producción)?				1
7	¿El Informe de Auditoría puede ser deducido de la información obtenida?		1		

9.1.11 Respuestas Entrevistado 1, Indicador 3, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Existe un acuerdo de confidencialidad entre las partes intervinientes?	1			
2	¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?		1		
3	¿El Informe de Auditoría es distribuido solo a personal debidamente autorizado?		1		
4	¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?		1		
5	¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?		1		

9.1.12 Respuestas Entrevistado 2, Indicador 3, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Existe un acuerdo de confidencialidad entre las partes intervinientes?	1			
2	¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?	1			
3	¿El Informe de Auditoría es distribuido solo a personal debidamente autorizado?	1			
4	¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?		1		
5	¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?	1			

9.1.13 Respuestas Entrevistado 3, Indicador 3, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Existe un acuerdo de confidencialidad entre las partes intervinientes?	1			
2	¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?		1		
3	¿El Informe de Auditoría es distribuido solo a personal debidamente autorizado?		1		
4	¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?	1			
5	¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?	1			

9.1.14 Respuestas Entrevistado 4, Indicador 3, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Existe un acuerdo de confidencialidad entre las partes intervinientes?		1		
2	¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?	1			
3	¿El Informe de Auditoría es distribuido solo a personal debidamente autorizado?		1		
4	¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?	1			
5	¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?	1			

9.1.15 Respuestas Entrevistado 5, Indicador 3, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿Existe un acuerdo de confidencialidad entre las partes intervinientes?		1		
2	¿El Informe de Auditoría es accedido solo por el personal debidamente autorizado?		1		
3	¿El Informe de Auditoría es distribuido solo a personal debidamente autorizado?		1		
4	¿El Informe de Auditoría físico es entregado por un canal seguro y confiable?		1		
5	¿El Informe de Auditoría utiliza mecanismos de encriptación que aseguren su protección digital?		1		

9.1.16 Respuestas Entrevistado 1, Indicador 4, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Sistema Experto usa un lenguaje entendible?		1		
2	¿El Sistema Experto emite mensajes entendibles?			1	
3	¿El Sistema Experto está divido en módulos?		1		
4	¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?		1		
5	¿El Sistema Experto permite emitir reportes de manera personalizada?			1	

9.1.17 Respuestas Entrevistado 2, Indicador 4, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Sistema Experto usa un lenguaje entendible?	1			
2	¿El Sistema Experto emite mensajes entendibles?	1			
3	¿El Sistema Experto está divido en módulos?		1		
4	¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?		1		
5	¿El Sistema Experto permite emitir reportes de manera personalizada?		1		

9.1.18 Respuestas Entrevistado 3, Indicador 4, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Sistema Experto usa un lenguaje entendible?	1			
2	¿El Sistema Experto emite mensajes entendibles?			1	
3	¿El Sistema Experto está divido en módulos?		1		
4	¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?		1		
5	¿El Sistema Experto permite emitir reportes de manera personalizada?			1	

9.1.19 Respuestas Entrevistado 4, Indicador 4, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Sistema Experto usa un lenguaje entendible?		1		
2	¿El Sistema Experto emite mensajes entendibles?		1		
3	¿El Sistema Experto está divido en módulos?		1		
4	¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?			1	
5	¿El Sistema Experto permite emitir reportes de manera personalizada?			1	

9.1.20 Respuestas Entrevistado 5, Indicador 4, Evaluación del Indicadores

Nº	Pregunta	Respuestas			
		MI	I	PI	NI
		3	2	1	0
1	¿El Sistema Experto usa un lenguaje entendible?	1			
2	¿El Sistema Experto emite mensajes entendibles?	1			
3	¿El Sistema Experto está divido en módulos?	1			
4	¿El Sistema Experto distribuye correctamente la información en sus interfaces de usuario?	1			
5	¿El Sistema Experto permite emitir reportes de manera personalizada?	1			

9.2 ANEXO Nº 2: Entrevista al Ing. Eduardo Francisco Alonso Pérez.

SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTP ISO 27001 Y 27002 Y COBIT 5

El presente proyecto plantea el desarrollo de un Sistema Experto en Seguridad de la información basado en los criterios de auditoría NTP 27001, NTP 27002 Y COBIT 5, el cual será desarrollo bajo tecnologías libres web, manejado por personal experto y no experto de auditoría.

Se plantean las siguientes interrogantes:

1. ¿Es necesario utilizar un lenguaje de programación lógica como PROLOG o podría usarse otro tipo de lenguaje de programación?

No necesariamente, la ventaja del Prolog es que ya tiene incorporado el motor de inferencia, lo mas importante en la base de conocimiento. El motor de inferencia se puede implementar en cualquier lenguaje y si el razonamiento a utilizar es Forward Ch., la implementación es relativamente sencilla.

2. De usarse uno de propósito general, ¿Se perdería la esencia de Sistema Experto?

No; siempre y cuando se mantenga el principio básico de los S.E de la independencia entre la BC y el Motor de inferencia. De esta manera se puede incrementar, corregir, etc la BC sin modificar la aplicación.

3. ¿Se puede implementar un Sistema Experto bajo un escenario de procesamiento de transacciones tal igual como los Sistemas de Información? Es decir, las preguntas que se formulen a los usuarios pueden ser redactadas, almacenadas y modificadas en el tiempo y sobretodo, debería adaptarse a cualquier estándar o buena práctica de Auditoría.

Sí, siempre y cuando se diseñe de forma tal que la BC sea independiente de la aplicación (motor de inferencia). La aplicación utilizará formularios para ingresar los datos (hechos) de forma general y el motor de inferencia (Forward chaining) obtendrá estos datos y la BC para obtener los resultados.

Experto Mgtr Eduardo F. Alonso Pérez