ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN – SEGURIDAD DE LA INFORMACIÓN – SGSI, EN EMTELSA S.A. E.S.P

NATALIA ANDREA VALENCIA CARDONA

UNIVERSIDAD DE MANIZALES
FACULTAD DE INGENIERIA
INGENIERIA DE SISTEMAS Y TELECOMUNICACIÓNES
MANIZALES- CALDAS
2008

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN – SEGURIDAD DE LA INFORMACIÓN – SGSI, EN EMTELSA S.A. E.S.P

NATALIA ANDREA VALENCIA CARDONA

Trabajo de Grado para optar al titulo de Ingeniera de Sistemas y Telecomunicaciones

Presidente
LUIS CARLOS CORREA ORTIZ
Ingeniero Electrónico

UNIVERSIDAD DE MANIZALES
FACULTAD DE INGENIERIA
INGENIERIA DE SISTEMAS Y TELECOMUNICACIONES
MANIZALES- CALDAS
2008

Nota de aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Manizales 21- Julio- 2008

A mi familia, gracias por ser el Soporte e Impulso en cada momento de mi vida...

CONTENIDO

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE TABLAS

Pág.

LISTADO DE ANEXOS

Pág.

ANEXO A. MANUAL DE USUARIO

RESUMEN

El proyecto que se describe a continuación contiene la información que documenta el proceso de elaboración del SISTEMA DE GESTION- SEGURIDAD DE LA INFORMACIÓN para EMTELSA S.A E.S.P. Después del levantamiento de la información, etapa inicial, la definición explicita de cada uno de los conceptos incorporados en el sistema permitió el modelado del mismo, evitando redundancias y ofreciéndole al usuario la mayor claridad y funcionalidad. Al final de este proceso se obtuvo un diagrama Entidad - Relación, base fundamental para el desarrollo del proyecto.

Teniendo en cuenta que el alcance de este trabajo abarcaba solo algunos aspectos de la implementación, se desarrollaron una serie de formularios -Activo, Evaluación del Riesgo, Amenazas y Controles-, bajo la plataforma NET Framework y manejando bases de datos en Oracle usando el SQL Developer por medio de package.

ABSTRACT

The Project described below contains the information that documenting the making process of MANAGEMENT SYSTEM-INFORMATION SECURITY for EMTELSA S.A E.S.P. After compilation of data, initial stage, the explicit definition of each of the concepts incorporated in the system allowed the modeling of it, avoiding redundancies and offering to user greater clearness and functionality. At the end of this process a Entity- Relation diagram was obtained, fundamental base for the development of project.

Taking into account that the reach of this document covered just any implementation aspects, a serie of formats – Active, Risk Valuation, Menaces and Controls was developed using .Net Framework plataform and managing databases in Oracle using the SQL Developer by means of package.

RESUMEN ANALÍTICO

Título del Proyecto	ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN – SEGURIDAD DE LA INFORMACIÓN – SGSI, EN EMTELSA S.A. E.S.P
Autor(es)	Valencia Cardona, Natalia Andrea cachi42@hotmail.com
Presidente	Correa Ortiz, Luís Carlos lcarloscorrea@hotmail.com Ingeniero Electrónico, Docente Facultad de Ingeniería, Universidad de Manizales
Tipo de documento	Trabajo de Grado
Referencia documento	Natalia Andrea Valencia Cardona. ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN – SEGURIDAD DE LA INFORMACIÓN – SGSI, EN EMTELSA S.A. E.S.P. Manizales, 2008, 194 Páginas. Ingeniera de Sistemas y Telecomunicaciones. Universidad de Manizales. Facultad de Ingeniería. Centro de Investigaciones
Institución	Programa de Ingeniería de Sistemas y Telecomunicaciones, Facultad de Ingeniería, Universidad de Manizales
Palabras claves	Activo, Control, Amenaza, Evaluación de Riesgo, Norma
Descripción	Este trabajo presenta la implementación de la norma NTC-ISO/IEC 27001 como sistema de información que permita controlar los activos de una empresa.
Contenido	RESUMEN, ABSTRACT, INTRODUCCIÓN, DESCRIPCIÓN DEL ÁREA PROBLEMÁTICA, OBJETIVOS, JUSTIFICACIÓN, MARCO TEÓRICO, METODOLOGÍA, SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN), RESULTADOS, CONCLUSIÓN, RECOMENDACIONES, BIBLIOGRAFÍA, ANEXO

Metodología	Inicialmente se estableció el levantamiento de información que fue la etapa más importante donde se establecieron los parámetros necesarios para entender y modelar completamente el sistema (teniendo en cuenta que solo algunos módulos serian finalmente desarrollados) de una forma dinámica. Una vez teniendo el diagrama terminado fue iniciado el desarrollo de los formularios que están enfocados bajo la plataforma .NET Framework y manejando bases de datos en Oracle usando SQL Developer por medio de procedimientos almacenados (package), los cuales permitieron recurrir a la reutilización de código en consultas SQL que podían duplicarse en el sistema para ciertos formularios.
Conclusiones	No se debe olvidar que para desarrollar con éxito esta norma en cualquier empresa es necesario enfrentarse primero al análisis diseño e implantación que difiere notablemente en todas las empresas dependiendo de sus definiciones internas de seguridad, estándares de procesos que posiblemente nunca se habían evaluado y en los cuales todos los interesados deben aportar y aprobar para poder homogenizar el proceso global de seguridad de la empresa.
Anexos	ANEXO A MANUAL DE USUARIO, ANEXO B MANUAL TÉCNICO

INTRODUCCIÓN

El siguiente trabajo describe y da muestra del alcance, objetivos, procesos, políticas, procedimientos documentadas de EMTELSA S.A. E.S.P. que soportan el Sistema de Gestión de la Seguridad de la Información SGSI, todo esto dando cumplimiento y basándose en la **Norma Técnica Colombiana NTC-ISO/IEC 27001.**

Este es un proceso de delicado análisis, documentación e implementación, se encuentra relacionado con cada una de las áreas de la empresa, debe ser conocido por toda la organización y debe incluir todo activo dentro de la empresa, esté en uso o fuera de rotación ya que en este orden es posible garantizar adecuados niveles de protección que permitan las buenas prácticas de la empresa.

Teniendo como propósito la aplicación de dicha norma, el proceso usado se basa en el modelo PHVA (Planificar- Hacer- Verificar- Actuar) enfoque esencial y necesario para el éxito del proyecto que permite una resolución óptima de los problemas identificados, se reconocen las actividades desarrolladas dentro del Sistema de Gestión de la Seguridad de la Información que proporcionan confianza de los procesos, basados en el cumplimiento de las condiciones de seguridad establecidas y en los requerimientos y expectativas de los usuarios directos dentro de la empresa y partes interesadas.

1. DESCRIPCIÓN DEL ÁREA PROBLEMÁTICA

Se puede entender como seguridad un estado de cualquier sistema (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro se debe dotar de tres características al mismo:

- Integridad.
- Confidencialidad.
- Disponibilidad.

La **seguridad informática** generalmente consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera establecida por la empresa. Es por este motivo que hoy en día, la información en las organizaciones es un insumo fundamental para el manejo de los negocios y se hace vital para la supervivencia de las mismas, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), adquiere una especial importancia en los procesos de manejo y tratamiento de la información en cualquier organización y mas cuando estas son implementadas siguiendo normas de reconocimiento internacional.

Partiendo de esta necesidad se hace visible la importancia de que todos los Departamentos de Tecnología cuenten como parte de su estructura organizativa, con el apoyo de un área responsable de la seguridad informática debidamente delimitada, a fin de que se atiendan adecuadamente las funciones que corresponde con ese campo.

Así mismo, se profundiza en una serie de aspectos relacionados con el tema de la seguridad informática, que evidencian la necesidad que tiene la empresa de una metodología dedicada exclusivamente a atender las tareas que se requieren para minimizar los riesgos que la Tecnología de Información acarrea.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Realizar el análisis, el diseño, e implementación del **Sistema de Gestión de la Seguridad de la Información** de TODOS los ACTIVOS de EMTELSA S.A. E.S.P. [*]

2.2. OBJETIVOS ESPECÍFICOS

Definir todas aquellas medidas de mitigación del riesgo, también llamados controles, que se representan a través de la definición de mecanismos físicos, lógicos o documentales que actúan sobre la amenaza que puede llegar a impactar el activo.

Realizar el análisis y diseño del sistema bajo OMT, bajo lenguaje UML, siguiendo los parámetros establecidos para este fin por EMTELSA S.A E.S.P.

Implementar un modelo de control tecnológico que permita optimizar, mantener y garantizar una seguridad razonable para proteger la inversión instalada con niveles adecuados de funcionalidad.

Implementar el sistema de gestión, en lo referente a Activo, Evaluación del Riesgo, Amenazas y Controles.

[*] El nombre Sistema de gestión de la Seguridad de la información fue empleado fundamentándose en los parámetros que propone la norma NTC-ISO/IEC 27001.

3. JUSTIFICACIÓN

La implantación en la sociedad de las tecnologías de la comunicación e información, está produciendo cambios sorprendentes en la estructura que el hombre se ha venido planteando de la humanidad, los efectos y alcances de este proyecto generan un importante modelo de innovación en cuanto al manejo de la información y como estructurar (Distribuir, Relacionar y Organizar) los procesos que propone la norma ISO/IEC 27001, proponiendo así un modelo de control tecnológico funcional que permita ejecutar los procesos de forma practica generando altos niveles de eficacia una vez sea puesto en funcionamiento el software.

Este no sólo se sitúa en el terreno de la información y comunicación, sino que lo sobrepasan para llegar a provocar y proponer cambios a todo nivel y en diferentes entornos. Esto es debido a que no sólo se centran en la captación de la información, sino también, y es lo verdaderamente significativo, a las posibilidades que tienen para manipularla, almacenarla y distribuirla.

Es por esta razón que los cambios tecnológicos y de negocios que han surgido y que surgirán en la empresa, requieren el fortalecimiento de la auditoria y la seguridad informática, (dependencia tecnológica de terceros, negocios en función de la tecnología...) ya que la seguridad no es un gasto, es una inversión que protege la inversión instalada.

Si la tecnología es la base de la empresa, se debe invertir en su adecuada protección, para de esta forma estar en capacidad de garantizar Confidencialidad, Integridad y Disponibilidad.

La seguridad informática y la auditoria de sistemas deben ser un instrumento de valor agregado al negocio de la empresa donde las actividades desarrolladas dentro del Sistema de Gestión de la Seguridad de la Información deben proporcionan confianza de los procesos, basados en el cumplimiento de las condiciones de seguridad establecidas y en los requerimientos y expectativas de los clientes internos y partes interesadas.

El interés de un Sistema de Gestión de la Seguridad de la Información no es garantizar la seguridad –que nunca podrá ser absoluta- sino garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

Un SGSI demuestra la necesidad de estudiar los riesgos a los que está sometida toda la información a su vez evalúa qué nivel de riesgo asume, implanta controles (no sólo tecnológicos, sino también organizativos) para aquellos riesgos que superan dicho nivel, documenta las políticas y procedimientos relacionados y entra en un proceso continuo de revisión y mejora de todo el sistema.

4. MARCO TEÓRICO

4.1. EMTELSA

La empresa EMTELSA S.A E.S.P. inició sus labores en agosto de 1996, debido al proceso de transformación que se realizó en las Empresas Públicas de Manizales.

Han transcurrido más de diez años desde entonces, tiempo en el cual EMTELSA ha sufrido muchas transformaciones convirtiéndose en lo que ahora se denomina la fusión UNE EMTELSA, esta misma ha crecido notablemente, no sólo en el incremento de su personal, sino en los productos y servicios que esta empresa de telecomunicaciones ofrece a la comunidad. Es una empresa pujante, líder en los procesos comunicacionales más importantes de la región, posee un amplio portafolio de servicios y tecnología de avanzada en telefonía, televisión e Internet, que han beneficiado en la última década a miles de usuarios en el departamento de Caldas

Es importante para EMTELSA como una empresa seria mantener la seguridad de todos y cada uno de los activos que posee, buscando con esto reducir las amenazas que podrían traerles pérdidas millonarias de dinero, tiempo y mala ejecución de sus procesos internos, es por esta razón que EMTELSA decide hacerse cargo de estandarizar sus procesos y contar con adecuados niveles de seguridad tecnológica, que deberá abarcar todas las tecnologías informáticas y de telecomunicaciones que posee la empresa implementando la norma NTC-ISO/IEC 27001 (Sistemas de Gestión de Seguridad de la Información –SGSI-)

4.2 SEGURIDAD DE LA INFORMACIÓN

La **seguridad informática** generalmente consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera establecida por la empresa.

Es por este motivo que hoy en día, la información en las organizaciones es un insumo fundamental para el manejo de los

negocios y se hace vital para la supervivencia de las mismas, la implementación de un sistema de gestión de seguridad de la información (SGSI), adquiere una especial importancia en los procesos de manejo y tratamiento de la información en cualquier organización y más cuando estas son implementadas siguiendo normas de reconocimiento internacional.

Partiendo de esta necesidad se hace visible la importancia de que todos los Departamentos de Tecnología cuenten como parte de su estructura organizativa, con el apoyo de un área responsable de la seguridad informática debidamente delimitada, a fin de que se atiendan adecuadamente las funciones que corresponde con ese campo.

Así mismo, se profundiza en una serie de aspectos relacionados con el tema de la seguridad informática, que evidencian la necesidad de que nuestra empresa tenga una metodología dedicada exclusivamente a atender las tareas que se requieren para minimizar los riesgos que la Tecnología de Información acarrea.

El propósito principal de este proyecto es involucrar a todos los miembros de la empresa como entes activos de la seguridad de la información, colaborando con el proceso que se viene adelantando en cuanto a este tema. De esta forma el software está enfocado directamente a efectuar un conjunto de controles que tienen la finalidad de mantener la confidencialidad, integridad y confiabilidad de la información electrónica; así como resguardar los activos tecnológicos de una organización.

Para ello, dicha seguridad comprende aspectos relacionados con políticas, estándares, sanas prácticas, controles, valoración de riesgos, capacitación y otros elementos necesarios para la adecuada administración de los recursos tecnológicos y de la información que se maneja por esos medios.

En ese sentido, la seguridad informática salvaguarda los activos contra daños, destrucción, uso no autorizado o robo; mantiene la integridad de los datos, permitiendo que la información electrónica sea oportuna, precisa, confiable y completa; ayuda a alcanzar las metas institucionales y permite el uso eficiente de los recursos tecnológicos destinados para el procesamiento de la información.

El usuario final de éste, dependiendo de su cargo en la empresa, estará en capacidad de efectuar el ingreso de activos, así como

de hacer modificaciones a activos existentes, tendrá acceso a informes detallados que le mostrarán el análisis de riesgos y amenazas que posee. Este análisis le dará una idea de la forma en la cual se encuentra protegido el activo frente a amenazas o riesgos, que planes de contingencia pueden ser empleados para mitigar el riesgo y están a disposición para la oportuna corrección del mismo, además de esto calificará la amenaza dándole la posibilidad al usuario de valorar con claridad cuales activos son críticos para la empresa y podrían causarle pérdidas millonarias si no son modificados correctamente.

4.3. DEFINICIÓN ESTRATEGIA METODOLÓGICA EMTELSA S.A E.S.P ÁREA SISTEMA DE GESTIÓN-SEGURIDAD DE LA INFORMACIÓN (SGSI)

Teniendo en cuenta las características de desarrollo en área SGSI y manejando los principales aspectos de la Metodología OMT - Metodología de Análisis y Diseño Orientadas a Objetos (de primera generación) madura y eficiente- y Lenguaje de Notación Unificado (UML), se desarrolló una Metodología orientada al manejo eficiente y rápido de documentación y diagramas.

4.3.1 ESPECIFICACIÓN DE PROCESO

Actividad 1. FASE DE DEFINICIÓN DE REQUERIMIENTOS.

- **Enunciado:** Descripción detallada que representa la situación actual. Mediante esta se delimita la problemática que se va a tratar, se plantea una posible solución evidenciando la necesidad de plantear una solución a la misma haciendo énfasis en la novedad e interés que esta representa en el campo de aplicación.

- **Requerimientos Funcionales del Sistema:** Se refieren a las funciones y/o operaciones a desarrollar. Para la Especificación de Requerimientos Funcionales se propone realizar un Listado de las funciones del sistema con su Código de Referencia y su Grado de Visibilidad (Categoría).

- **Cronograma de Actividades:** Determinar las actividades a desarrollar en las fechas correspondientes, así como la entrega de los avances del proyecto basándose en los alcances del proyecto.

- **Conclusiones:** Observaciones y conclusiones para el desarrollo del sistema.

Actividad 2. FASE DE ANÁLISIS

- **Modelo Funcional:** En esta etapa se realiza una definición del modelo de casos de uso del sistema.

Casos de Uso: Los casos de uso se emplean para capturar información de cómo un sistema o negocio trabaja, o de cómo se desea que trabaje. Esta técnica es usada para captar el comportamiento deseado del sistema en desarrollo sin tener que especificar como se implementa este comportamiento. Los casos de uso proporcionan un medio para que los desarrolladores, los usuarios finales y los expertos del dominio lleguen a una comprensión común del sistema. Los Casos de Uso Actuales representaran la visión inicial del sistema a plantear.

Para el caso concreto de la Estrategia Metodológica a aplicarse en EMTELSA S.A., los casos de uso principales de un diagrama se escribirán de arriba abajo y los actores que intervienen en su operación estarán a los lados. En caso tal de especificar relaciones de casos de uso primarios con casos de uso secundarios, el sentido de la relación se realizará de izquierda a derecha.

Descripción de Casos de Uso: Este formato muestra una descripción para ayudar a comprender los Casos y SubCasos de Uso.

Diagramas de Casos de Uso. Estos diagramas representan la funcionalidad completa de un sistema (o una clase) mostrando su interacción con los agentes externos. Esta representación se hace a través de las relaciones entre los actores (agentes externos) y los casos de uso (acciones) dentro del sistema. Los diagramas de casos de uso definen conjuntos de funcionalidades afines que el sistema debe cumplir para satisfacer todos los requerimientos que tiene a su cargo. Se pueden visualizar como las funciones más importantes que la aplicación puede realizar o como las opciones presentes en el menú de la aplicación.

- **Modelo Estático**

Diagrama de Clases: Estructura del sistema que se va a modelar.

- **Modelo Dinámico:**

Es aquel que muestra las interacciones de un usuario con el sistema. Interacción es una cadena de mensajes enviados entre los objetos en respuesta a un evento generado por el usuario sobre la aplicación. Los diagramas de interacción pueden ser Diagramas de Secuencia.

Diagrama de Secuencia

El Diagrama de Secuencia es uno de los diagramas más efectivos para modelar interacción entre objetos en un sistema. Un diagrama de secuencia se modela para cada caso de uso. El diagrama de secuencia contiene detalles de implementación, incluyendo los objetos y las clases, y mensajes pasados entre los objetos.

Típicamente uno examina la descripción de un caso de uso para determinar qué objetos son necesarios para la implementación del escenario. Si tienes modelada la descripción de cada caso de uso como una secuencia de varios pasos, entonces puedes "caminar sobre" esos pasos para descubrir qué objetos son necesarios para que se puedan seguir los pasos.

Actividad 3. FASE DE DISEÑO DEL SISTEMA

- **Casos de Uso Finales**

En esta primera etapa de la fase de diseño del sistema se toman los casos de uso iniciales para ser refinados si así el sistema lo requiere. Generalmente al culminar la etapa de Análisis, aparecen nuevas especificaciones no tenidas en cuenta en el momento de modelar los casos de uso en la etapa anterior.

- **Especificación de la Arquitectura del Sistema**

La arquitectura de una aplicación es la vista conceptual de la estructura de esta. En las aplicaciones que manejan Bases de Datos generalmente se trabaja en un ambiente Cliente–Servidor.

- **Diagramas de Implementación**

Un diagrama de implementación muestra la estructura del sistema y la relación entre los diferentes componentes del mismo.

- **Diagrama de Componentes**

Un diagrama de componentes muestra las dependencias lógicas entre componentes software, sean éstos componentes fuentes, binarios o ejecutables.

Se representa como un grafo de componentes software unidos por medio de relaciones de dependencia (generalmente de compilación). Puede mostrar también contenencia de entre componentes software e interfaces soportadas.

Actividad 4. FASE DE DISEÑO DE OBJETOS

- **Diagrama Entidad – Relación**

El Diagrama Entidad - Relación es el modelo conceptual más utilizado para el diseño conceptual de bases de datos. El Diagrama Entidad - Relación está formado por un conjunto de conceptos que permiten describir la realidad mediante un conjunto de representaciones gráficas y lingüísticas. La diferencia de este tipo de diagrama con lo Diagramas de Clases radica en el hecho que el Diagrama Entidad – Relación se centra solo en los datos, los Diagramas de Clases van un poco mas allá, permitiendo el modelado de comportamiento.

4.4 NORMA ISO/IEC 27001

La norma "ISO/IEC 27001:2005- Information Technology Security Techniques", es la evolución certificable del código de buenas prácticas ISO 17799. ICONTEC desde el año 2003 viene desarrollando la normalización nacional de técnicas de seguridad de la información, que se inició con la adopción a escala nacional de las normas BS 7799-2 e ISO 17799 durante el año 2003. Con la publicación por parte de la ISO de la norma ISO 27001 en el año 2005, el ICONTEC emprende la labor de adoptarla como una norma nacional y en el mes de marzo del 2006 es ratificada como la NTC-ISO/IEC 2700.

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un (SGSI), siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones.[*]

Las empresas tienen la necesidad de gestionar la información en todos los niveles que posea, teniendo en cuenta que el

[*] La información mas completa acerca de la norma ISO/IEC 27001 puede encontrarla en el libro Nueve Claves para el Éxito, una visión general de la implementación de la norma.

conocimiento o desconocimiento de la misma, ayuda a las personas y a las organizaciones a alcanzar el éxito o el fracaso.
Por esta razón la implementación de un Sistema de Gestión de seguridad de la Información (SGSI), adquiere una especial importancia en los procesos de manejo y tratamiento de la información de las organizaciones, y más cuando se implementan basados en normas de reconocimiento Internacional.

¿Para qué sirve un SGSI?
La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, delincuentes informáticos o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.[*]

[*] La información más completa acerca del manejo de un SGSI puede encontrarla en siguiente dirección de Internet www.iso27000.es.

FIGURA 1. FLUJO NORMAL DE UN SGSI

4.4.1 OBJETIVOS DE CONTROL

Los objetivos de control que serán descritos a continuación se han obtenido directamente de la norma NTC-ISO/IEC 17799:2005, numerales 5 al 15 y pretenden dar claridad en el propósito especifico para el que se ha establecido algún tipo de control dentro de la norma, pueden ser tenidos en cuenta o no por la organización dependiendo de sus propios intereses.

Actividad 1. POLÍTICA DE SEGURIDAD	
Política de seguridad de la información	Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Tabla 1. Política de Seguridad

Actividad 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
Organización Interna	Objetivo: Gestionar la seguridad de la información dentro de la organización.
Partes Externas	Objetivo: Mantener la seguridad de la información de los servicios de procesamiento de información de la organización a los cuales tiene acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

Tabla 2. Organización de la Seguridad de la Información

Actividad 3. GESTIÓN DE ACTIVOS	
Responsabilidad por los activos	Objetivo: Lograr y mantener la protección adecuada de los activos organizacionales.
Clasificación de la información	Objetivo: Asegurar que la información recibe el nivel de protección adecuado.

Tabla 3. Gestión de Activos

Actividad 4. SEGURIDAD DE LOS RECURSOS HUMANOS	
Antes de la contratación laboral	Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.
Durante la vigencia de la contratación laboral	Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén consientes de las amenazas y preocupaciones

	respecto a la seguridad de la información, sus responsabilidades y sus deberes y que estén equipados para apoyar la política de seguridad de la organización en transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.
Terminación o cambio de contratación laboral	Objetivo: Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.

Tabla 4. Seguridad de los Recursos Humanos

Actividad 5. SEGURIDAD FÍSICA Y DEL ENTORNO	
Áreas seguras	Objetivo: Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.
Seguridad de los equipos	Objetivo: Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.

Tabla 5. Seguridad Física y del Entorno

Actividad 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Procedimientos operacionales y responsabilidades	Objetivo: Asegurar la operación correcta y segura de los servicios de procesamiento de información.
Gestión de la prestación del servicio por terceras partes	Objetivo: Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio,

	de conformidad con los acuerdos de prestación del servicio por terceras partes.
Planificación y aceptación del Sistema	Objetivo: Minimizar el riesgo de fallas de los sistemas.
Protección contra códigos maliciosos y móviles	Objetivo: Proteger la integridad del software y de la información.
Respaldo	Objetivo: Mantener la disponibilidad de la información y de los servicios de procesamiento de información.
Gestión de la seguridad de las redes	Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
Manejo de los medios	Objetivo: evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.
Intercambio de la Información	Objetivo: Mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.
Servicios de comercio electrónico	Objetivo: Garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.
Monitoreo	Objetivo: Detectar actividades de procesamiento de la información no autorizadas.

Tabla 6. Gestión de Comunicaciones y Operaciones

Actividad 7. CONTROL DE ACCESO	
Requisito del negocio para el control de acceso	Objetivo: Controlar el acceso a la información.
Gestión del acceso de usuarios	Objetivo: Asegurar el acceso de usuarios autorizados y

	evitar el acceso de usuarios no autorizados a los sistemas de información.
Responsabilidades de los usuarios	Objetivo: Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.
Control de acceso a las redes	Objetivo: Evitar el acceso no autorizado a servicios en red.
Control de acceso al sistema operativo	Objetivo: Evitar el acceso no autorizado a los sistemas operativos.
Control de acceso a las aplicaciones y a la información	Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas de información.
Computación móvil y trabajo remoto	Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

Tabla 7. Control de Acceso

Actividad 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	
Requisitos de seguridad de los sistemas de información	Objetivo: Garantizar que la seguridad es parte integral de los sistemas de información.
Procesamiento correcto en las aplicaciones	Objetivo: Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.
Controles criptográficos	Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.
Seguridad de los archivos del sistema	Objetivo: Garantizar la seguridad de los archivos del Sistema.

Seguridad en los procesos de desarrollo y soporte	Objetivo: Mantener la seguridad del software y de la información del sistema de aplicaciones.
Gestión de la vulnerabilidad técnica	Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

Tabla 8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Actividad 9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	
Reporte sobre los eventos y las debilidades de la seguridad de la información	Objetivo: Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.
Gestión de los incidentes y las mejoras en la seguridad de la información	Objetivo: Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Tabla 9. Gestión de los Incidentes de la Seguridad de la Información

Actividad 10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Aspectos de seguridad de la información, de la gestión de la continuidad del negocio	Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación

	oportuna.

Tabla 10. Gestión de la Continuidad del Negocio

Actividad 11. CUMPLIMIENTO	
Cumplimiento de los requisitos legales	Objetivo: Evitar el incumplimiento de cualquier ley de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.
Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico	Objetivo: Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.
Consideraciones de la auditoria de los sistemas de información	Objetivo: Maximizar la eficacia de los procesos de auditoria de los sistemas de información y minimizar su interferencia.

Tabla 11. Cumplimiento

4.5 ANTECEDENTES

EMTELSA S.A. E.S.P.
La empresa como tal dedicó gran parte de su esfuerzo en campañas de concientización con el fin de hacer comprender a todos los empleados la gran importancia que tiene la seguridad como base de un óptimo funcionamiento, de esta forma se difundió el lema:

"LA SEGURIDAD TECNOLÓGICA ES PARTE INTEGRAL DE NUESTRO NEGOCIO"

La política de seguridad del Sistema de Gestión de la Seguridad de la Información está encaminada a que todos los recursos tecnológicos sean cuidados y aprovechados de la manera más eficiente, por todos los colaboradores, con niveles de seguridad acordes a los recursos financieros, a los requisitos legales y a las obligaciones de seguridad contractuales.

El nivel de riesgo a que quedan expuestos los activos o nivel de riesgo residual, se encuentra evaluado, para cada amenaza por activo, en el Sistema de Información para la Gestión de la Seguridad de las Tecnologías de Información y Comunicaciones

(SIGESTIC, base de datos en Access que permite la recopilación de la información de forma ordenada y entendible).

El Sistema de Gestión de la Seguridad de la Información busca dar un nivel de seguridad adecuado a los recursos tecnológicos de la empresa de tal forma que no estemos totalmente expuestos y se garantice la continuidad de los servicios que se prestan a nuestros clientes. Con base en esta determinación se establecen en la empresa 7 capas o dominios en los cuales esta dividida la empresa y que permiten seleccionar a su vez todos los activos de esta.[1]

NEXTEL S.A

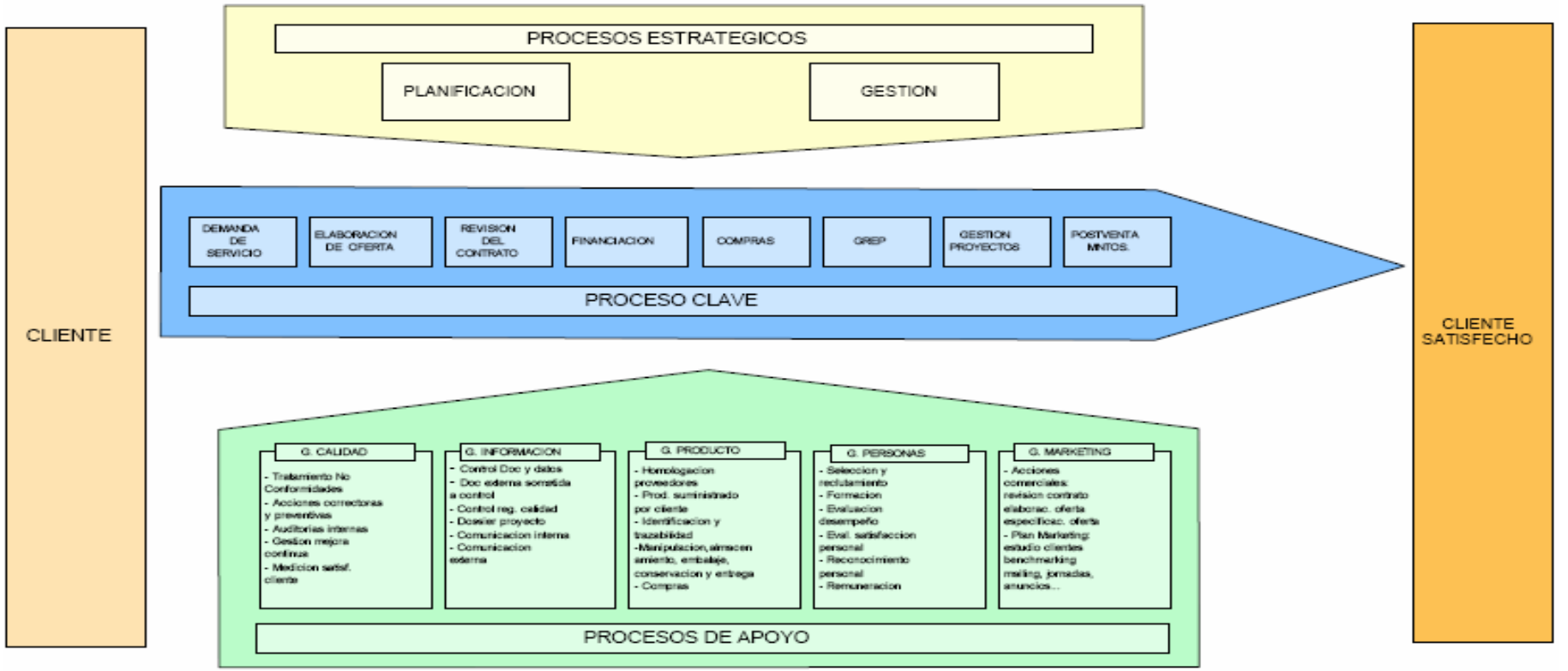
Como empresa de ingeniería telemática, NEXTEL S.A. tiene como objeto ofrecer soluciones globales y abiertas en telecomunicaciones a empresas y organizaciones con necesidades de intercambio de información o de interconexión.
Esta empresa se mueve en un sector en el que la mejora continua es esencial para mantener el nivel de competitividad que goza actualmente, nuestra forma de actuación sigue las pautas del P.D.C.A (planificar, hacer, controlar y actuar), con una constante retroalimentación sobre la gestión de nuestros procesos.
Nextel S.A. es una de las primeras consultoras del mercado en obtener una Certificación para Sistema de Gestión de la Seguridad de la Información bajo un estándar de Seguridad de la Información internacionalmente reconocido: BS 7799-2:2002. La implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en una empresa como Nextel S.A. supone la gestión integral de la seguridad de la información. Esto se consigue mediante planificación, análisis de activos y de riesgos, aplicación de controles técnicos, gestión de recursos humanos, difusión, formación y planes de contingencia. La seguridad de la información implica tanto a la información que está basada en sistemas informáticos o en papel, como a las personas.
Gracias a esta certificación, la empresa se consolida como referente y pionera en el ámbito de la Seguridad de la Información en España, de esta forma puede asegurar a sus clientes que la información que se gestiona en las relaciones de negocio habituales es tratada con la máxima garantía de integridad, confidencialidad y disponibilidad.

[1] EMTELSA S.A. E.S.P. Documentación Interna. Colombia. 2007

Esquema de Proceso

Nextel ha identificado diferentes procesos de negocio claves como:

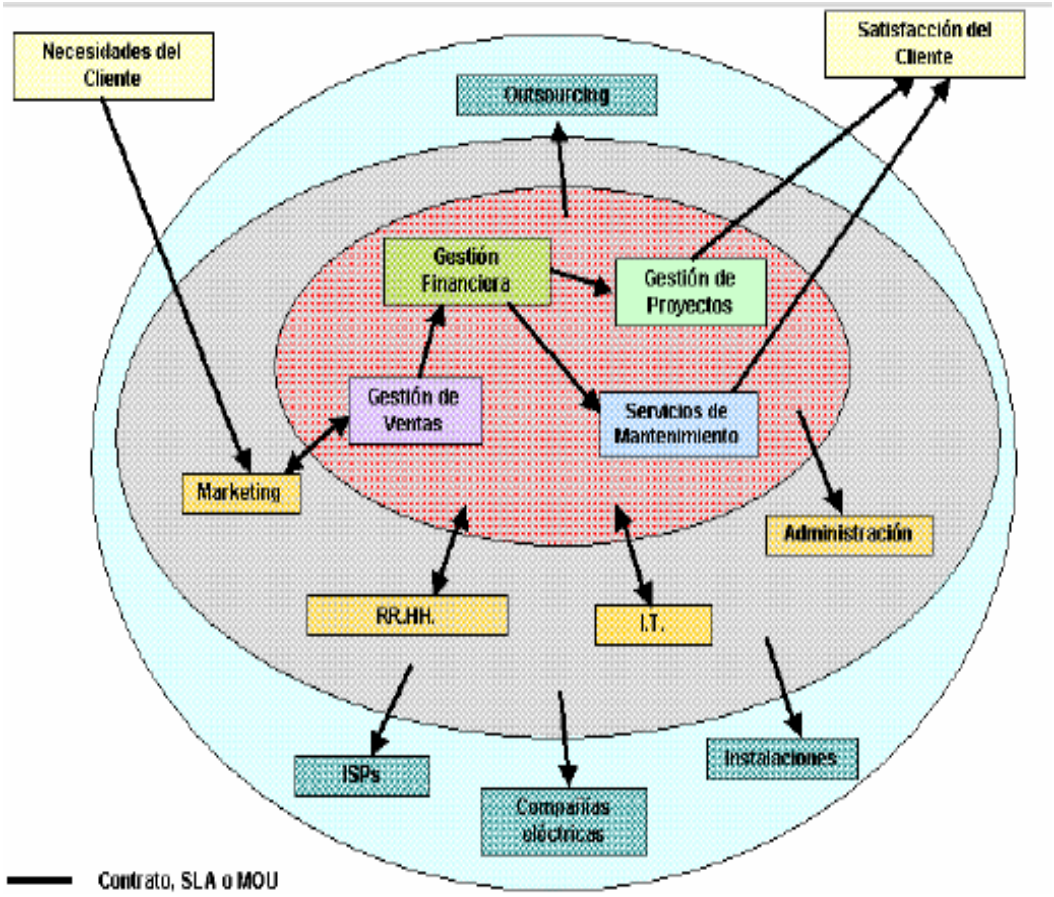
FIGURA 2. PROCESOS DE NEGOCIO EN NEXTEL S.A.



El alcance del SGSI esta enfocado hacia los cuatro procesos clave que se indican a continuación:

1. Gestión de proyectos
2. Servicios de mantenimiento al cliente
3. Gestión financiara
4. Gestión de ventas[2]

FIGURA 3. ESQUEMA DE ALCANCE DEL SGSI EN NEXTEL S.A.



[2] NEXTEL S.A. Certificación de la Seguridad de la Información. [en Línea]. Madrid, España. 2007. Inicio > Empresa > Seguridad de la Información. Disponible en: http://www.nextel.es/aNW/web/cas/empresa/seguridad/index.jsp

START-UP

Para cubrir la urgente necesidad de hacer frente a los riesgos a los que se enfrentan las empresas hoy en día, START-UP, empresa certificada por AENOR según la norma ISO 27001, ofrece sus servicios de consultoría para el diseño y la implantación de un Sistema de Gestión de Seguridad de la Información.

En START-UP diseñamos su plan de seguridad para evitar costosas pérdidas de información, basándonos en una evaluación del riesgo y posterior análisis del mismo, que comprenda todos los niveles de las actividades del negocio y todos los aspectos de sus operaciones. Los resultados de este análisis serán los criterios para elegir los mecanismos que permitan respuestas anticipadas a riesgos emergentes y gestionar efectivamente la prevención, detección y respuesta a incidentes que afecten a la seguridad.

Es muy importante que las políticas de seguridad de los sistemas y redes de información, así como las prácticas, medidas y procedimientos estén coordinadas e integradas para crear un sistema coherente de seguridad.

La información es el principal activo de muchas organizaciones y precisa ser protegida adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio.

En la actualidad las empresas, de cualquier tipo y sector de actividad, se enfrentan cada vez más con riesgos e inseguridades (ya sean físicos o lógicos) de diversas procedencias que pueden dañar de forma importante sus sistemas de información:

- Riesgos físicos: Incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados, etc.
- Riesgos lógicos: Fraudes informáticos, espionaje, virus, ataques de intrusión, denegación de servicios, etc.

Es por esto que se define la Seguridad de la Información como la protección de dicha información de manera que se mantengan su:

- **Confidencialidad**. Para asegurar que sólo quienes estén autorizados puedan acceder a la información

- **Integridad**. Para asegurar que la información y sus métodos de proceso son exactos y completos
  - **Disponibilidad**. Para asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran

La disponibilidad, integridad y confidencialidad de la información son aspectos esenciales para que la organización mantenga su nivel de competencia, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Para proteger la información de una manera coherente y eficiente, es necesario establecer un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos del negocio, que permite asegurar la información frente a la pérdida de confidencialidad, integridad y disponibilidad.

En caso de desastre, el contar con un plan de contingencia reduce notablemente los efectos negativos y permite restablecer en un plazo las actividades habituales y con ellas el flujo de ingresos.

No hay una receta infalible para diseñar un sistema de seguridad, ni existe la seguridad total, pero mediante el proceso de mejora continua del sistema se puede llegar a un nivel muy satisfactorio de seguridad que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que estos ocasionarían si ocurrieran.
Un SGSI cubre los siguientes aspectos de seguridad

FIGURA 4. ASPECTOS DE SEGURIDAD EN START- UP

[3]

[3] START-UP. Normas en Sistema de Gestión de Seguridad de la Información. [en Línea]. Oviedo (Asturias), España. 2007. Inicio>Portada. Disponible en: http://www.seguridadinformacion.com/seguinfo.php

ETICOM

La finalidad de este proyecto es promover un sistema TIC seguro, como medio para consolidar y avanzar en la Sociedad de la información; así como crear una red empresarial capaz de prestar servicios destinados a implantar una política de seguridad entre las empresas, autónomos y profesionales.

OBJETIVO

Implantar un sistema de gestión de seguridad de la información y certificarlo, según la norma UNE-ISO/IEC 27001:2006, en 30 empresas del sector TIC Andaluz

FIGURA 5. GESTION DE LA SEGURIDAD EN PYMETICA SEGURIDAD

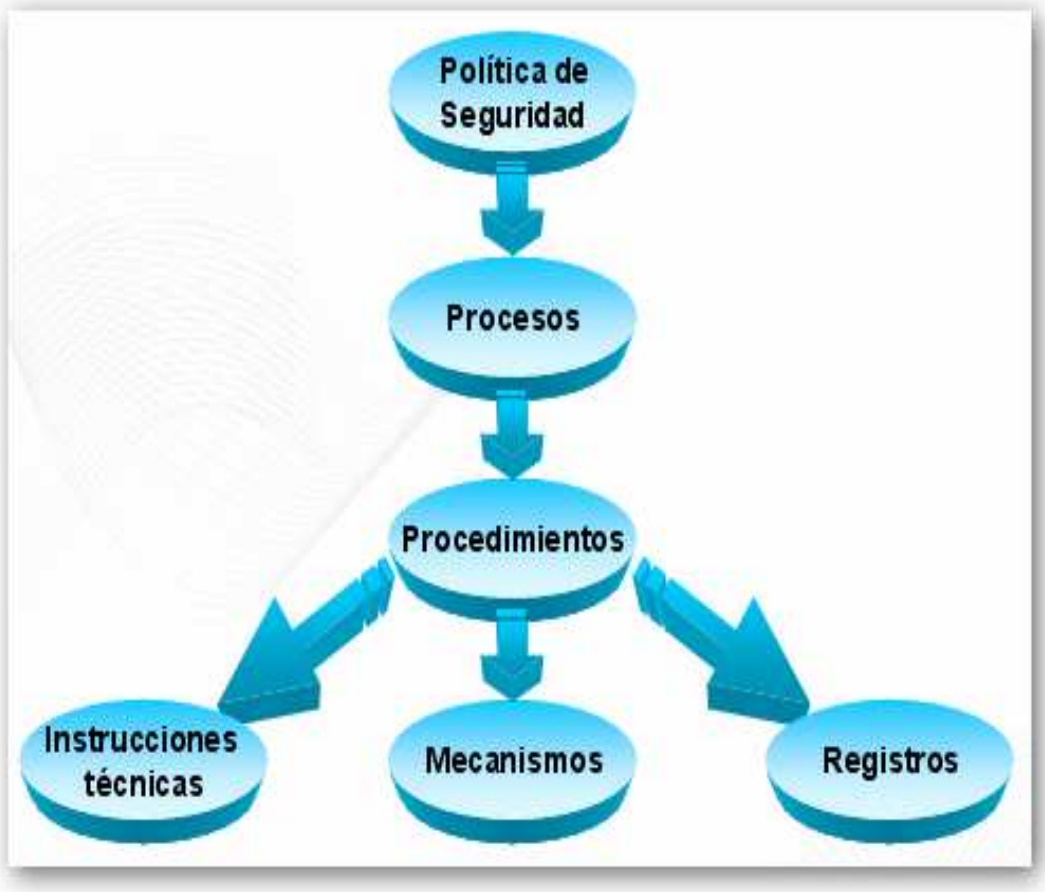


FIGURA 6. MODELO IMPLANTADO EN PYMETICA SEGURIDAD

FASES DEL PROYECTO

- Elaboración del Plan General de seguridad
- Implantación del SGCI
- Validación y seguimiento del SGCI
- Certificación

ELABORACIÓN DEL PLAN GLOBAL DE SEGURIDAD

- Estudio de la situación actual de seguridad
- Formación y concienciación
- Política de Seguridad
- Análisis de riesgos
- Selección de controles

IMPLANTACIÓN DEL SGSI

- Estructura organizativa para la seguridad
- Implantación de controles
- Plan de contingencia
- Arquitectura de red

VALIDACIÓN Y SEGUIMIENTO DEL SGSI

- Validación de la estructura de Seguridad
- Validación de Políticas y Directivas de Seguridad
- Auditoria Interna[4]

[4] ETICOM. Pymetica Seguridad. [en Línea]. Andalucía España. 2007. Disponible en: http://www.eticom.com/upload/noticias/PROYECTO%20PYMETICA%20SEGURIDAD.%20ETICOM.ppt

5. METODOLOGÍA

5.1 TIPO DE TRABAJO

Este proyecto corresponde a un desarrollo a un desarrollo tecnológico enmarcado en el área de conocimiento electrónica telecomunicaciones e informática en el campo de conocimiento desarrollos empresariales.

5.2 PROCEDIMIENTO

Teniendo en cuenta los parámetros ya establecidos por la Universidad y los intereses particulares de EMTELSA S.A. E.S.P. fueron desarrolladas actividades que encadenadas moldearon finalmente lo que es ahora el SISTEMA DE GESTION-SEGURIDAD DE LA INFORMACIÓN. Inicialmente se estableció el levantamiento de información que fue la etapa más importante donde se establecieron los parámetros necesarios para entender y modelar completamente el sistema (teniendo en cuenta que solo algunos módulos serian finalmente desarrollados) de una forma dinámica. En esta etapa se cumplió como labor especifica la aclaración de conceptos entre las partes ya que en muchos casos no se tenía precisión en las definiciones o redundancia de conceptos, nociones o ideas acerca de funcionalidades que debían estar presentes en el sistema.

Gracias a esta labor se pudo dar una correcta orientación al sistema y de esta forma se comenzó a encauzar el desarrollo hacia la parte de análisis que permitió corregir errores y encaminar el software bajo nuevas perspectivas teniendo aún más claridad de lo que se pretendía al hablar de SEGURIDAD DE LA INFORMACIÓN, teniendo estas bases se moldeó el sistema intentando presentarlo al usuario como algo sencillo, eficaz y de gran utilidad para el crecimiento interno como empresa; paralelo a esto se incorporo el diseño de los diagramas siguiendo los lineamientos de OMT, bajo UML , según lo establece EMTELSA, dando como resultado un diagrama final (Diagrama Entidad/Relación) el cual fue estudiado y analizado varias veces, agrupando las observaciones de las personas que estaban al frente del proceso y obteniendo finalmente un diagrama aprobado que cumplió con todas las características y requisitos indispensables para comenzar el desarrollo sin contratiempos.

Una vez teniendo el diagrama terminado fue iniciado el desarrollo de los formularios que están enfocados bajo la plataforma .NET Framework y manejando bases de datos en Oracle usando SQL Developer por medio de procedimientos almacenados (package), los cuales permitieron recurrir a la reutilización de código en consultas SQL que podían duplicarse en el sistema para ciertos formularios.

Los formularios (Activo, Evaluación del Riesgo, Plan de Mitigación y Controles) -que fueron definidos previamente en el documento presentado ante la Universidad – fueron utilizados por los usuarios finales del sistema, por este motivo fue necesario establecer un entorno visualmente agradable en el cual el usuario pudiera sentirse a gusto y en confianza con el sistema, el entorno visual está programado utilizando el lenguaje que ofrece ASP.NET produciendo una interfaz amigable para usuarios que por primera vez ingresan al sistema.

5.2.1 FASE 1. IDENTIFICACIÓN Y DESCRIPCIÓN DE CONCEPTOS

Actividad 1. CLASIFICACIÓN DE USUARIOS

EMPLEADO:
Persona que desempeña un cargo o trabajo y que a cambio de ello recibe una remuneración.

USUARIO:
Es la persona, organización u otra entidad que depende de los servicios de algún elemento o sistema, esta persona utiliza o trabaja con algún objeto o es destinario de algún servicio público o privado, empresarial o profesional.

ADMINISTRADOR:
El usuario Administrador es aquel que tiene derechos ilimitados sobre la información del sistema (consultar, ingresar, modificar, eliminar) al igual que acceso a todas las opciones de configuración de la aplicación.

USUARIO REGISTRADO:
Se denomina así a la persona que tiene derechos especiales en algún servicio por acreditarse en el mismo mediante un identificador y una clave de acceso, obtenidos previamente al registrar el servicio. Normalmente, un usuario registrado tiene

asignada una cuenta propia que mantiene información personalizada del usuario en el servidor.

Actividad 2. MODELO DE CONTROL TECNOLÓGICO EN EMTELSA S.A. E.S.P. (PHVA)

Siendo el enfoque PHVA (Planificar, Hacer, Verificar, Actuar) un factor esencial y planteado en la mayoría de las normas de calidad para el éxito de los proyectos, se implemento el modelo de control tecnológico siguiendo los parámetros establecidos en la norma ISO27001 de la siguiente manera:

- **Planificar**

  a) Definir el alcance del SGSI.
  b) Definir la política de seguridad de la información.
  c) Definir un enfoque sistemático hacia la evaluación del riesgo.
  d) Realizar una evaluación del riesgo a fin de identificar, dentro del contexto de la política y el alcance del SGSI, los activos de información importantes de la organización y los riesgos que enfrentan.
  e) Evaluar los riesgos.
  f) Identificar y evaluar opciones para el tratamiento de los riesgos.
  g) Seleccionar, para cada enfoque, los objetivos de control y los controles que se van a implementar.
  h) Preparar una declaración de aplicabilidad (DA).

- **Hacer**

  a) Formular el plan de tratamiento de riesgos, su documentación, incluidos procesos planificados y procedimientos detallados.
  b) Implementar el plan de tratamiento del riesgo y controles planificados.
  c) Dar formación apropiada al personal afectado, lo mismo que programas de concientización.
  d) Administrar operaciones y recursos en línea con el SGSI.
  e) Implementar procedimientos que posibiliten la detección pronta de incidentes de seguridad y su resolución.

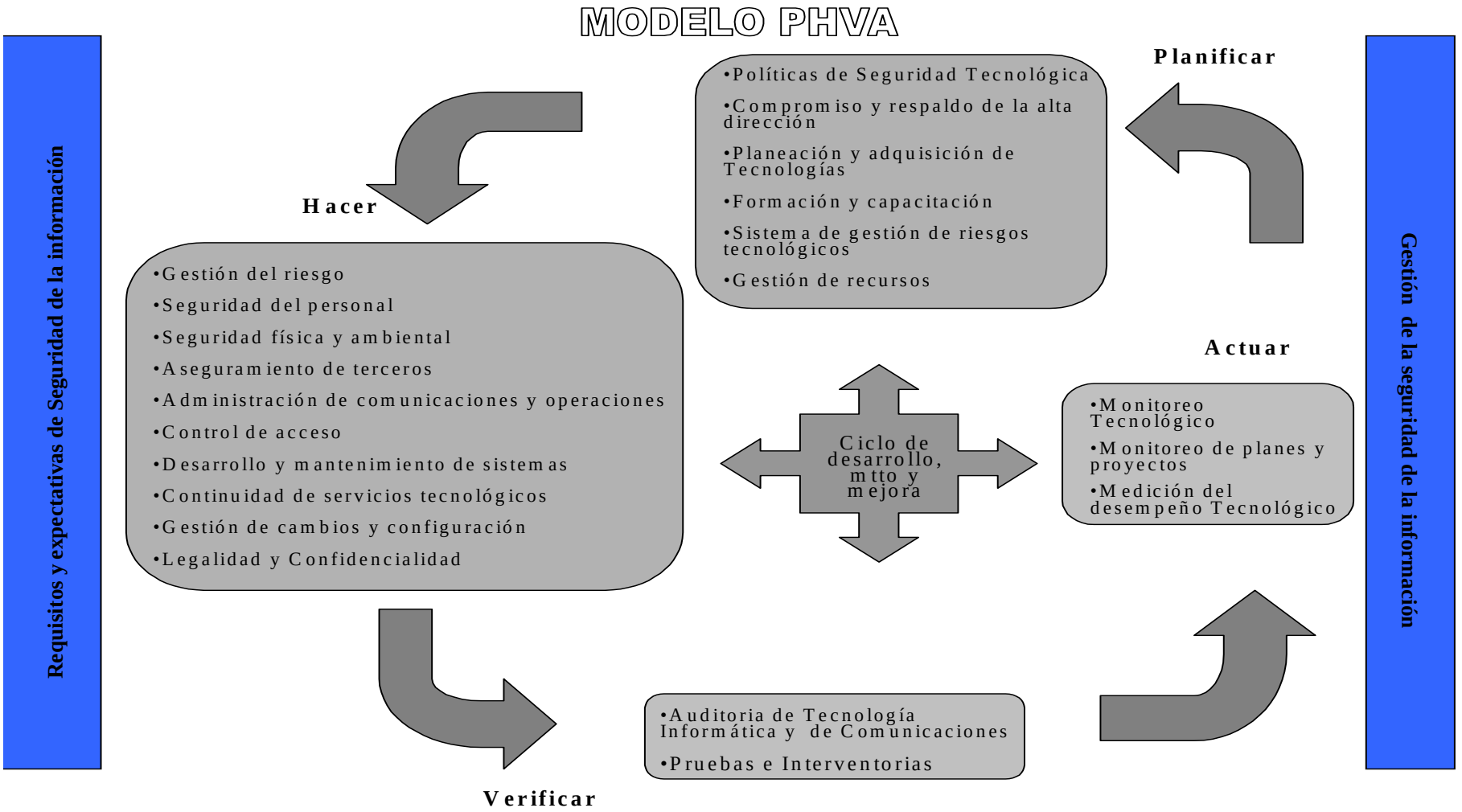
- **Verificar**

La etapa de verificación consta esencialmente de un solo paso (o conjunto de pasos): monitoreo, revisión, ensayo y auditoria. No obstante, estas acciones constituyen un proceso continuo que debe cubrir la totalidad del sistema; y los organismos de certificación buscaran evidencia de por lo menos un ciclo de ensayos y auditorias del SGSI que se haya implementado antes de alguna visita de certificación.

- **Actuar**

La dirección debe revisar los resultados del ensayo y la auditoria, al igual que el SGSI, a la luz del cambiante ambiente de riesgos, la tecnología u otras circunstancias; se deben identificar, documentar e implementar las mejoras del SGSI. En adelante, se realiza un proceso de revisión continua, ensayo adicional e implementación de mejoras, el cual se conoce como "mejora continua".

FIGURA 7. DIAGRAMA MODELO PHVA



Siguiendo estos lineamientos, se definió para Emtelsa el modelo de control tecnológico (controla los activos tecnológicos) para el SGSI, que siendo cíclico, es realizado año tras año.

En la empresa se tienen diferentes activos tecnológicos que necesitan ser evaluados constantemente para demostrar que están siendo utilizados de forma correcta, por las personas correctas y que están cumpliendo con la tarea para la que fueron adquiridos, es decir que la forma de usar y mitigar los riesgos de estos activos tecnológicos dentro de la organización esta generando ganancias y no perdidas.
Para lograr esto los activos tecnológicos son clasificados en las 7 capas que ha definido Emtelsa, para las cuales tiene personal igualmente clasificado y escogido según su nivel de conocimientos por capa ya que estos serán los responsables del buen funcionamiento de los activos tecnológicos que les correspondan.

Una vez clasificados los activos tecnológicos pasan a ser evaluados según sus propias características, las amenazas que poseen y los controles que pueden ser útiles para lograr combatir dichas amenazas, teniendo estos datos claros se hace una evaluación del riesgo que corre el activo ante una amenaza determinada, esta evaluación se hace teniendo en cuenta los siguientes aspectos:[*]

- Probabilidad de ocurrencia
- Impacto que generaría en la empresa
- Riesgo, proximidad de ocurrencia de daño
- Vulnerabilidad, posibilidad de sufrir daño
- Vulnerabilidad residual, posibilidad real de sufrir daño de acuerdo a la aceptabilidad (nivel permitido de vulnerabilidad) que maneja la empresa
- Calificación

Estos aspectos permiten encontrar finalmente una Calificación de riesgo para el activo que puede ser:

- Aceptable
- Tolerable
- Inaceptable
- Inadmisible

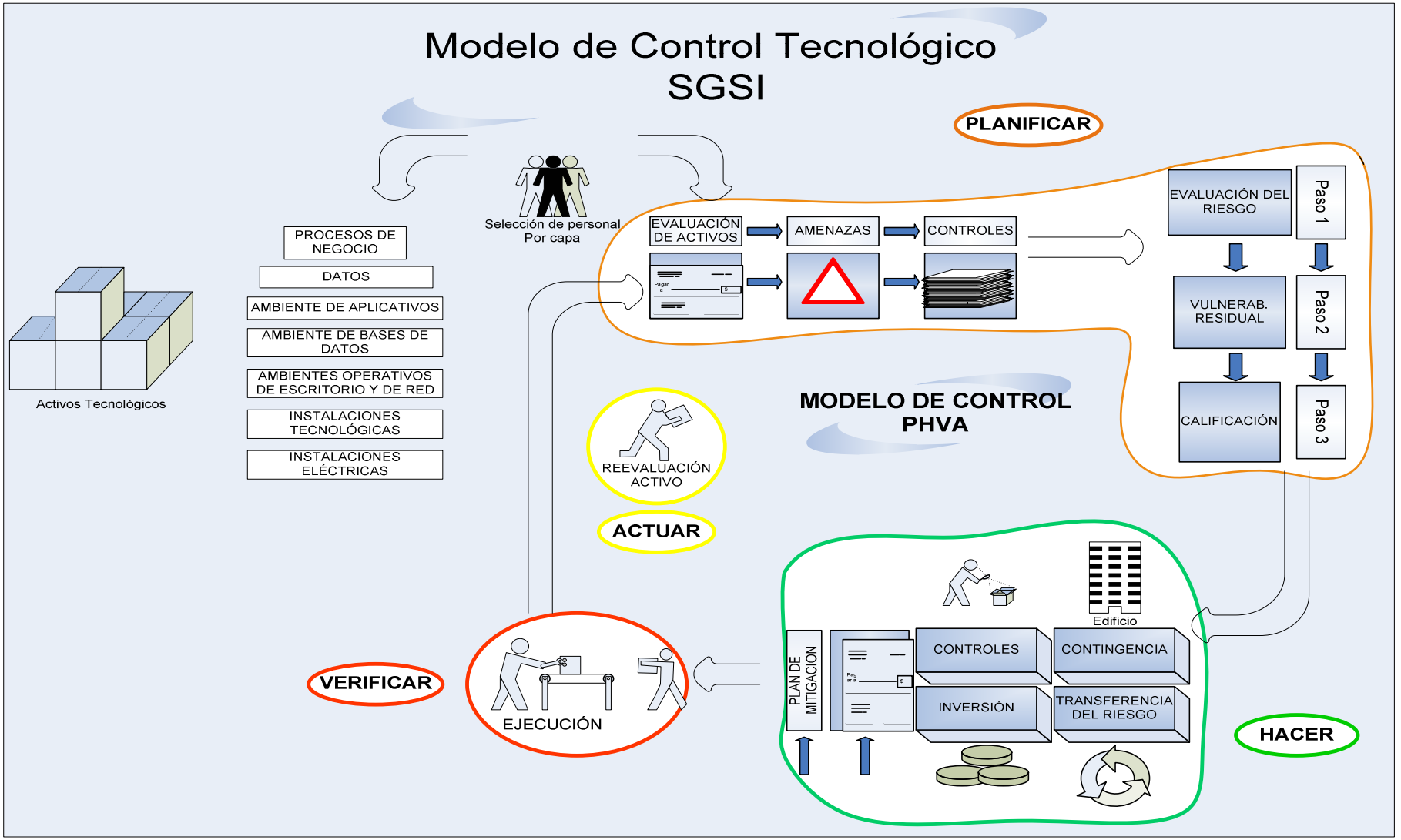
[*] La aclaración y descripción específica del proceso establecido para evaluar el riesgo, se encuentra en el capitulo Evaluación e Impacto del Riesgo en la página 38.

Teniendo esta calificación se generará un Plan de Mitigación (modera el resultado de la calificación) que puede constar de diferentes medidas como:

Hacer uso adecuado de diferentes controles
Generar planes de contingencia (permiten solucionar problemas que se plantean de forma imprevista)
Proponer inversiones necesarias
Transferencia del riesgo (Llevar a terceros el problema para su solución)

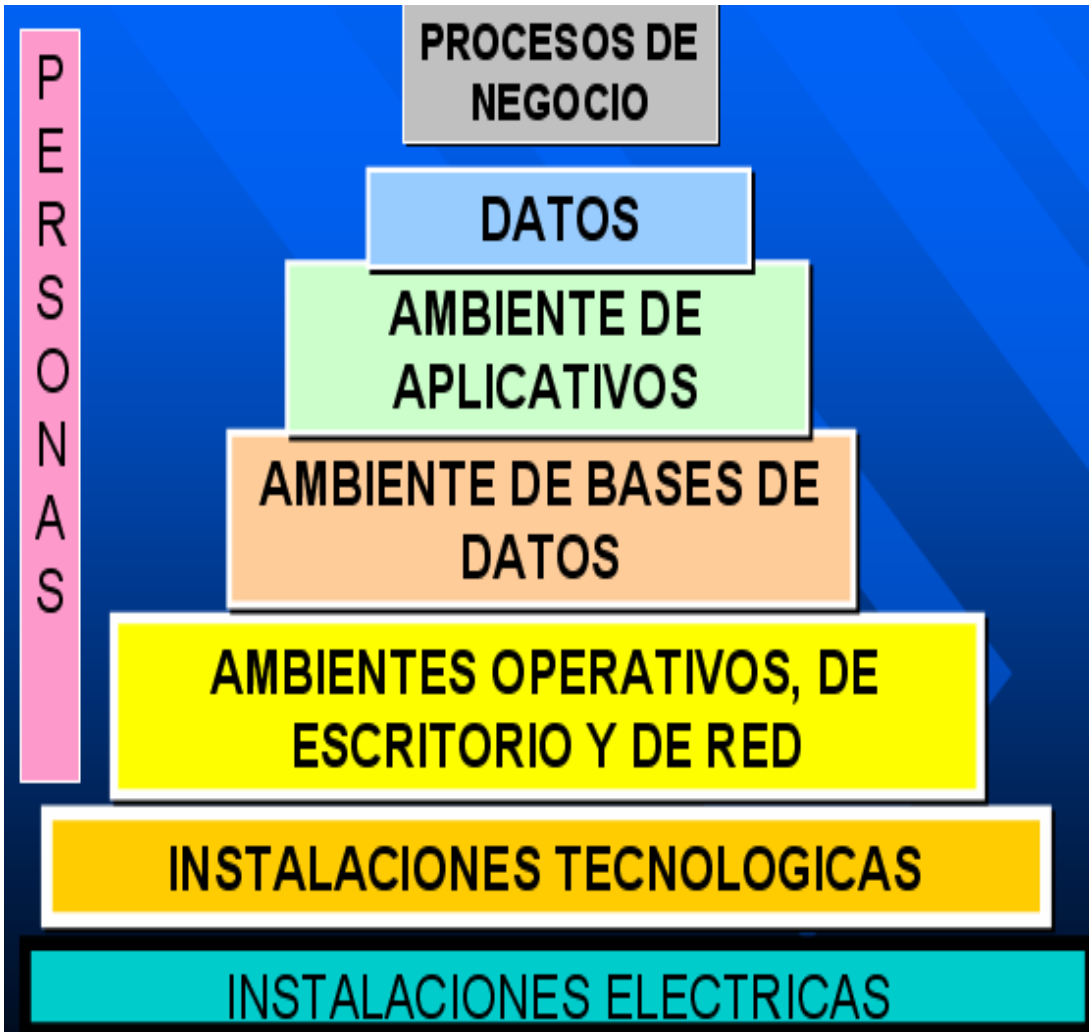
De esta forma se proponen PROCESOS que permiten proteger el activo de posibles amenazas, si es posible antes que estas lo ataquen.
En este punto del modelo el personal de la empresa pasa a EJECUTAR estos planes buscando hacer más bajos los niveles de riesgo y permitiendo tener un activo de utilidad en la empresa, por esta misma razón y en este punto el ciclo vuelve a empezar y el activo es reevaluado, buscando con esto observar si el riesgo ha sido controlado, es decir; que la calificación del riesgo una vez implementados los planes de mitigación, paso de ser Inadmisible a ser Tolerable por ejemplo.
En caso de no ser así se seguirá el flujo normal del ciclo hasta obtener una calificación aceptable según los lineamientos de la empresa.

FIGURA 8. MODELO DE CONTROL TECNOLÓGICO SGSI



Actividad 3. DOMINIOS O CAPAS EMTELSA S.A E.S.P

FIGURA 9. NIVELES DE SEGURIDAD DE EMTELSA



A continuación se hará claridad como por medio de la evaluación del riesgo y la obtención del riesgo residual se han empleado en Emtelsa planes de mitigación para activos cuya calificación no era aceptable según los parámetros establecidos.

- **NIVEL 1**

INSTALACIONES ELÉCTRICAS

Comprende los sitios y elementos que componen el sistema de energía de la empresa y representa el primer nivel de seguridad dentro de la escala de los dominios establecidos para el SGSI.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
• Aparatos o equipos regulados por electricidad.	• Perdida de información por apagado

	• Perdida de energía • Sobrevoltaje
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • UPS • Motogeneradores • Sistemas de energía regulada	

Tabla 12. Ejemplo Instalaciones Eléctricas

Los sistemas eléctricos que soportan las redes de datos, comunicaciones, sistema de seguridad electrónica y en general sistemas sensibles y de alta disponibilidad deben estar soportadas por fuentes de alimentación no interrumpidas (UPS), que le permitan operar aun ante fallos de la red de alimentación normal.

- **NIVEL 2**

INSTALACIONES TECNOLÓGICAS

Este ambiente comprende los sitios en donde están ubicados los diferentes recursos tecnológicos de la empresa y comprenden el primer nivel de seguridad de las tecnologías informáticas.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
• Centro de Cómputo • Granja de Servidores • Sitios donde están ubicadas las centrales telefónicas • Sitios donde están ubicados elementos activos de la red	• Incendio • Terremoto • Inundación • Robo
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • Reforzamiento estructural de los edificios • Implementación de sitios de contingencia alternos • Implementación de planes de evacuación • Señalización de los planes de evacuación	

Tabla 13. Ejemplo Instalaciones Tecnológicas

- **NIVEL 3**

AMBIENTES OPERATIVOS DE ESCRITORIO Y DE RED

Este ambiente es la segunda capa de seguridad, y depende de la primera. Es una de las capas más gruesas y más sensibles a la seguridad, por cuanto en este nivel encontramos 2 subcapas:
La primera subcapa cubre toda la infraestructura de red que permite interconectar diferentes tecnologías en lo relacionado a servidores, equipos, centrales.

La segunda subcapa es la capa de los sistemas operativos de red y los sistemas operativos de escritorio, los cuales son críticos dentro de la infraestructura tecnológica de la empresa.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
• Windows NT Server • Servidores • Windows 2000 Server • Windows XP • AIX • Routers • Switches • Fibra Optica • Cable Coaxial	• Bugs • Robo • Rompimiento • Inadecuada Configuración • Falta de Parches • Afectación de Virus • Inadecuada asignación de permisos
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • Procesos de seguimiento y control de movimiento de equipos • Controles de acceso mediante huellas dactilares • Plataforma de actualización automática WSOURCE • Antivirus	

Tabla 14. Ejemplo Ambientes Operativos de Escritorio y Red

- **NIVEL 4**

CAPA AMBIENTE DE BASES DE DATOS

Este ambiente depende del nivel de seguridad que proporcionan las capas anteriores, y representa los diferentes motores de bases de datos con que cuenta la empresa, tanto a nivel informático como de centrales.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
• Oracle • SQL Server • DBA	• Acceso no Autorizado • Múltiples Súper Usuarios • Configuración Insegura o por Defecto.
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • Alta Disponibilidad • Esquemas de backup de BD • Fortalecimiento de la seguridad en los sistemas de BD • Restricción de permisos	

Tabla 15. Ejemplo Ambiente de Bases de Datos

- **NIVEL 5**

AMBIENTE DE APLICATIVOS

Este ambiente a su vez depende de las capas anteriores, y esta compuesto de 2 subcapas:

La primera subcapa comprende herramientas ofimáticas, utilitarios y herramientas genéricas de software.

La segunda subcapa comprende las aplicaciones empresariales que soportan directamente los procesos de negocio.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
Subcapa 1: • Office • Lotus Notes • Compiladores Subcapa 2: • Sistema de Gestión Financiera • Sistema de Facturación • Sistema de Nomina • Team File	• Alteración de código • Algoritmos Defectuosos • Ilegalidad de Software
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • Aseguramiento de fuentes (Copia de las fuentes originales para ser guardadas en caja fuerte) • Sistema de control de cambios (Cambio en software, se hace un proceso de solicitud y posteriormente se da la autorización para ejecutarlo)	

Tabla 16. Ejemplo Ambiente Aplicativos

- **NIVEL 6**

DATOS

Este ambiente, es uno de los más importantes, dado que es el fin último de todas las TIC'S, dado que a través de estos es que se genera la información operativa, táctica y estratégica que permita que la empresa tome decisiones en los diferentes niveles de la organización.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
• Datos financieros • CDR's	• Borrado Accidental • Borrado Intencional • Pérdida • Modificación no autorizada
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • Esquemas de backup	

• Fortalecimiento de la seguridad (Aumento en la restricción de acceso)

Tabla 17. Ejemplo Datos

- **NIVEL 7**

PROCESOS DE NEGOCIO

Comprende los diferentes procesos de negocio de la empresa que están representados a través de reglas de negocio que se implementan en el software y los datos que se generan a través de la interacción de los diferentes actores del negocio de la empresa.

EJEMPLO DE ACTIVOS	EJEMPLO DE AMENAZAS
• Compras • Presupuesto • Tesorería	• Fraude • Desvío de procesos
CONTROLES IMPLEMENTADOS EN EMTELSA	
• Auditorias internas • Indicativos de cumplimiento o gestión (permite hacer comparación entre evaluaciones de riesgo después de de efectuar los planes de mitigación)	

Tabla 18. Ejemplo Procesos de Negocio

Actividad 4. DEFINICIÓN DE TERMINOS

INVENTARIO DE RECURSOS:

Hace referencia a la información de todos los activos que deben estar claramente identificados y de los cuales se debe elaborar y mantener una eficaz actualización.

ACTIVO:

Hace referencia a cualquier elemento que tiene valor para la organización.

ADMINISTRACIÓN DE INCIDENTES:

Pretende proveer al sistema información básica de un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

DIAGNOSTICO DE AMENAZAS- RIESGOS:

Proceso global de análisis y evaluación del riesgo.

ANÁLISIS:
Es el uso sistemático de la información para identificar las fuentes y estimar el riesgo al que se encuentra expuesto el activo.

CONTROLES:
Es definido como el medio para manejar el riesgo, incluidas las políticas, los procedimientos, las orientaciones, las prácticas o estructuras organizacionales usada como salvaguarda o medida preventiva.

RECURSOS:
Pretende establecer la comparación entre los costos de controles y planes de mitigación y las pérdidas de la organización por el daño de un activo determinado.

GENERAR INFORMES:
Ofrece al usuario la posibilidad de obtener documentación o información del análisis de activos específicos.

ACTAS APROBACIÓN COMITÉ DE SEGURIDAD:
Pretende ofrecer al usuario la posibilidad de acceder a documentos en los cuales queden plasmados movimientos de todo tipo en el sistema.

ENVIAR CORREO ACTIVIDADES PENDIENTES:
Pretende mantener informados a los diferentes usuarios del sistema de las actividades pendientes o los compromisos que están próximos a ser desarrollados.

RESPONSABLE ACTIVO:
Es la persona encargada del funcionamiento o manejo de activos en específico.

NIVEL DE CRITICIDAD:
Es definido como el impacto que se podría llegar a generar en la empresa, en caso de que algo le llegará a suceder a algún recuso dentro de la misma, se encuentra dividido en 3 niveles: *

- Muy Critico

Recurso que en caso de ser afectado por una amenaza, podría llegar a paralizar la empresa o a generar una pérdida económica

* Los valores en los niveles de criticidad y metodología que se utilizan en Emtelsa, se aplican de acuerdo a lineamientos entregados por Control Interno de las Empresas Públicas de Medellín y ellos a su vez se acogen a Estándares Internacionales.

significativa (de gran importancia o relevancia para la organización)
Valor= 3

- Critico

Recurso que en caso de ser afectado por una amenaza, podría llegar a tener impacto en una o varias áreas de la empresa, y no llegaría a generar pérdidas económicas importantes para la organización.
Valor= 2

- Normal

Recurso que en caso de ser afectado por una amenaza, tendría un impacto muy leve en áreas de la empresa o en la empresa en general y no generaría ningún tipo de pérdida económica.
Valor= 1

ESTADO ACTUAL
Este define la condición actual en la cual se encuentra el activo, existen 5 estados:

- Permanente: Activo que es manejado continuamente.
- Rotatorio: Activo usado ocasionalmente (alterna constantemente).
- En producción: Activo que es usado actualmente (En el presente, en el momento).
- Fuera de Producción: Activo que ha sido retirado y no esta en uso
- De Terceros: Activo que pertenece a otros

5.5.2 FASE 2. LEVANTAMIENTO DE INFORMACIÓN

ACTIVIDAD 1. ESTABLECIMIENTO Y GESTIÓN DEL SGSI

ALCANCE

El concepto de seguridad de la información abarca todas las tecnologías informáticas y de comunicaciones que posee la empresa, entendidas estas, como las tecnologías que soportan los diferentes servicios de la empresa a saber: Telefonía, Contact Center, Televisión, Datos e Internet, Gobierno en Línea.

EMTELSA S.A. E.S.P define que el alcance de la seguridad de la información está representado en dominios o capas que permiten gestionar los riesgos de los activos de información de la empresa que se soportan a través de las tecnologías informáticas y de telecomunicaciones. El grado de protección requerido para cada uno de ellos está directamente relacionado con el nivel en el que se encuentren dentro de los dominios o capas establecidos. [*]

POLÍTICA DE SGSI

"LA SEGURIDAD DE LA INFORMACIÓN ES PARTE INTEGRAL DE NUESTRO NEGOCIO"

La información es la base de negocio de Emtelsa y soporta todas las actividades a nivel operativo, táctico y estratégico de la organización. Los recursos tecnológicos con los cuales prestamos los servicios se encuentran adecuadamente protegidos frente a las diferentes amenazas naturales, tecnológicas y sociales.

La política de seguridad del Sistema de Gestión de la Seguridad de la Información está encaminada a que todos los recursos relacionados con el manejo de la información sean cuidados y aprovechados de la manera más eficiente, por todos los colaboradores, con niveles de seguridad acordes a los recursos financieros, a los requisitos legales y a las obligaciones de seguridad contractuales.

El Sistema de Gestión de la Seguridad de la Información busca dar un nivel de seguridad adecuado a los recursos de la

[*] El diagrama Niveles de Seguridad de Emtelsa, se encuentra en la página 31, seguido de la definición específica de las capas.

empresa de tal forma que no estemos totalmente expuestos y se garantice la continuidad de los servicios que se prestan a nuestros clientes.

ACTIVIDAD 2. EVALUACIÓN E IMPACTO DEL RIESGO

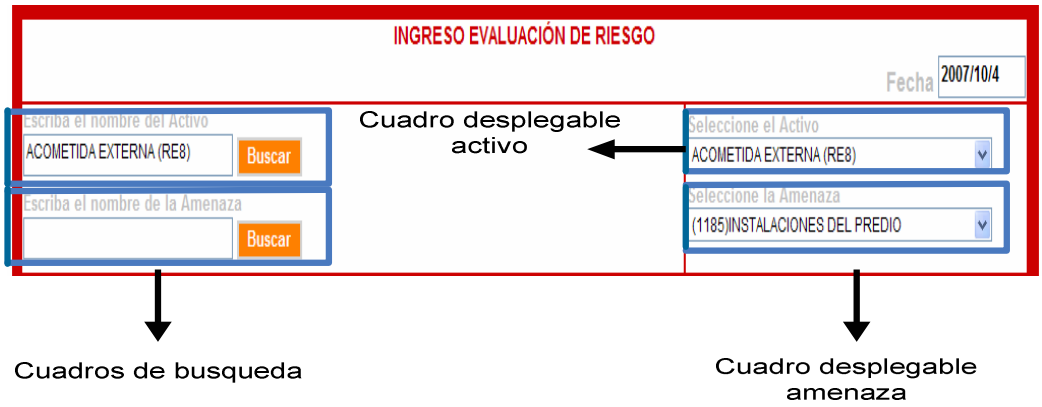
A continuación se explica detalladamente la forma de evaluación de riesgo empleada en EMTELSA S.A. E.S.P.
El formato general de evaluación de riesgo muestra todos los datos necesarios para la ejecución de una acertada evaluación y esta dispuesto de forma tal que facilite visualmente la comprensión del mismo, este formato hace parte del procedimiento PC 035 ADMINISTRACIÓN DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION, cuyo objetivo es Lograr que los sistemas tecnológicos de la empresa cumplan con los requerimientos de seguridad de la norma.

FIGURA 10. EVALUACIÓN E IMPACTO DEL RIESGO

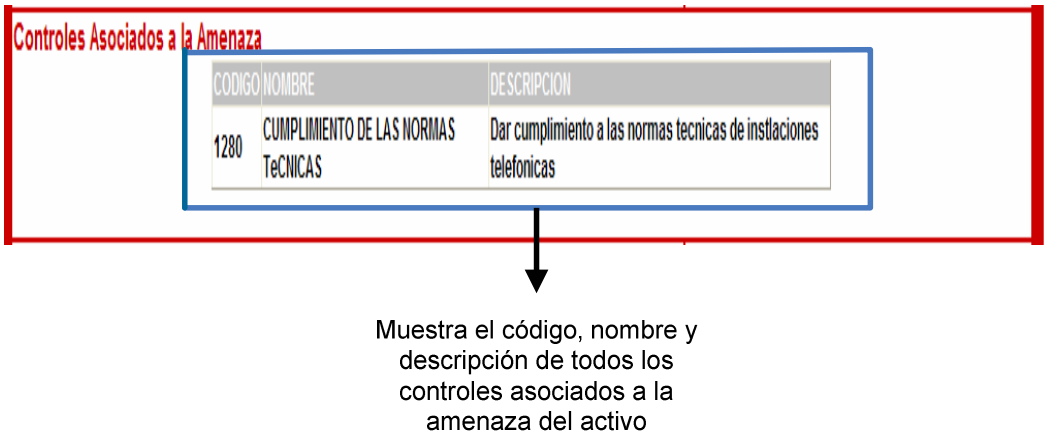
EXPLICACIÓN DETALLADA

El primer paso que se debe seguir para obtener la evaluación es buscar el activo a evaluar (que debe haber sido previamente ingresado en el sistema) o seleccionarlo directamente desde el cuadro desplegable de activo.

Al hacer esto automáticamente el sistema carga en el cuadro desplegable de amenazas, las amenazas que se encuentren asociadas a ese activo en particular (que deben haber sido ingresadas previamente en el sistema), también da la posibilidad al usuario de buscar la amenaza si así lo desea



Una vez seleccionada la amenaza, el sistema carga una lista de los controles (que deben haber sido ingresados previamente) existentes en el sistema para contrarrestar el riesgo del activo, mostrando de cada uno su código, nombre y descripción.



En este punto el usuario tiene las herramientas suficientes para catalogar el riesgo del activo, estos datos son seleccionados según el criterio del usuario capacitado y seleccionado para realizar la evaluación.

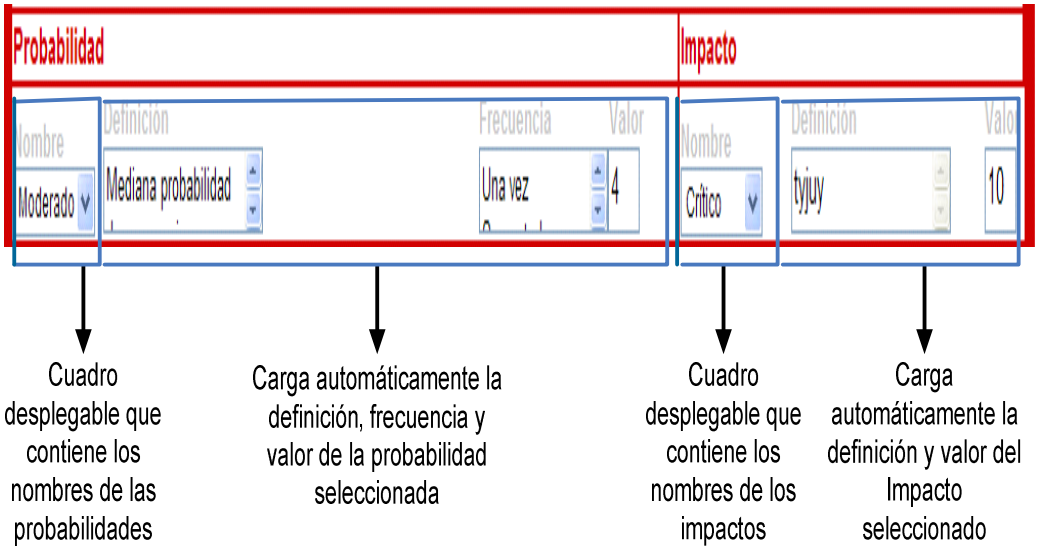
El primer paso es seleccionar la probabilidad, esta define la posibilidad de desarrollo de la amenaza que afecta al activo,

existen para este fin 5 posibles probabilidades:

NOMBRE	DEFINICIÓN	FRECUENCIA	VALOR
IMPROBABLE	Difícil que ocurra	5 años en adelante	1
REMOTO	Baja probabilidad de ocurrencia	Una vez entre 1 y 5 años	2
OCASIONAL	Limitada probabilidad de ocurrencia	Una vez anual	3
MODERADO	Mediana probabilidad de ocurrencia	Una vez semestral	4
FRECUENTE	Significativa probabilidad de ocurrencia	Una vez trimestral	5
CONSTANTE	Alta probabilidad de ocurrencia	Una o más veces al mes	6

Tabla 19. Probabilidades

El usuario selecciona la probabilidad que considera adecuada y el sistema carga automáticamente la definición, frecuencia y valor de dicha probabilidad.



Igualmente sucede con el Impacto, que define el efecto que produce en la empresa la ocurrencia de la amenaza en el activo, existen para este fin 6 posibles impactos:

NOMBRE	AFECTACIÓN DE OPERACONES	VALOR
INSIFNIFICANTE	Sin afectación en la prestación de servicios informáticos y/o de negocios	1
MARGINAL	Afectación de la prestación de servicios informáticos y/o de negocios no críticos	2
GRAVE	Afectación de la prestación de servicios informáticos y/o de negocios críticos hasta por 4 horas	5
CRÍTICO	Afectación de la prestación de servicios informáticos y/o de negocios críticos entre 4 y 24 horas	10
DESASTROSO	Afectación de la prestación de servicios informáticos y/o de negocios críticos entre 24 y 120 horas	20
CATASTRÓFICO	Afectación de la prestación de servicios informáticos y/o de negocios críticos por mas de 120 horas	50

Tabla 20. Impactos

El usuario selecciona el impacto que considera adecuado y el sistema carga automáticamente la definición y valor de dicho impacto.

En el momento que el usuario selecciona el impacto adecuado, el sistema carga 3 valores:

- Riesgo: Proximidad de daño o peligro del activo frente a la amenaza representado en un valor (en este caso 40), este valor se obtiene de la multiplicación directa del valor de la probabilidad escogida (en este caso 4) por el valor del impacto escogido (en este caso 10).

Riesgo= Probabilidad (4) * Impacto (10)
Riesgo= 40

- Vulnerabilidad: Posibilidad de sufrir daños representada en un valor porcentual (en este caso 13.33333), este valor porcentual se obtiene por medio de una regla de 3 simple de la siguiente manera:

La máxima vulnerabilidad (valor constante 300) es un valor que

se obtiene mediante la multiplicación del máximo valor de probabilidad (valor constante 6) y del máximo valor del impacto (valor constante 50).

MáximaVulnerabilidad= Máx. Probabilidad (6)*Máx. Impacto (50)
Máxima Vulnerabilidad= 300

Teniendo claro que este valor representa el 100% de la vulnerabilidad existente se aplica una regla de 3 simple entre el valor del riesgo y el valor de la máxima probabilidad para hallar el valor de la vulnerabilidad asi:

Si Máxima vulnerabilidad (300) ⟶ es el 100%
Riesgo (40) ⟶ es el 13.33333%
Vulnerabilidad en porcentaje

Vulnerabilidad Residual: Posibilidad real de sufrir daño de acuerdo a la aceptabilidad (nivel permitido de vulnerabilidad) que en Emtelsa tiene un valor de 3, para obtener el valor de la vulnerabilidad residual se hace una sustracción entre el valor porcentual de la vulnerabilidad (en este caso 13.33333) y el criterio de aceptabilidad establecido (valor constante 3).

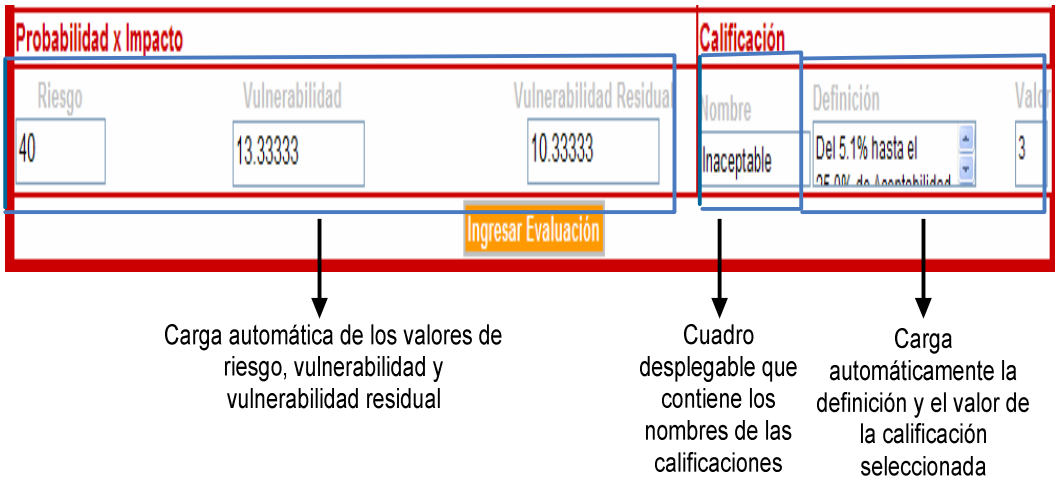
Vulnerabilidad Residual= Vuln. (13.33333%) - Aceptabilidad (3)
Vulnerabilidad Residual= 10.33333%

En el momento que el usuario obtiene el valor de la vulnerabilidad residual se encuentra en capacidad de dar una calificación al activo, existen para este fin 4 posibles calificaciones:

ZONA	**CRITERIO DE ACEPTABILIDAD**	**VALOR**
Aceptable	Hasta el 3.0% de vulnerabilidad residual	1
Tolerable	Del 3.1% hasta el 5.0% de vulnerabilidad residual	2
Inaceptable	Del 5.1% hasta el 25.0% de vulnerabilidad residual	3
Inadmisible	Más del 25.0% de vulnerabilidad residual	4

Tabla 21. Calificaciones

Teniendo como valor porcentual de vulnerabilidad residual 10.33333%, el usuario escoge entonces la calificación correspondiente a este valor (en este caso Inaceptable) para el activo evaluado y el sistema carga automáticamente la definición y el valor de dicha calificación.
Una vez culminado el proceso el usuario ingresa la evaluación en el sistema, en este caso en particular se debe volver a evaluar el activo y emplear los planes de mitigación correspondientes hasta que la calificación llegue a un nivel aceptable en la empresa, es decir, que no sobrepase el 5.0% de vulnerabilidad residual (calificación Aceptable o Tolerable).



5.2.3 FASE 3. ANÁLISIS

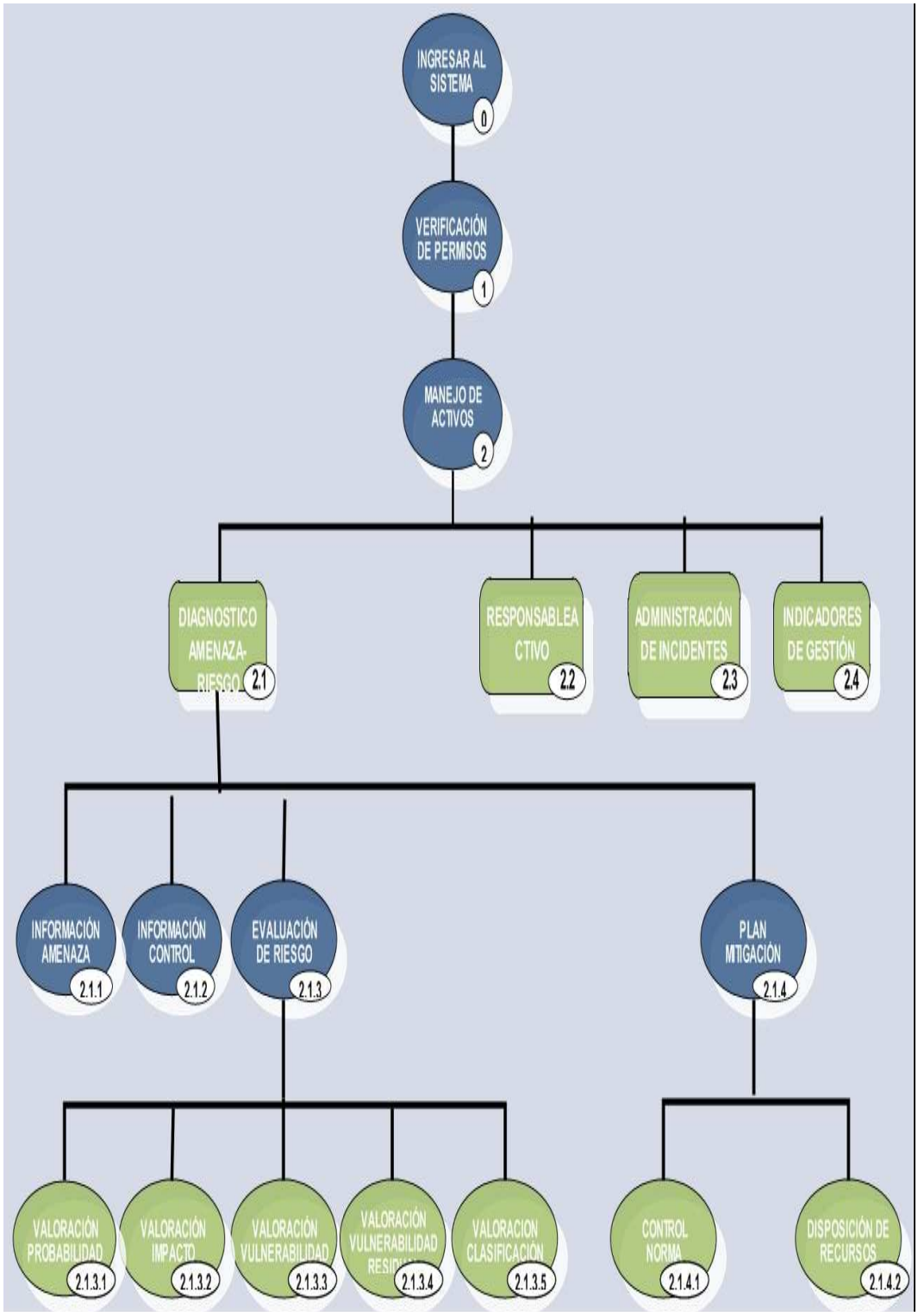
ACTIVIDAD 1. MODELO FUNCIONAL

Los diagramas que serán descritos a continuación como instrumento, pretenden dejar total claridad del enfoque del sistema y cumpliendo con este objetivo ser totalmente entendidos por el utilizador, tomando en cuenta todos los factores esenciales que serán de suma importancia para disponer de un propósito muy claro y preciso antes de comenzar a desarrollar el sistema.

- **ARBOL DE CASOS DE USO**

Este diagrama plantea un esquema estándar que divide y subdivide los casos de uso de acuerdo con su función dentro del sistema, ofrece una forma sencilla de entender el comportamiento del mismo.

FIGURA 11. ARBOL DE CASOS DE USO



- **DESCRIPCIÓN DE CASOS DE USO**

Para todos los casos de uso que van a ser descritos en este documento se estandarizaron procesos como: Consultar, Ingresar, Modificar, Eliminar. Estos procesos serán descritos a continuación.

CASO DE USO ESTANDAR CONSULTAR:

※ ***Descripción:*** Permite al usuario buscar datos dentro del sistema con el fin de obtener información sobre un activo específico.

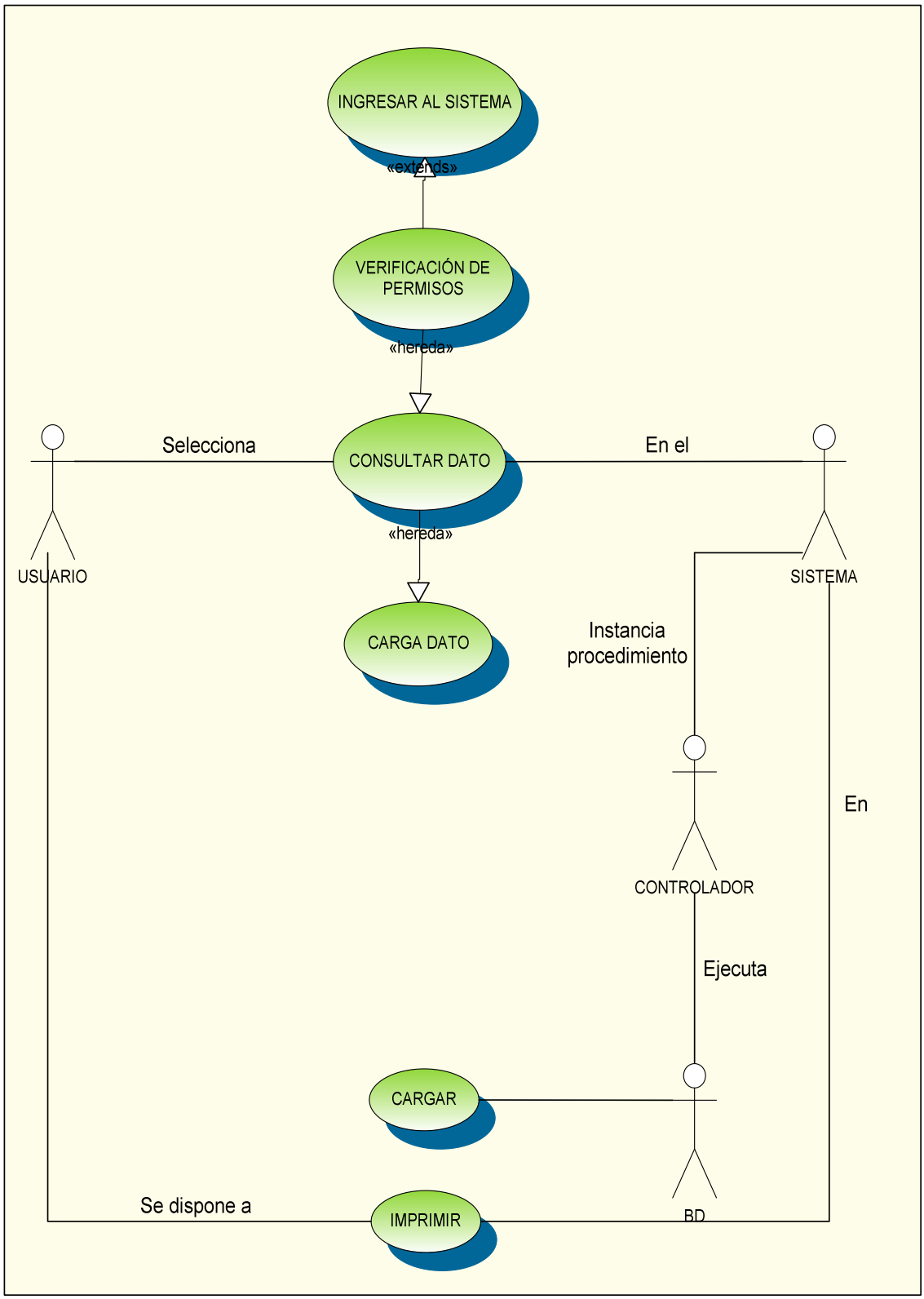
※ ***Actores:*** Usuario de tipo Administrador o usuario registrado.

※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem del cual pretende obtener información	**2.** Captura la selección **3.** Carga formato de consulta seleccionado con el fin de obtener la información necesaria **4.** Instancia procedimiento almacenado(Consultar)	**5.** Busca y ejecuta package	**6.** Inicia el proceso interno de consulta estándar **7.** OK
	8. Si es del caso carga el menú requerido		

Tabla 22. Caso de Uso Estándar Consultar

FIGURA 12. CASO DE USO ESTANDAR CONSULTAR



CASO DE USO ESTANDAR INGRESAR:

- ※ ***Descripción:*** Permite al usuario incluir o introducir información (controles, activos, amenazas, etc.) determinada en el sistema.

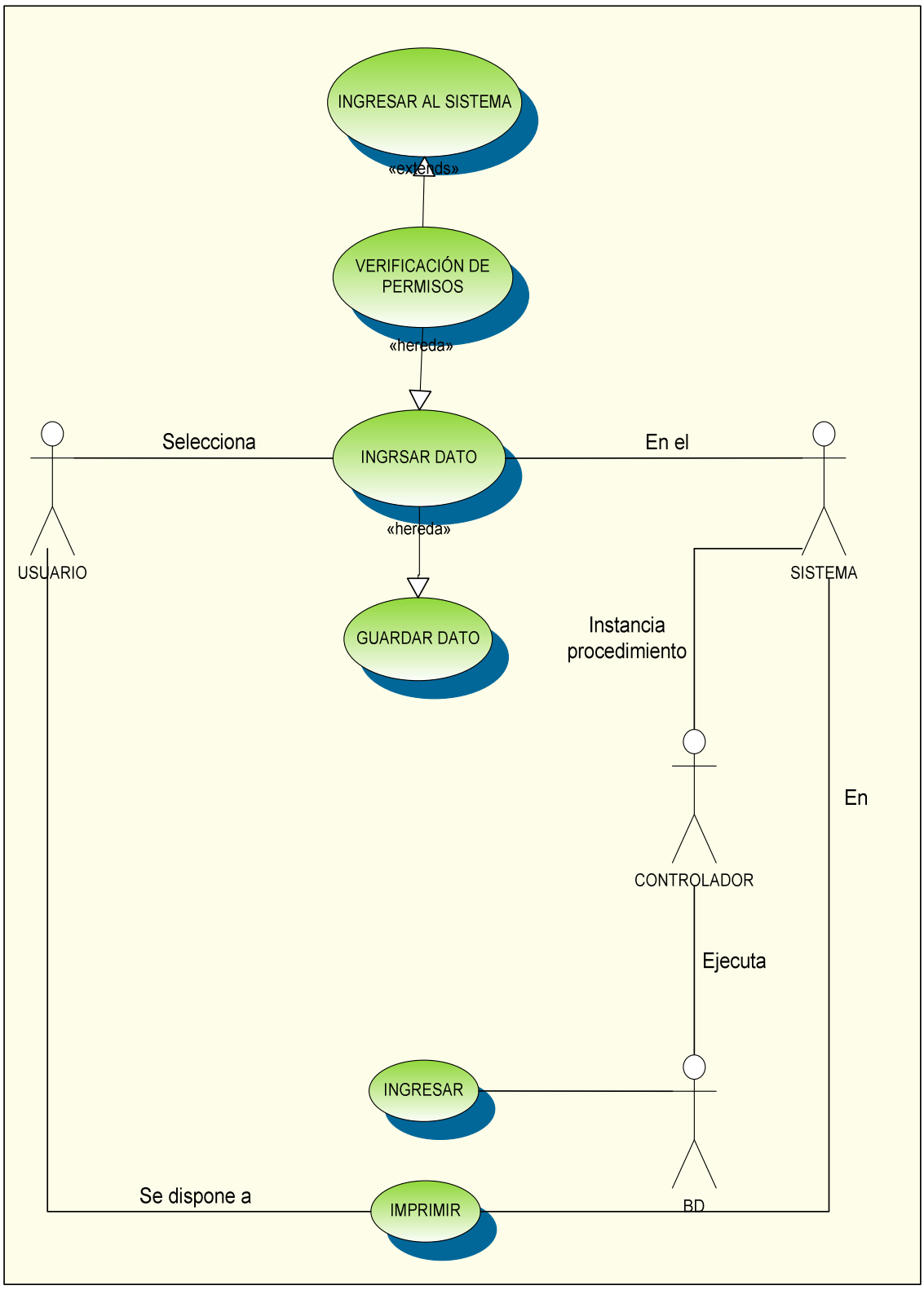
- ※ ***Actores:*** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona ítem ingresar			
	2. Valida selección **3.** Carga formato de ingreso seleccionado		
4. Ingresa información necesaria **5.** Confirma ingreso			
	6. Instancia procedimiento almacenado(Ingresar)		
		7. Busca y ejecuta package	
			8. Inicia el proceso interno de ingreso estándar **9.** OK
	10. Captura y valida datos **11.** Actualiza registro		

Tabla 23. Caso de Uso Estándar Ingresar

FIGURA 13. CASO DE USO ESTANDAR INGRESAR



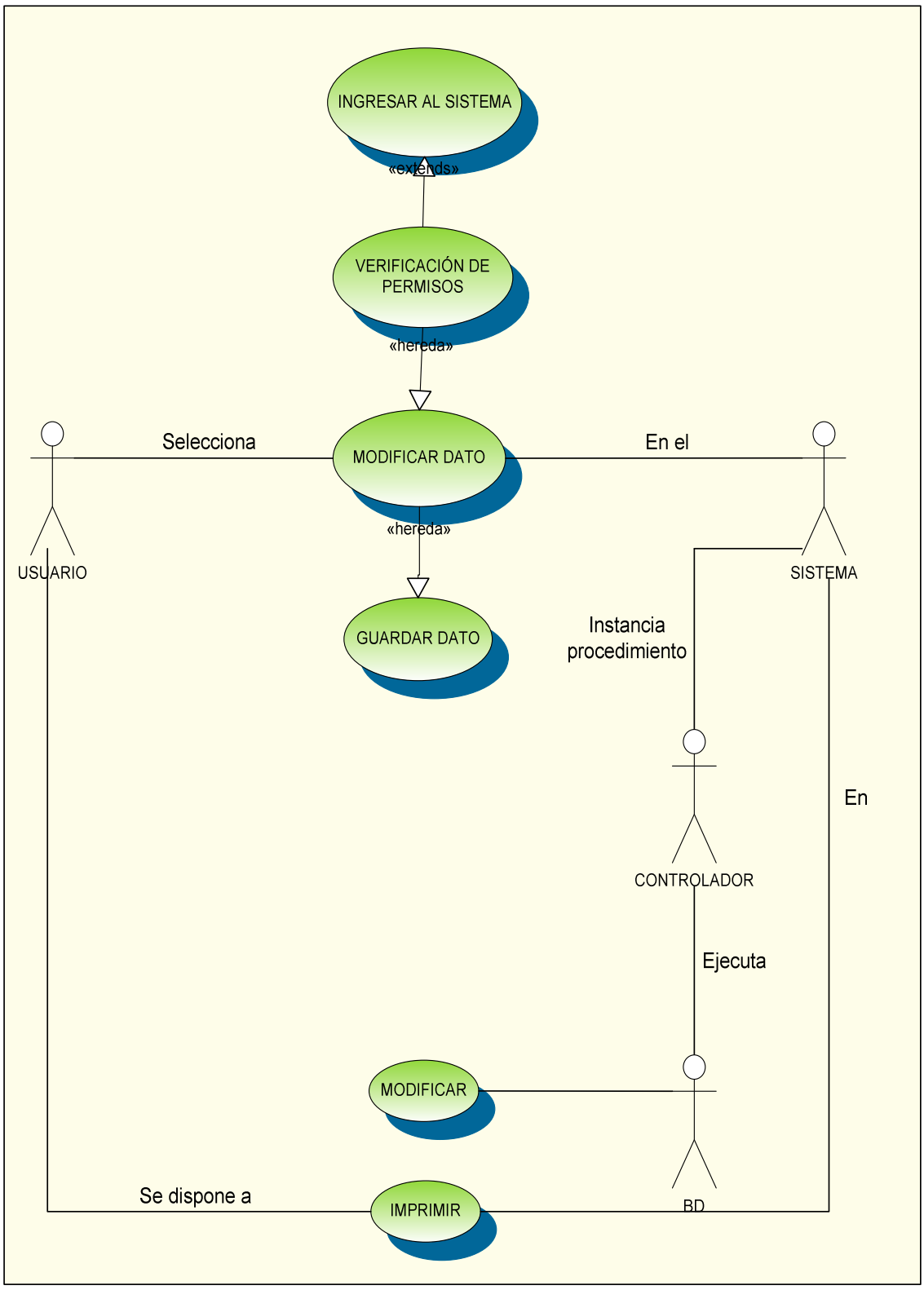
CASO DE USO ESTANDAR MODIFICAR:

- ※ ***Descripción:*** Permite al usuario cambiar o hacer variaciones respecto de un estado inicial de información.
- ※ ***Actores:*** Usuario de tipo Administrador o usuario registrado.
- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona ítem modificar			
	2. Valida selección **3.** Carga formato de modificación de información		
4. Realiza los cambios necesarios **5.** Confirma modificación			
	6. Instancia procedimiento almacenado(Modificar)		
		7. Busca y ejecuta package	
			8. Inicia el proceso interno de modificación estándar
	10. Captura y valida datos **11.** Actualiza registro		**9.** OK

Tabla 24. Caso de Uso Estándar Modificar

FIGURA 14. CASO DE USO ESTANDAR MODIFICAR



CASO DE USO ESTANDAR ELIMINAR:

- ※ ***Descripción:*** Le da la posibilidad al usuario de prescindir de información o excluirla del sistema si se considera necesario.

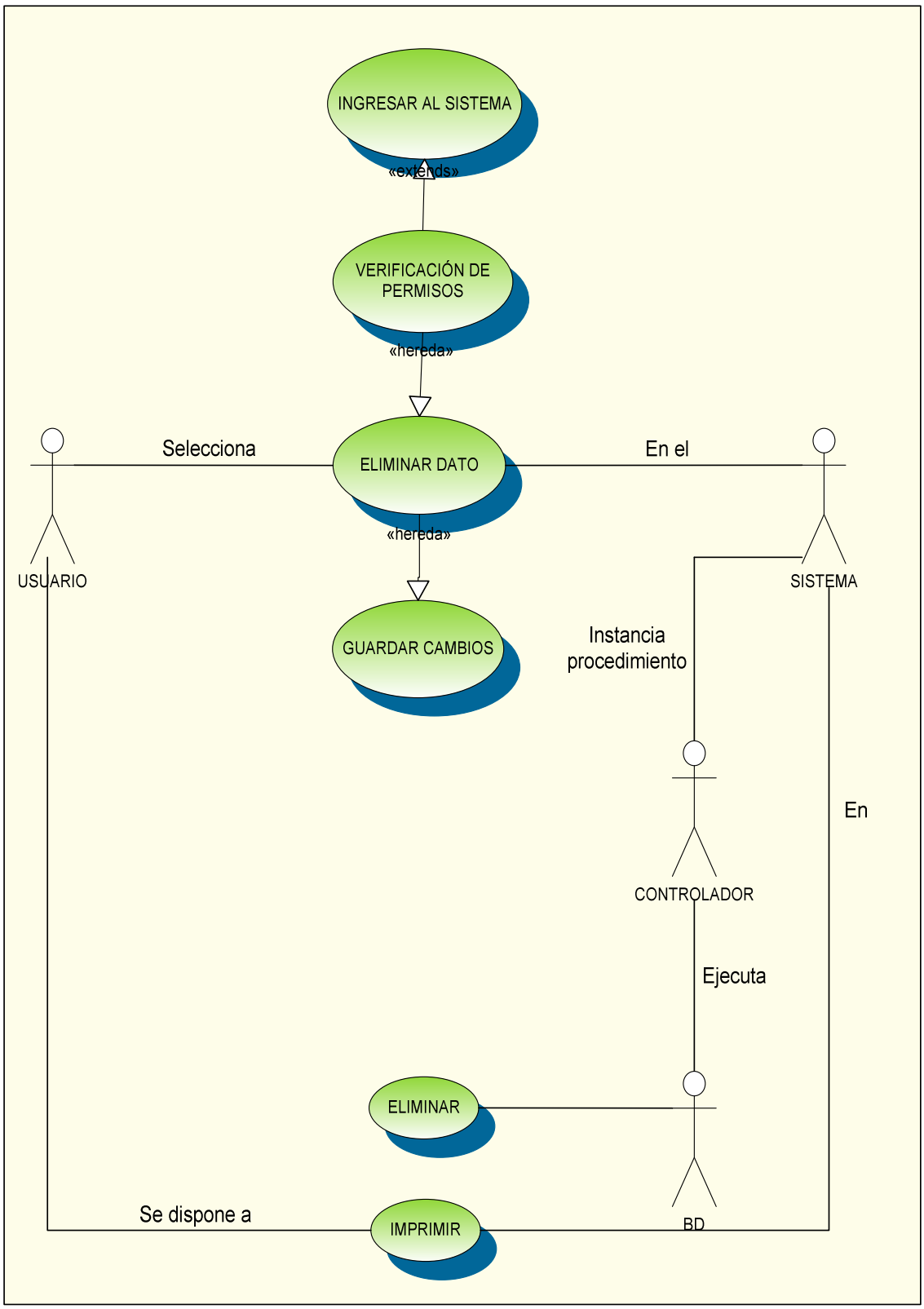
- ※ ***Actores:*** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem eliminar **3.** Selecciona información a eliminar **5.** Confirma eliminación	**2.** Captura la selección **4.** Solicita confirmación **6.** Instancia procedimiento almacenado(Eliminar) **10.** Captura y valida datos **11.** Actualiza registro	**7.** Busca y ejecuta package	**8.** Inicia el proceso interno de eliminación estándar **9.** OK

Tabla 25. Caso de Uso Estándar Eliminar

FIGURA 15. CASO DE USO ESTANDAR ELIMINAR



CASO DE USO 0:

- ※ ***Nombre*:** Ingresar al sistema

- ※ ***Descripción:*** Permite al usuario ingresar al sistema como administrador o como usuario registrado con el fin de consultar y/o hacer modificaciones de la información referente al activo.

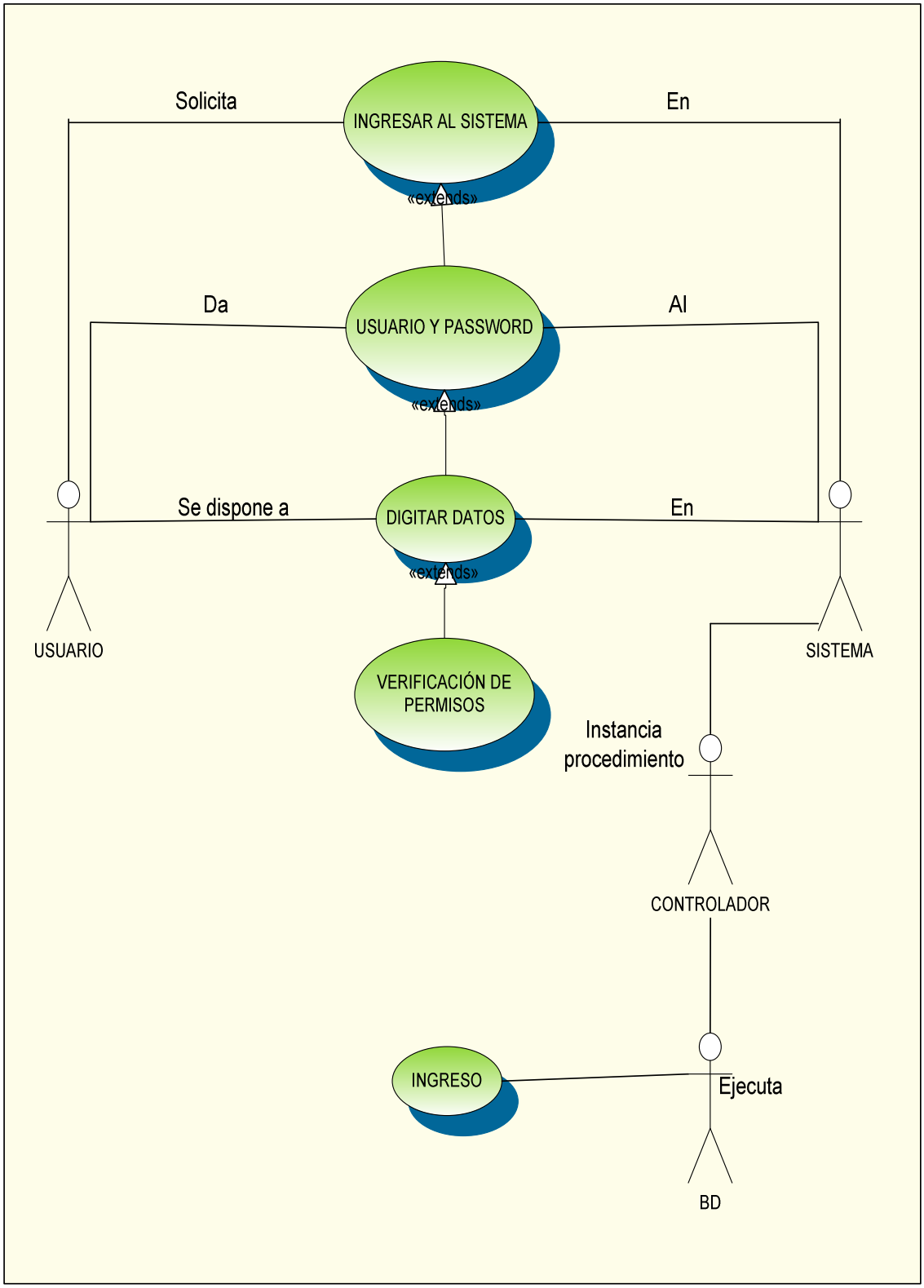
- ※ ***Actores:*** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	***SISTEMA***	***CONTROLADOR***	***BASE DE DATOS***
1. Solicita ingresar al sistema ***3.*** Digita su nombre y password obedeciendo a su identidad de administrador o usuario registrado	**2.** Solicita ingresar datos(usuario, password) **4.** Captura la información ***5.*** Instancia procedimiento almacenado(Ingresar) ***9.*** Permite ingreso al sistema	**6.** Busca y ejecuta package	***7.*** Inicia el proceso interno de verificación de permisos ***8.*** OK
CURSO ALTERNO DE EVENTOS Si el usuario no se encuentra registrado en el sistema o el password es inválido, este devuelve un mensaje de "usuario no registrado" y pide nuevamente los datos de identificación.			

Tabla 26. Caso de Uso 0, Ingresar al Sistema

FIGURA 16. CASO DE USO INGRESAR AL SISTEMA



CASO DE USO 1:

- ※ **Nombre:** Verificación de permisos.

- ※ **Descripción:** Permite al usuario ingresar al sistema con el fin de Validar las opciones de ingreso (consultar, ingresar, modificar, eliminar datos) dependiendo del tipo de usuario que ejecute la acción.

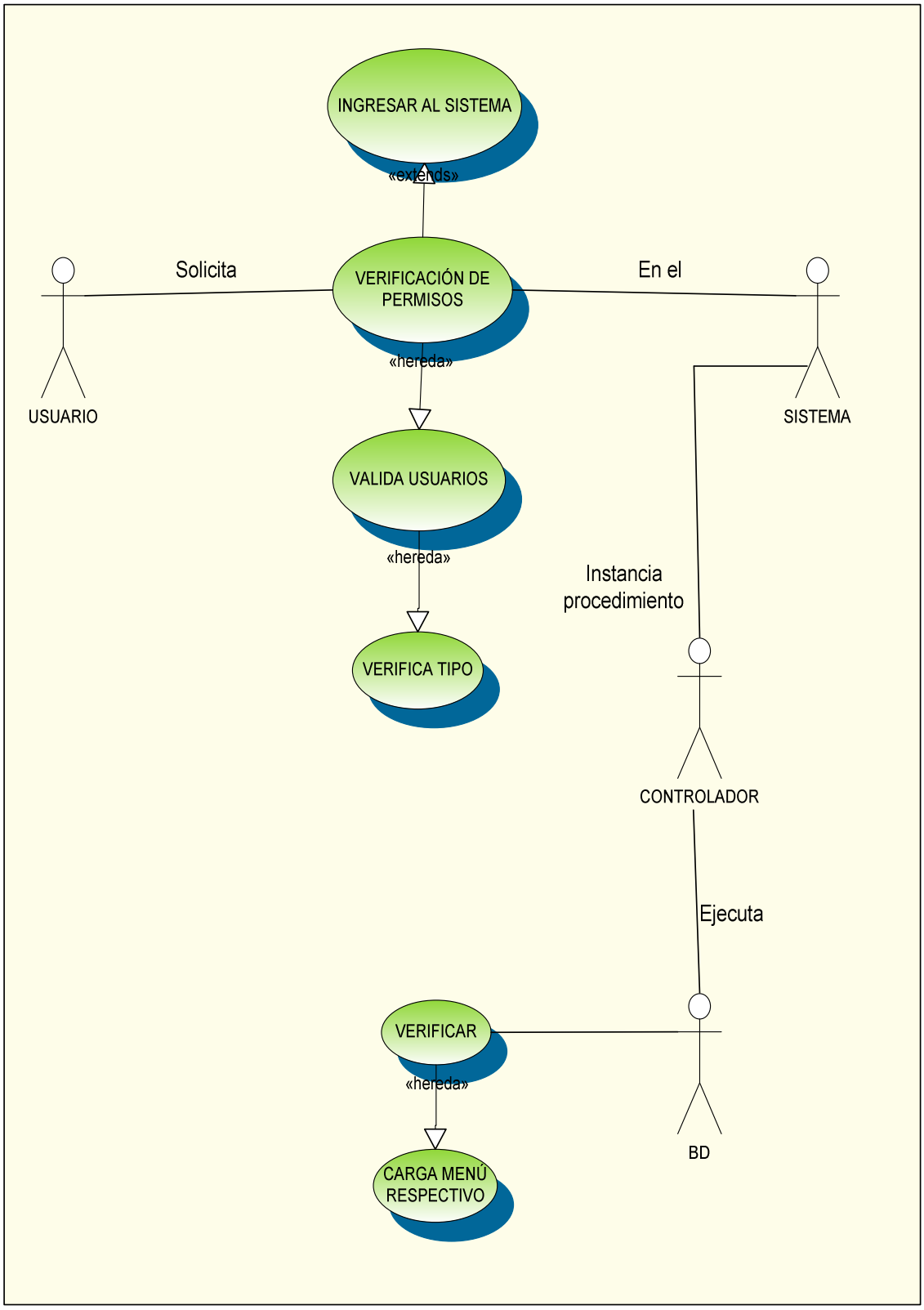
- ※ **Actores:** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	***SISTEMA***	***CONTROLADOR***	***BASE DE DATOS***
	1. Valida el usuario **2.** Si el usuario es valido verifica su tipo (administrador o usuario registrado) e identifica el rol dándole permisos para (consultar, ingresar, modificar y eliminar) ***3.*** Instancia procedimiento almacenado(Ingresar)		
		4. Busca y ejecuta package.	***5.*** Inicia el proceso interno de verificación de permisos
	7. Carga el respectivo menú relacionado directamente con los permisos que posea el usuario		***6.*** OK

Tabla 27. Caso de Uso 1, Verificación de Permisos

FIGURA 17. CASO DE USO VERIFICACIÓN DE PERMISOS



CASO DE USO 2:

- **Nombre:** Manejo de activos.

- **Descripción:** Permite al usuario ingresar al sistema con el fin de consultar, ingresar, modificar, eliminar datos y obtener información detallada sobre activos específicos.

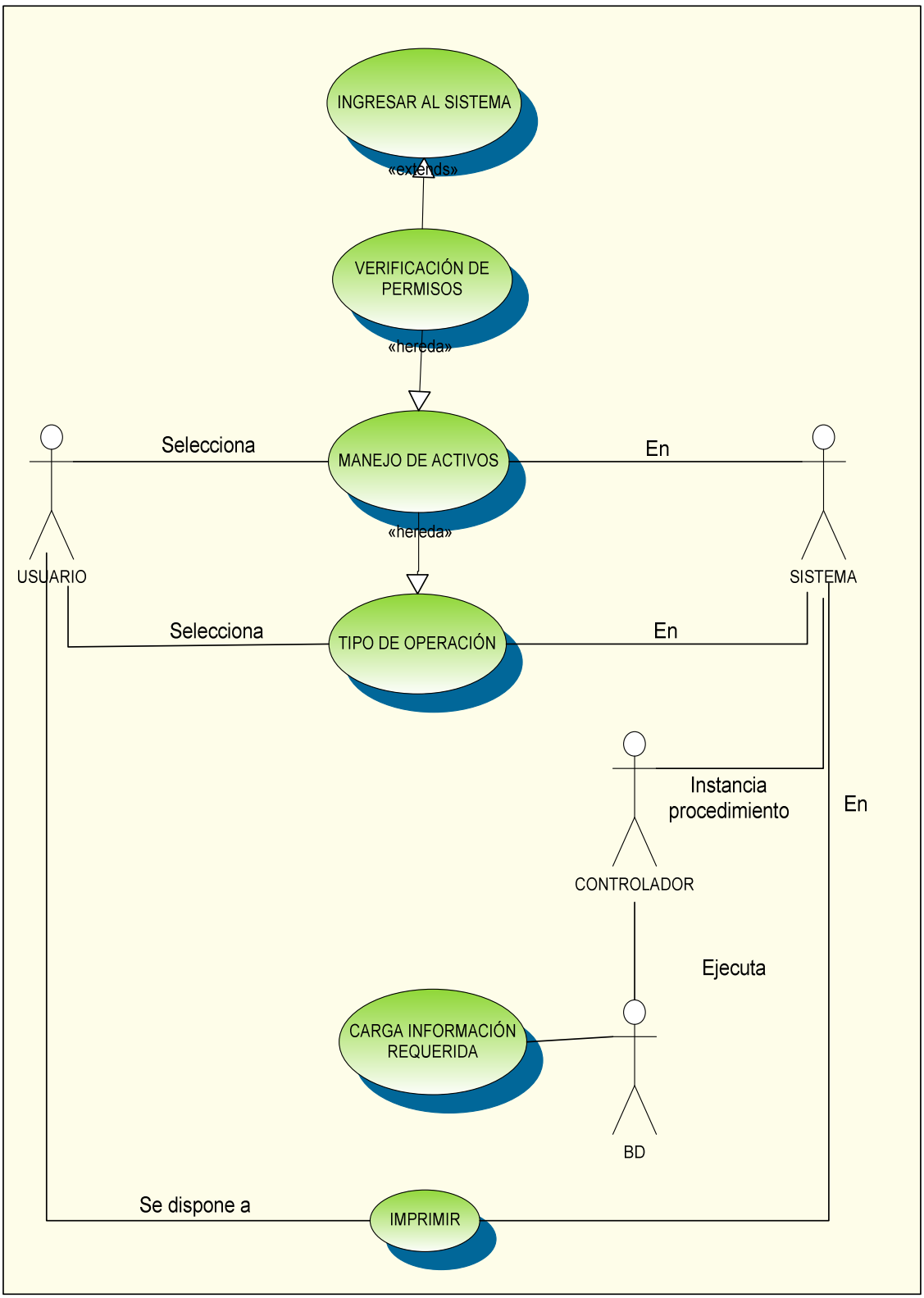
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	***SISTEMA***	***CONTROLADOR***	***BASE DE DATOS***
1. *Selecciona el ítem activo*	***2.*** Captura la selección **3.** Carga información de formato del activo ***4.*** *Solicita el tipo de operación a realizar*		
5. *Efectúa la selección*	**6.** Instancia procedimiento almacenado		
	10. Carga la información respectiva del activo dependiendo del tipo de operación seleccionada	**7.** Busca y ejecuta package.	***8.*** Inicia el proceso interno de manejo de activos ***9.*** OK

Tabla 28. Caso de Uso 2, Manejo de Activos

FIGURA 18. CASO DE USO MANEJO DE ACTIVOS



CASO DE USO 2.1:

- ※ **Nombre:** Diagnóstico amenaza-riesgo.

- ※ **Descripción:** Permite al usuario obtener información acerca del análisis del activo, esto con el fin de identificar fuentes y estimar el riesgo. Obedeciendo a los permisos de usuario permite consultar, ingresar, modificar y eliminar.

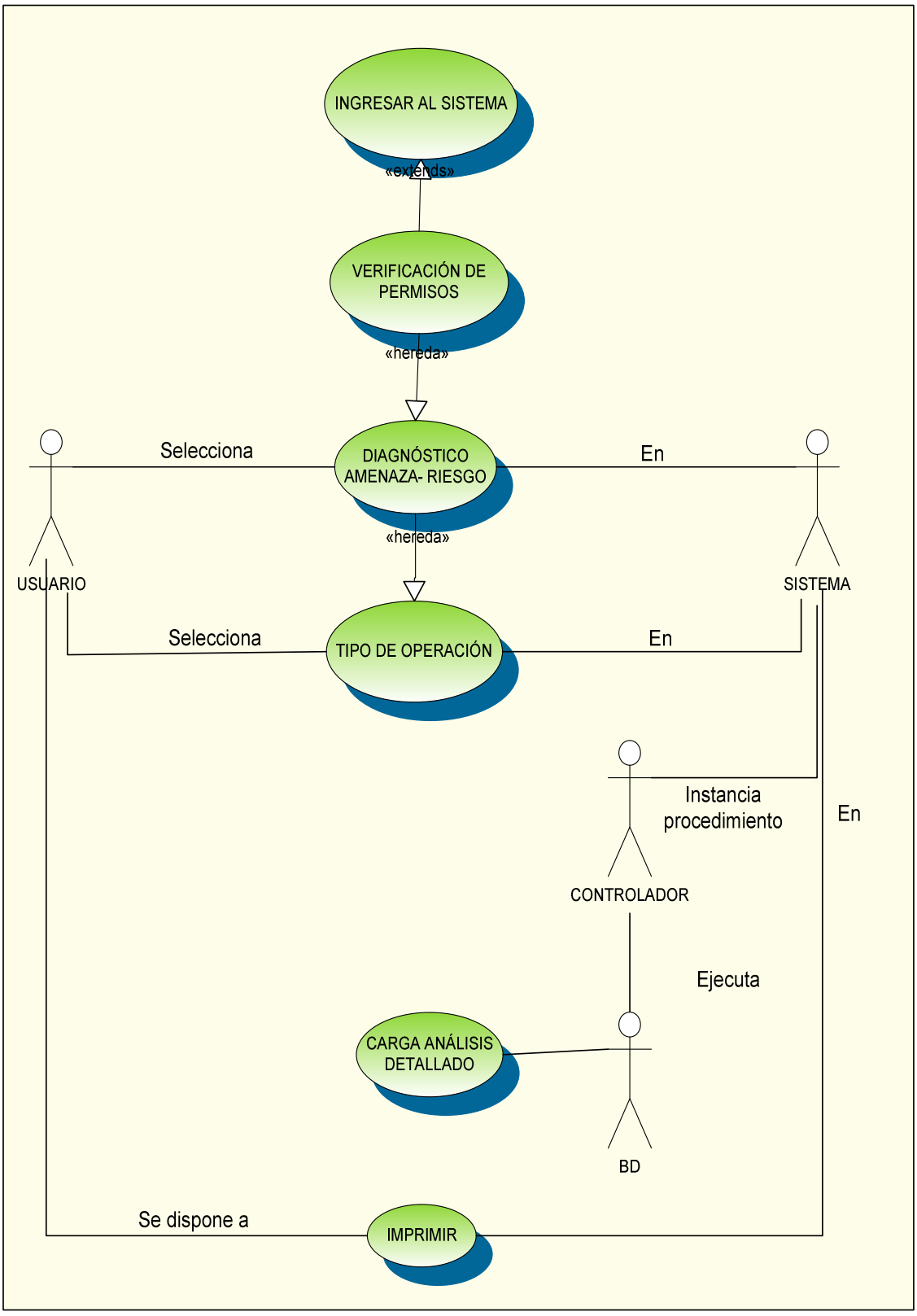
- ※ **Actores:** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	***SISTEMA***	***CONTROLADOR***	***BASE DE DATOS***
1. Selecciona el tipo de información	***2.*** Captura la selección **3.** Carga menú de activos según selección		
4. *Selecciona el activo de su interés*	***5.*** *Solicita el tipo de operación a realizar*		
6. *Efectúa la selección*	**7.** Instancia procedimiento almacenado		
		8. Busca y ejecuta package	***9.*** Inicia el proceso interno diagnóstico ***10.*** OK
	11. Carga el análisis detallado del activo seleccionado presentando los siguientes datos: código, amenaza, descripción, controles, fecha, probabilidad, impacto, plan de mitigación		

Tabla 29. Caso de Uso 2.1, Diagnóstico Amenaza-Riesgo

FIGURA 19. CASO DE USO DIAGNÓSTICO AMENAZA- RIESGO



CASO DE USO 2.1.1:

- **Nombre:** Información amenaza.

- **Descripción:** Muestra al usuario la información puntual de mal funcionamiento o actividades que puede atacar un activo y le permite a este modificar los datos de amenazas encontradas en activos o posibles amenazas que se puedan desarrollar.

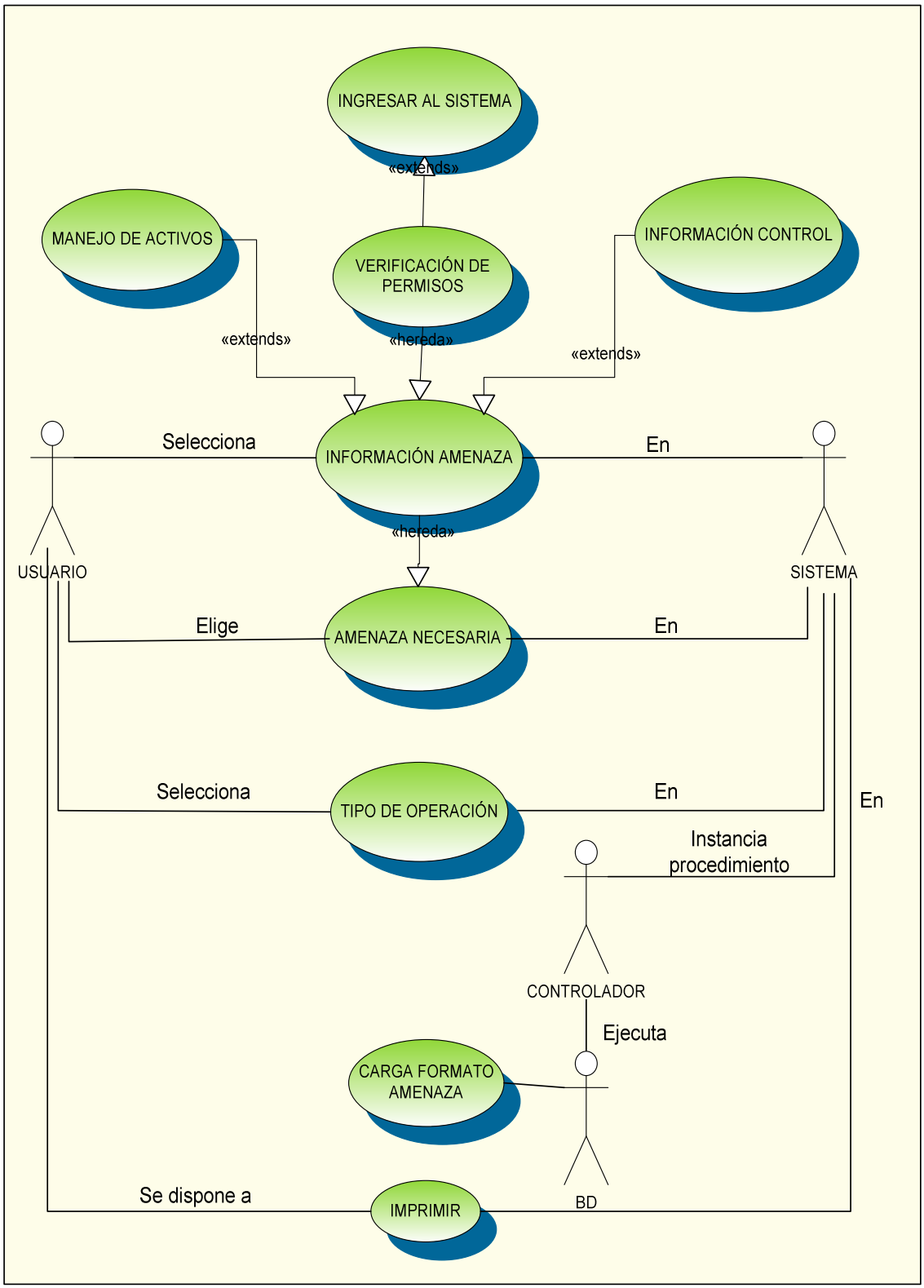
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	***SISTEMA***	***CONTROLADOR***	***BASE DE DATOS***
1. Selecciona el ítem amenaza	***2.*** Captura la selección **3.** Carga lista de amenazas encontradas		
4. *Elige la amenaza de la cual necesita información*	***5.*** *Solicita el tipo de operación a realizar*		
6. *Efectúa la selección*	**7.** Instancia procedimiento almacenado		
		8. Busca y ejecuta package	***9.*** Inicia el proceso interno información amenaza
	11. Carga formato de Información amenaza presentando los siguientes datos: código, nombre, descripción		***10.*** OK

Tabla 30. Caso de Uso 2.1.1, Información Amenaza

FIGURA 20. CASO DE USO INFORMACIÓN AMENAZA



CASO DE USO 2.1.2:

- **Nombre:** Información control.

- **Descripción:** Muestra al usuario la información de medidas que son o serán implementadas para modificar el riesgo a partir de la evaluación hecha y le permite a este modificar los datos de los controles efectuados o a efectuar.

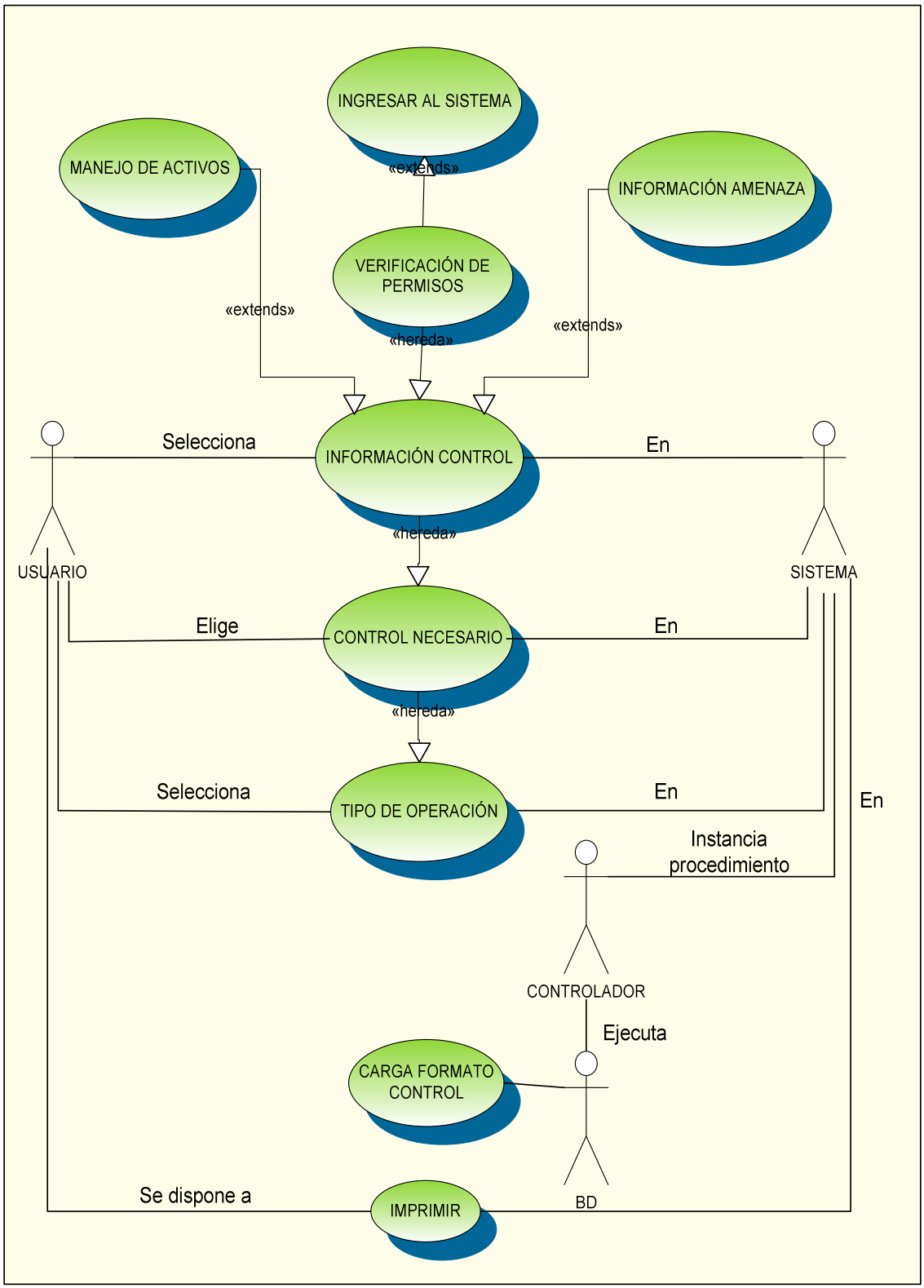
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem control			
	2. Captura la selección **3.** Carga lista de controles encontrados		
4. Elige el control del cual necesita información			
	5. Solicita el tipo de operación a realizar		
6. Efectúa la selección			
	7. Instancia procedimiento almacenado		
		8. Busca y ejecuta package	**9.** Inicia el proceso interno información control
			10. OK
	11. Carga formato de información control presentando los siguientes datos: código, nombre, descripción		

Tabla 31. Caso de Uso 2.1.2, Información Control

FIGURA 21. CASO DE USO INFORMACIÓN CONTROL



CASO DE USO 2.1.3:

- **Nombre:** Evaluación de riesgo.

- **Descripción:** Muestra al usuario el **nivel** del riesgo antes y después del tratamiento del mismo, exponiendo la información necesaria para valorar los activos y permitiendo modificar los datos cuando así se requiera.

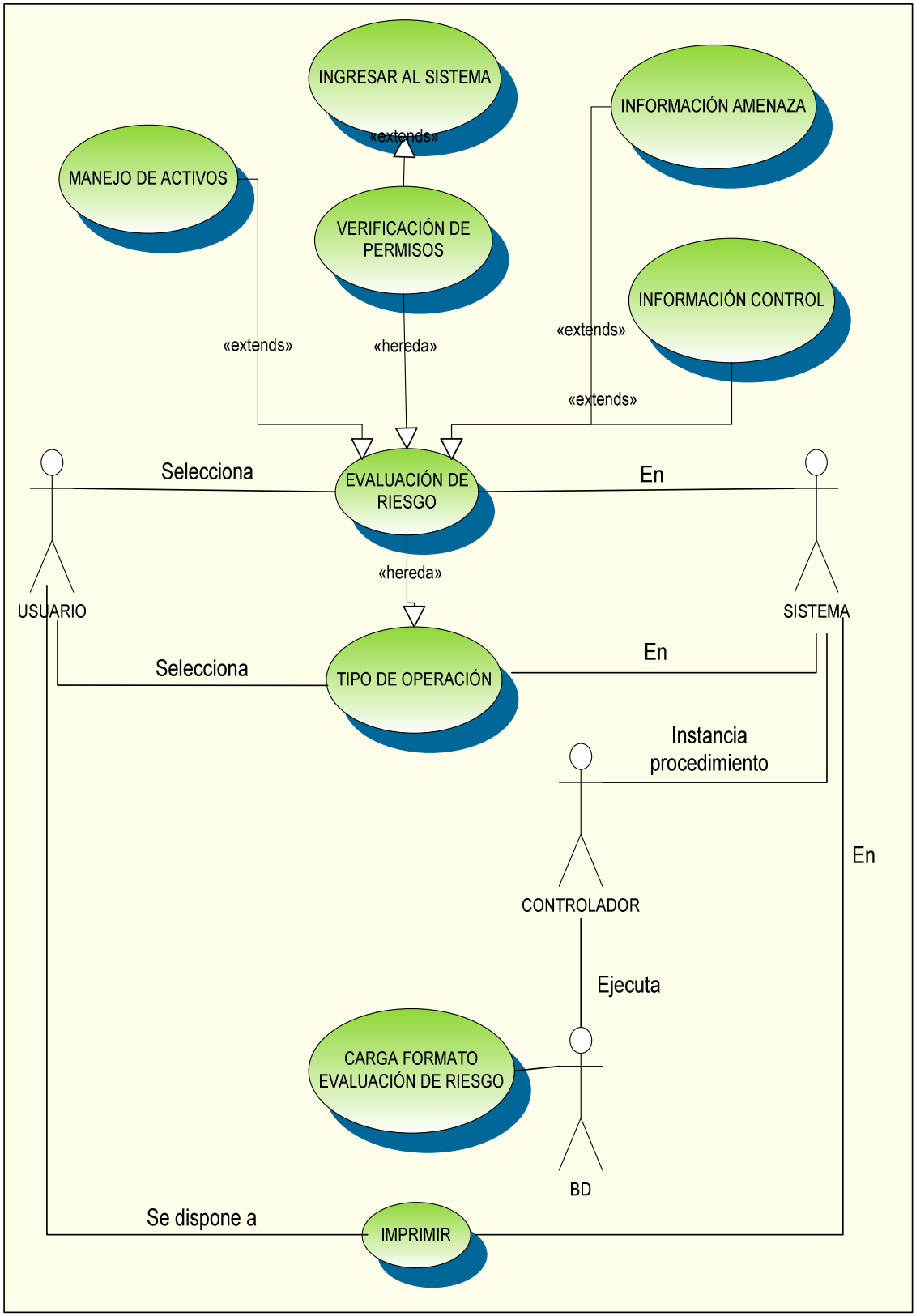
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem de Evaluación de riesgo	**2.** Captura la selección **3.** Solicita el tipo de operación a realizar		
4. Efectúa la selección	**5.** Instancia procedimiento almacenado	**6.** Busca y ejecuta package	**7.** Inicia el proceso interno evaluación de riesgo **8.** OK
	9. Carga el formato de evaluación de riesgo del activo presentando los siguientes datos: Fecha, probabilidad, impacto, riesgo, vulnerabilidad, vulnerabilidad residual, calificación		

Tabla 32. Caso de Uso 2.1.3, Evaluación de Riesgo

FIGURA 22. CASO DE USO EVALUACIÓN RIESGO



CASO DE USO 2.1.3.1:

- **Nombre:** Valoración Probabilidad.

- **Descripción:** Muestra la descripción de la probabilidad y el valor que le ha sido asignado a la amenaza según los parámetros establecidos, el usuario también puede hacer modificaciones a la probabilidad.

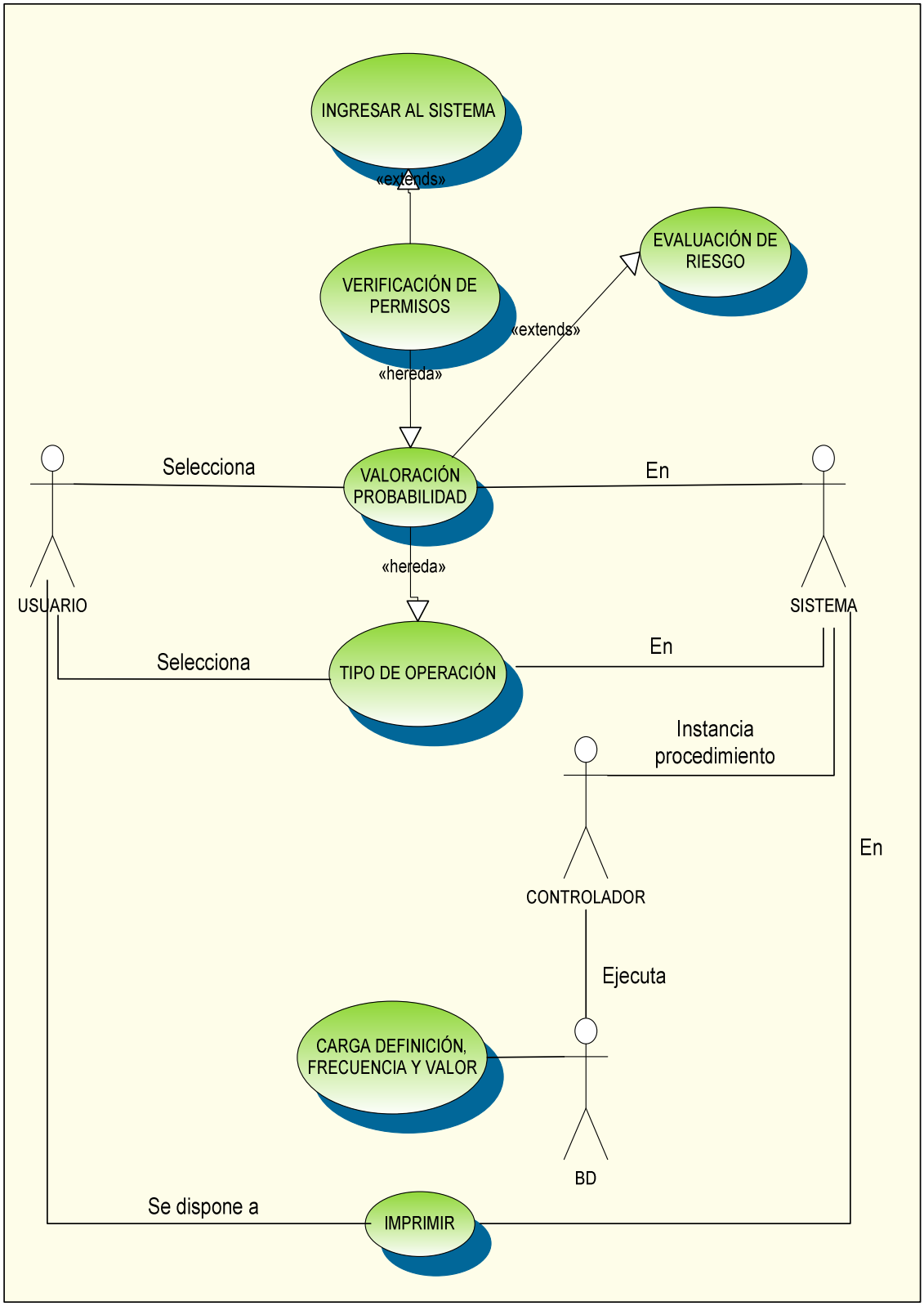
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona la probabilidad			
	2. Captura la selección **3.** Solicita el tipo de operación a realizar **4.** Instancia procedimiento almacenado		
		5. Busca y ejecuta package	
			6. Inicia el proceso interno valoración probabilidad **7.** OK
	8. Carga definición, frecuencia y valor de la probabilidad		

Tabla 33. Caso de Uso 2.1.3.1, Valoración Probabilidad

FIGURA 23. CASO DE USO VALORACIÓN PROBABILIDAD



CASO DE USO 2.1.3.2:

- ※ **Nombre:** Valoración Impacto.

- ※ **Descripción:** Muestra la descripción del impacto y el valor que le ha sido asignado según los parámetros establecidos, el usuario también puede hacer modificaciones al impacto.

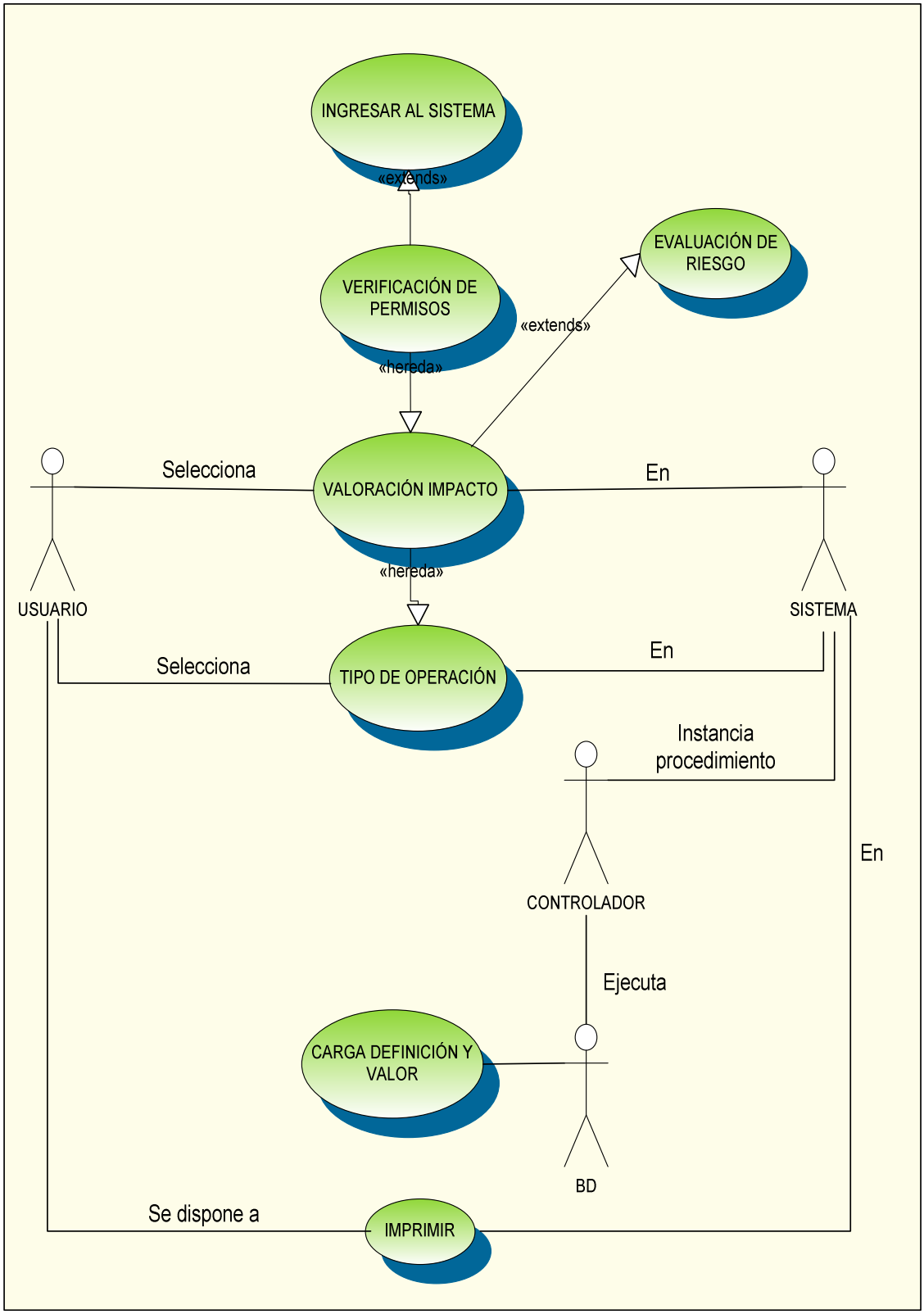
- ※ **Actores:** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el impacto	**2.** Captura la selección **3.** Solicita el tipo de operación a realizar **4.** Instancia procedimiento almacenado	**5.** Busca y ejecuta package	**6.** Inicia el proceso interno valoración impacto **7.** OK
	8. Carga definición y valor del impacto		

Tabla 34. Caso de Uso 2.1.3.2, Valoración Impacto

FIGURA 24. CASO DE USO VALORACIÓN IMPACTO



CASO DE USO 2.1.3.3:

- **Nombre:** Valoración Vulnerabilidad.

- **Descripción:** Las vulnerabilidades dejan a un sistema expuesto al ataque de una amenaza o permiten que un ataque tenga éxito o mayor impacto, con el fin de corregirlo se define una ecuación especifica y automática (al momento de seleccionar la probabilidad y el impacto) entre la máxima Probabilidad (valor 6) y el máximo Impacto (valor 50), la cual permite obtener el máximo Riesgo al cual se encuentran expuestos todos los activos y a partir de este encontrar el porcentaje exacto de vulnerabilidad del activo.

- **Actores:** Usuario de tipo Administrador o usuario registrado.

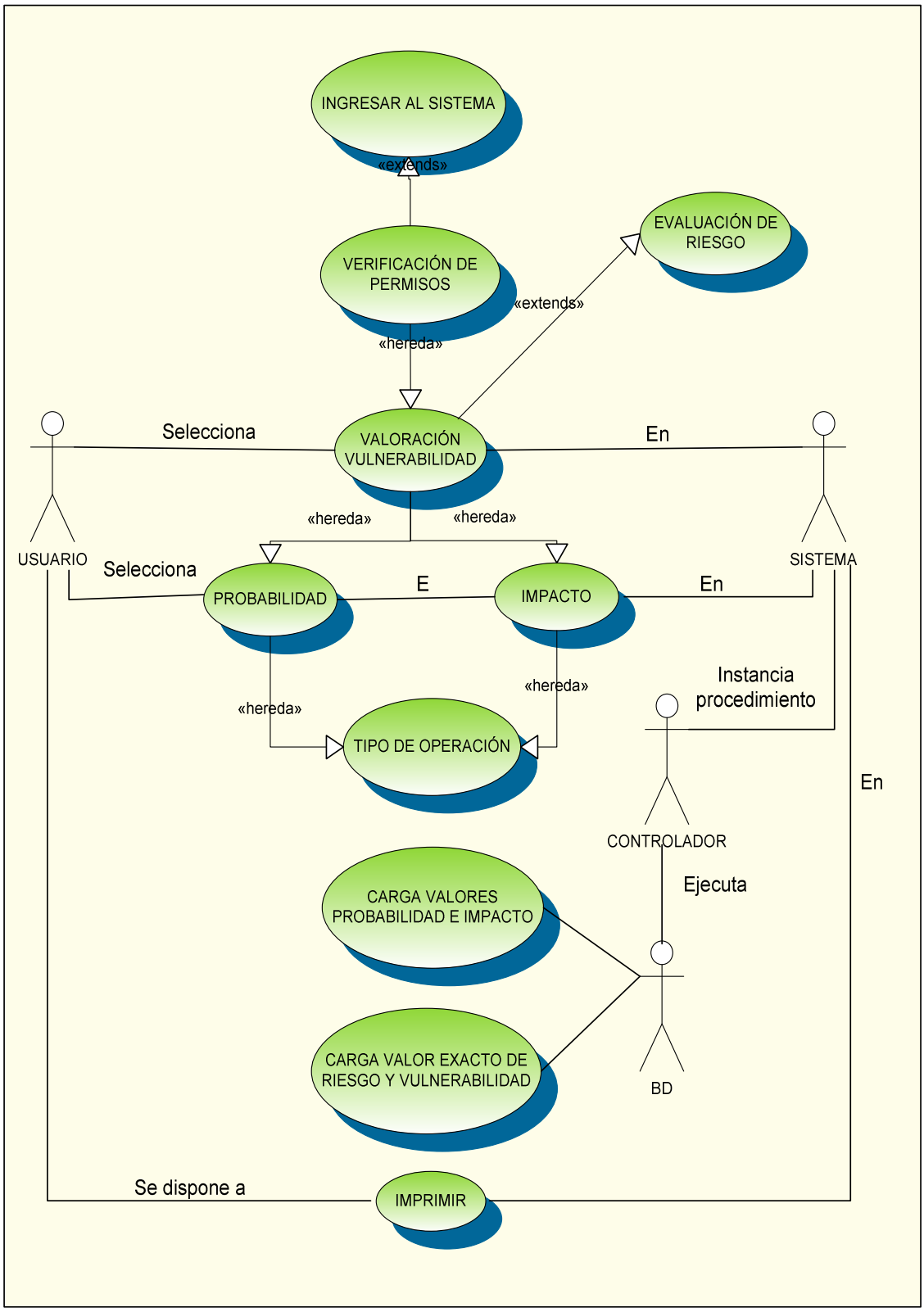
- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el nombre de la Probabilidad (Improbable, Remoto, Ocasional, Moderado, Frecuente, Constante)	**2.** Captura la selección **3.** Solicita el tipo de operación a realizar **4.** Instancia procedimiento almacenado	**5.** Busca y ejecuta package	**6.** Inicia el proceso interno valoración probabilidad **7.** OK

9. Selecciona el nombre del Impacto (Insignificante, Marginal, Grave, Crítico, Desastroso, Catastrófico)	**8.** Carga definición, frecuencia y valor de la probabilidad **10.** Captura la selección **11.** Solicita el tipo de operación a realizar **12.** Instancia procedimiento almacenado **16.** Carga definición y valor del impacto **17.** Carga automáticamente el valor exacto del riesgo y la vulnerabilidad	**13.** Busca y ejecuta package	**14.** Inicia el proceso interno valoración impacto **15.** OK

Tabla 35. Caso de Uso 2.1.3.3, Valoración Vulnerabilidad

FIGURA 25. CASO DE USO VALORACIÓN VULNERABILIDAD



CASO DE USO 2.1.3.4:

- ※ **Nombre:** Valoración Vulnerabilidad Residual.

- ※ **Descripción:** Define el criterio de aceptabilidad que permite un 3.0% de vulnerabilidad, el cual es restado de la vulnerabilidad final del activo y es este valor el que establece la calificación final del activo.

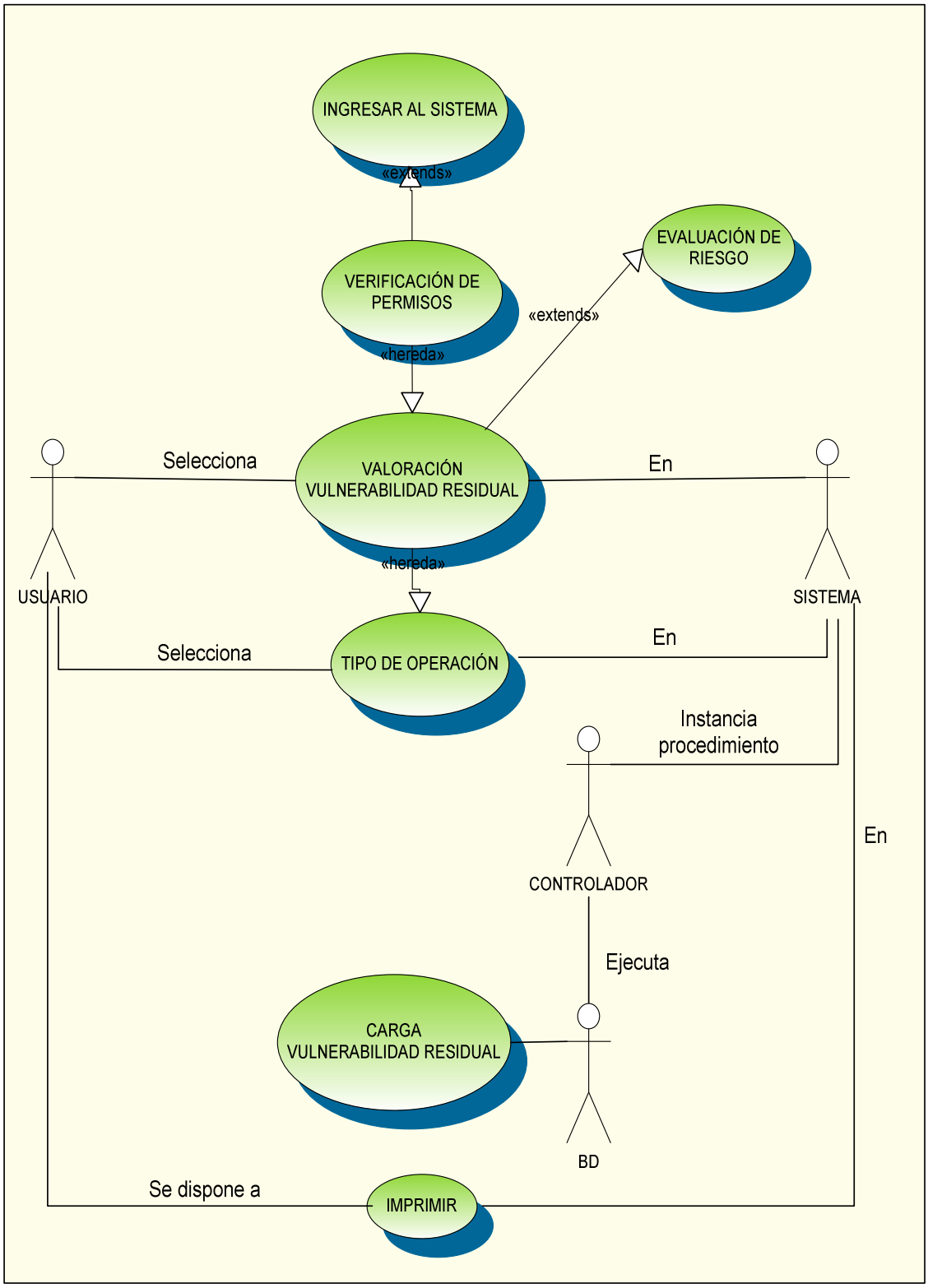
- ※ **Actores:** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
	1. Devuelve el valor de la vulnerabilidad **2.** Solicita el tipo de operación a realizar **3.** Instancia procedimiento almacenado	**4.** Busca y ejecuta package	**5.** Efectúa operaciones internas utilizando el valor obtenido **6.** OK
	7. Carga el valor de la vulnerabilidad residual final con la que quedara calificado el activo		

Tabla 36. Caso de Uso 2.1.3.4, Valoración Vulnerabilidad Residual

FIGURA 26. CASO DE USO VALORACIÓN VULNERABILIDAD RESIDUAL



CASO DE USO 2.1.3.5:

- ※ **Nombre:** Valoración Calificación.

- ※ **Descripción:** Define por medio de un valor específico el proceso global de análisis y evaluación del riesgo, permite establecer la aceptabilidad del riesgo en el activo. Las calificaciones pueden ser: Aceptable, Tolerable, Inaceptable, Inadmisible.

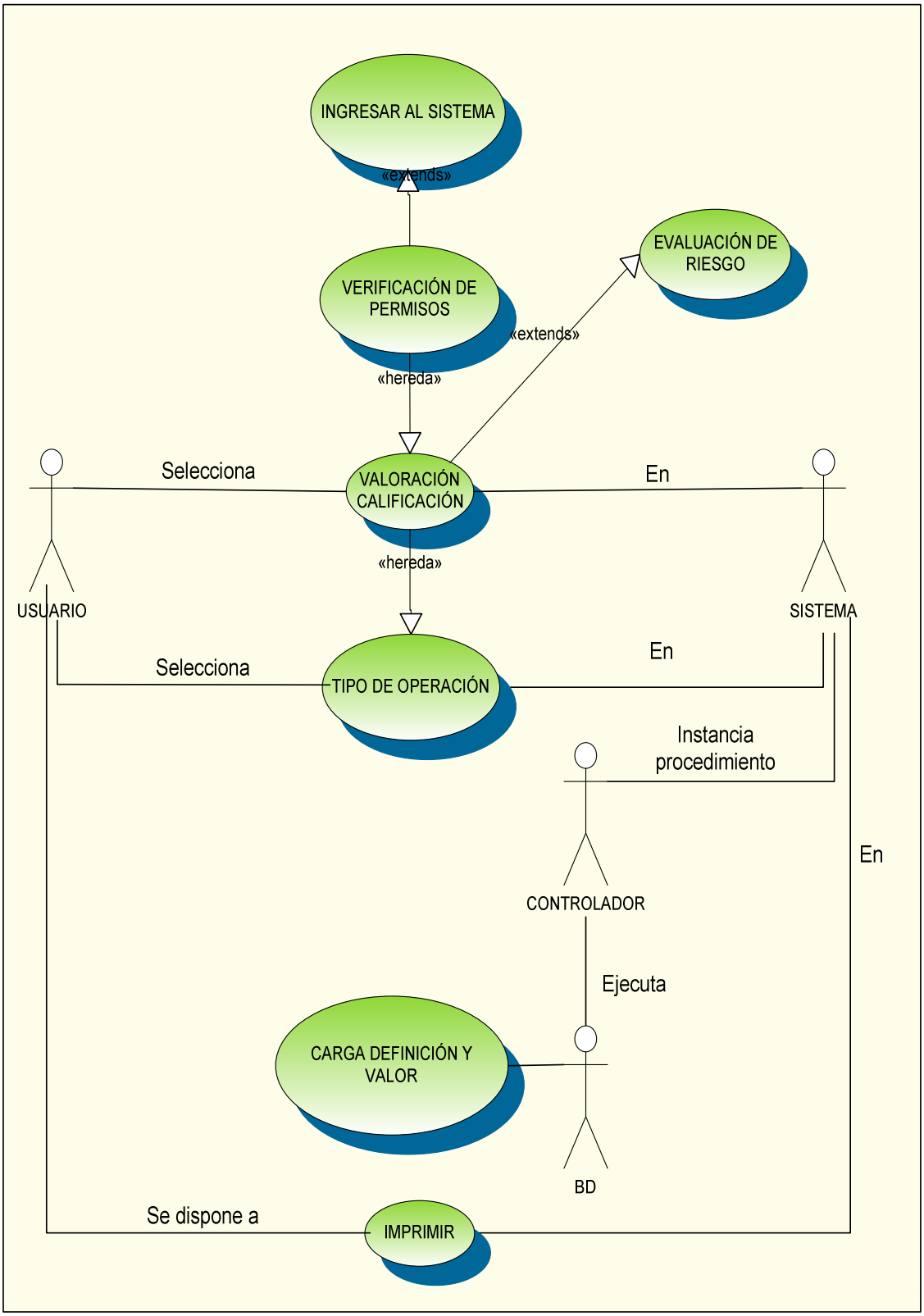
- ※ **Actores:** Usuario de tipo Administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el nombre de la calificación (Aceptable, Tolerable, Inaceptable, Inadmisible) dependiendo del valor de la vulnerabilidad residual			
	2. Captura la selección **3.** Solicita el tipo de operación a realizar		
4. Efectúa la selección			
	5. Instancia procedimiento almacenado		
		6. Busca y ejecuta package	
			7. Inicia el proceso interno valoración calificación
	9. Carga definición y valor de la calificación		**8.** OK

Tabla 37. Caso de Uso 2.1.3.5, Valoración Calificación

FIGURA 27. CASO DE USO VALORACIÓN CALIFICACIÓN



CASO DE USO 2.1.4:

- **Nombre:** Plan de Mitigación

- **Descripción:** Permite al usuario obtener información de un conjunto de controles que serán implementados frente un activo -sujeto a su evaluación- lo que llevara al sistema a una reevaluación del activo; el usuario final podrá efectuar modificaciones de los datos referentes al plan de mitigación.

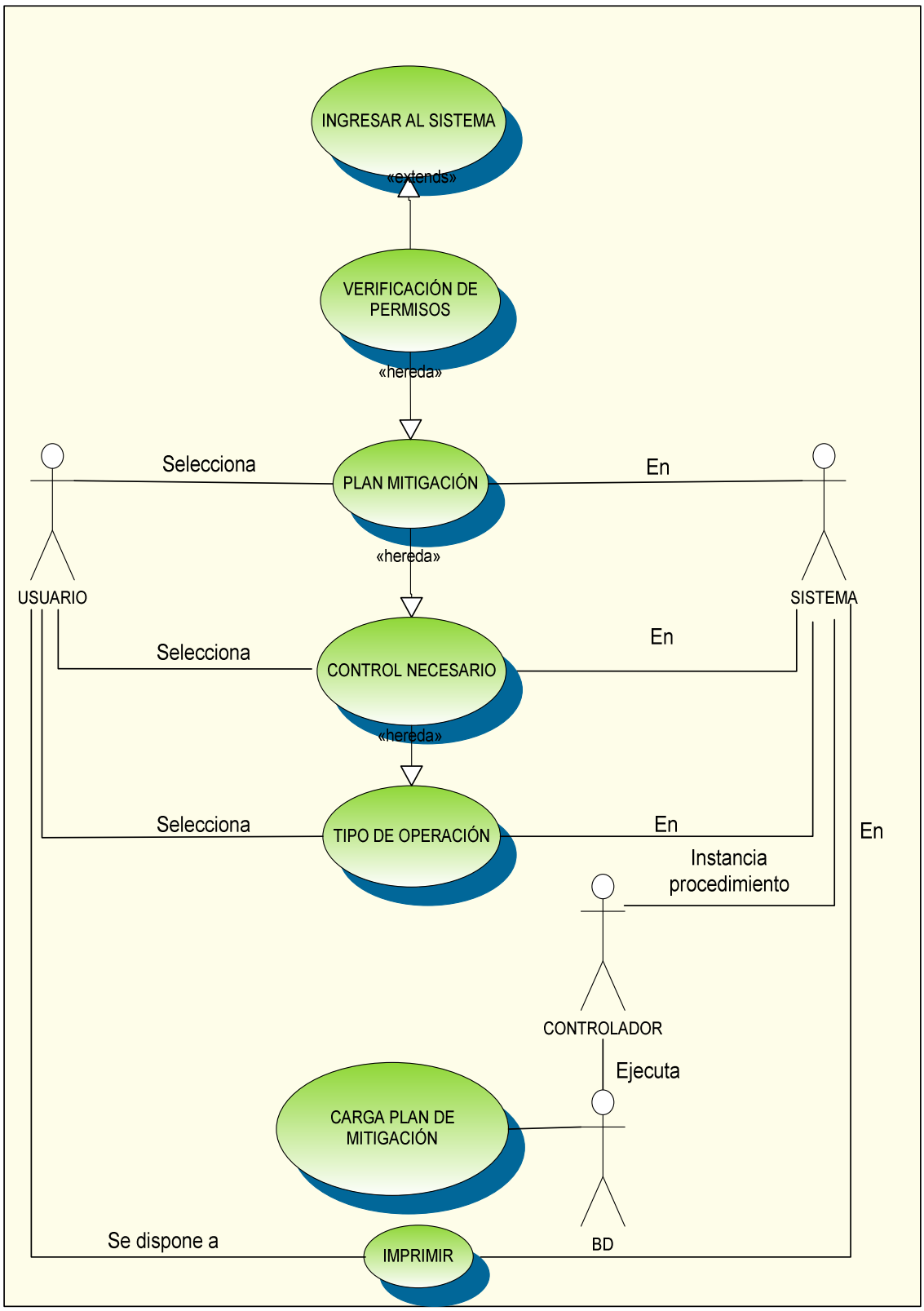
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem plan de mitigación			
	2. Captura la selección **3.** Carga lista de controles existentes		
4. Selecciona el control del cual necesita información			
	5. Solicita el tipo de operación a realizar		
6. Efectúa la selección			
	7. Instancia procedimiento almacenado		
		8. Busca y ejecuta package	
			9. Inicia el proceso interno plan de mitigación
			10. OK
	11. Carga la información respectiva acerca del plan de mitigación		

Tabla 38. Caso de Uso 2.1.4, Plan de Mitigación

FIGURA 28. CASO DE USO PLAN DE MITIGACIÓN



CASO DE USO 2.1.4.1:

- **Nombre:** Control norma

- **Descripción:** Permite al usuario hacer una confrontación entre los controles implementados en la empresa y los controles expuestos en la norma NTC-ISO/IEC 27001 y señalar la relación entre estos, también permite a este modificar la clasificación de los controles de la empresa.

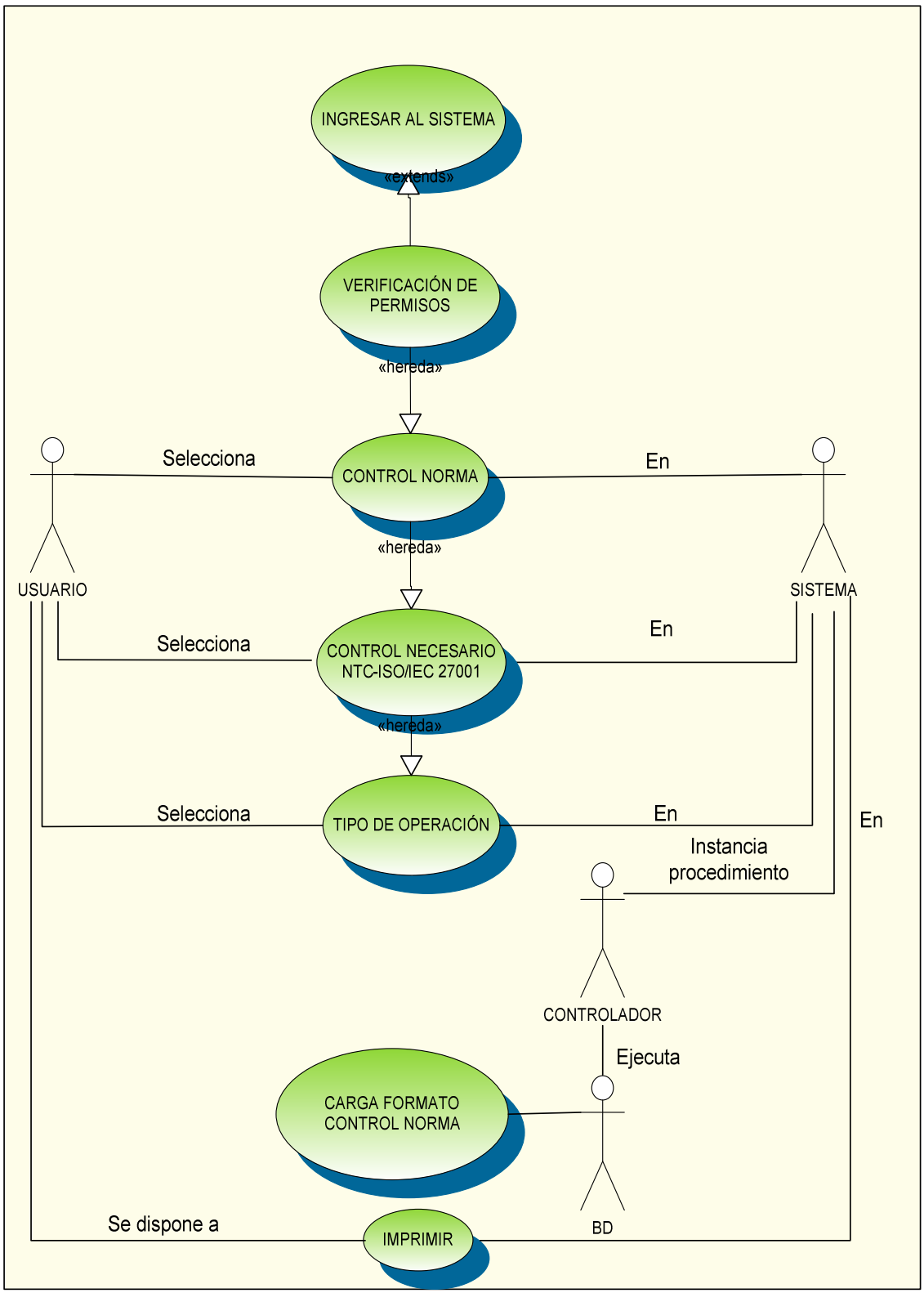
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem Control norma	**2.** Captura la selección **3.** Carga lista de controles que expone la norma NTC-ISO/IEC 27001		
4. Selecciona el control del cual necesita información	**5.** Solicita el tipo de operación a realizar		
6. Efectúa la selección	**7.** Instancia procedimiento almacenado	**8.** Busca y ejecuta package	**9.** Inicia el proceso interno control norma
	11. Carga formato de control norma presentando los siguientes datos: numeral control, nombre, descripción		**10.** OK

Tabla 39. Caso de Uso 2.1.4.1, Control Norma

FIGURA 29. CASO DE USO CONTROL NORMA



CASO DE USO 2.1.4.2:

- ※ **Nombre:** Disposición de Recursos.

- ※ **Descripción:** Permite al usuario obtener información detallada de los recursos que se deben obtener en la empresa obedeciendo a los controles que se deban implementar y a su vez modificar los datos de estos.

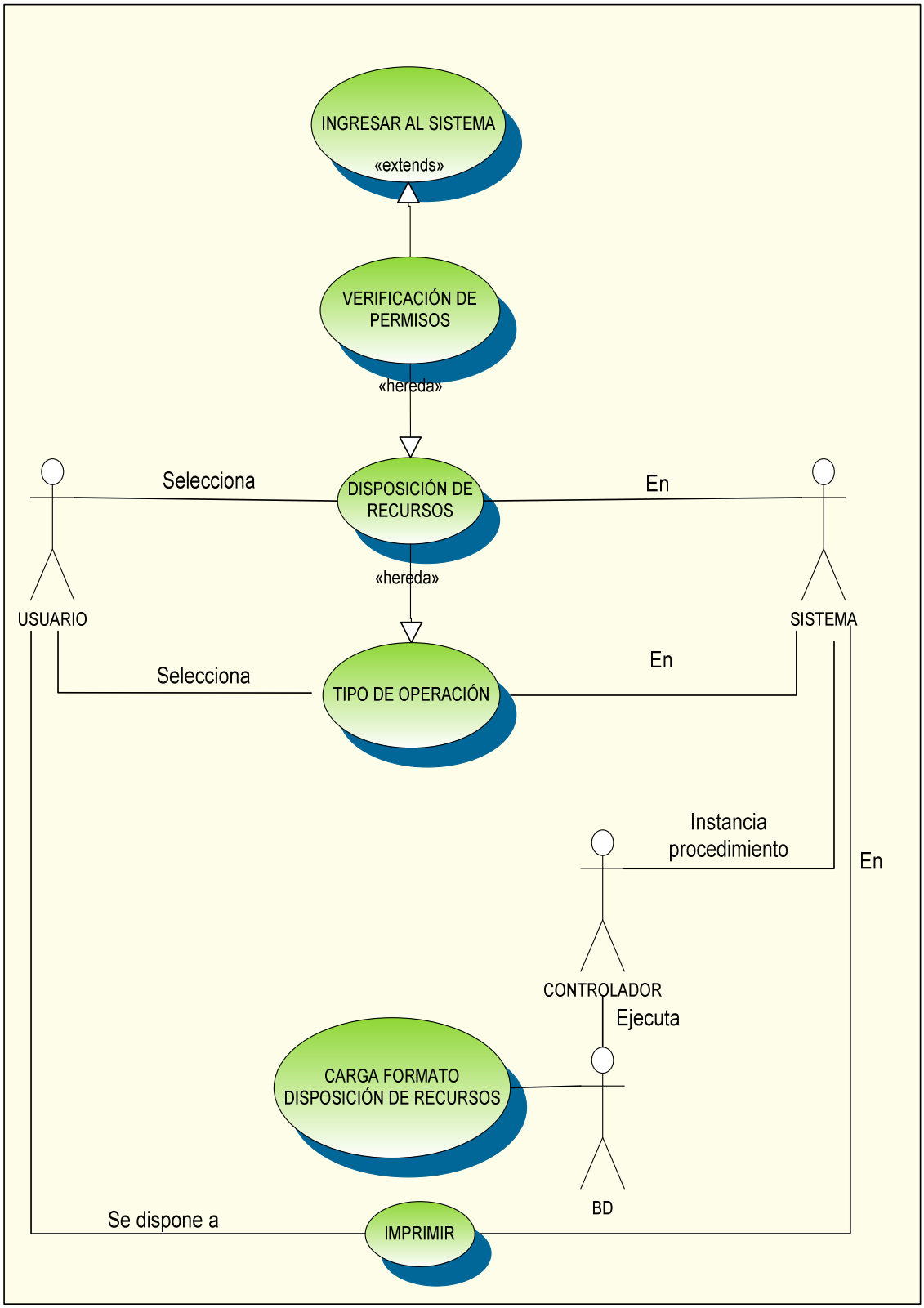
- ※ **Actores:** Usuario de tipo administrador o usuario registrado.

- ※ ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem disposición de recursos	**2.** Captura la selección **3.** Solicita el tipo de operación a realizar		
4. Efectúa la selección	**5.** Instancia procedimiento almacenado		
	9. Carga formato de Disposición de recursos presentando los siguientes datos: Nombre, fecha probable implementación, fecha real implementación, descripción, valor inversión, estado de implementación	**6.** Busca y ejecuta package	**7.** Inicia el proceso interno disposición de recursos **8.** OK

Tabla 40. Caso de Uso 2.1.4.2, Disposición de Recursos

FIGURA 30. CASO DE USO DISPOSICIÓN DE RECURSOS



CASO DE USO 2.2:

- **Nombre:** Responsable activo

- **Descripción:** Permite al usuario obtener información personal del responsable, que activos tiene bajo su manejo y le da la posibilidad de ingresar, modificar o eliminar los datos de los responsables de un activo.

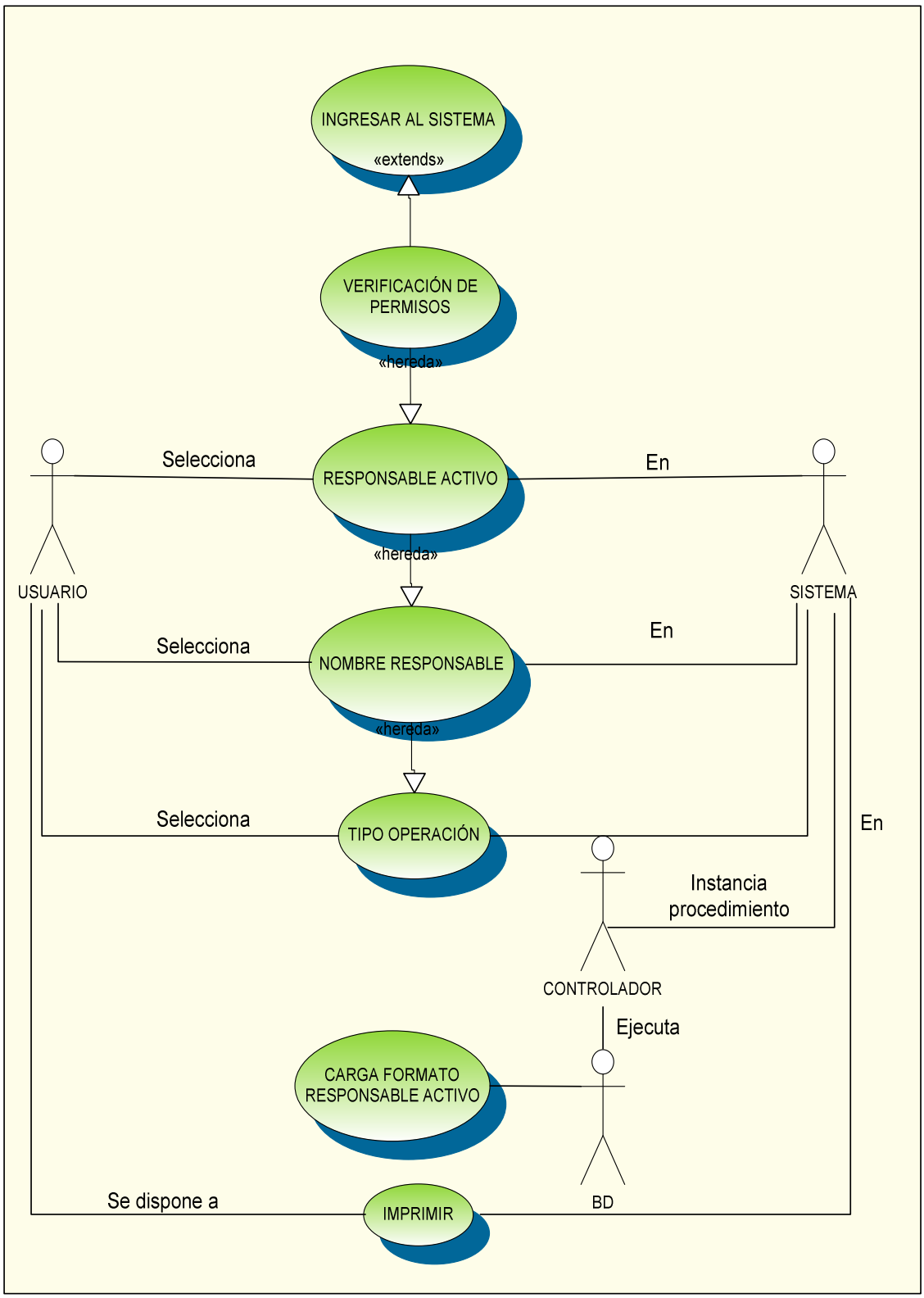
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el responsable activo			
	2. Captura la selección		
	3. Carga lista de responsable activo		
4. Selecciona el nombre del responsable			
	5. Solicita el tipo de operación a realizar		
6. Efectúa la selección			
	7. Instancia procedimiento almacenado		
		8. Busca y ejecuta package	
			9. Inicia el proceso interno responsable activo
	11. Carga formato de información sobre el responsable del activo con los siguientes datos: nombre, apellido, identificación		**10.** OK

Tabla 41. Caso de Uso 2.2, Responsable Activo

FIGURA 31. CASO DE USO RESPONSABLE ACTIVO



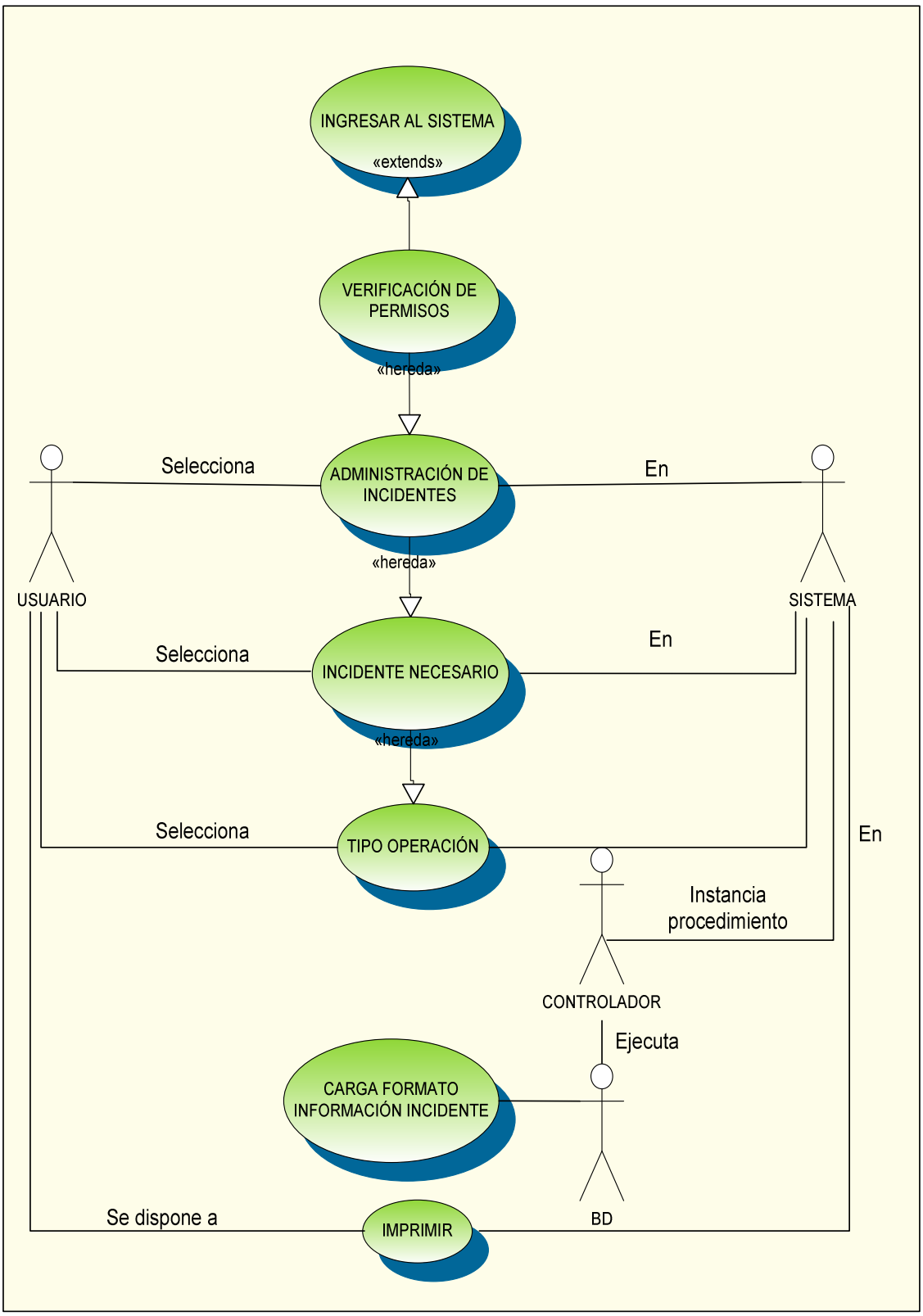
CASO DE USO 2.3:

- **Nombre:** Administración de incidentes.
- **Descripción:** Muestra al usuario datos relacionados con los incidentes y a su vez le permite a este modificar los datos de incidentes ocurridos con los activos.
- **Actores:** Usuario de tipo Administrador o usuario registrado.
- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem administración de incidentes	**2.** Captura la selección **3.** Carga lista de incidentes		
4. Selecciona el incidente del cual desea información	**5.** Solicita el tipo de operación a realizar		
6. Efectúa la selección	**7.** Instancia procedimiento almacenado	**8.** Busca y ejecuta package	**9.** Inicia el proceso interno administración de incidentes **10.** OK
	11. Carga formato de información del incidente presentando los siguientes datos: fecha, código, amenaza, descripción, responsable, seguimiento		

Tabla 42. Caso de Uso 2.3, Administración de Incidentes

FIGURA 32. CASO DE USO ADMINISTRACIÓN INCIDENTES



CASO DE USO 2.4:

- **Nombre:** Indicadores de gestión.

- **Descripción:** Muestra al usuario representaciones gráficas de relaciones entre diferentes factores de interacción y permite a este modificar los datos de gráficas en los indicadores.

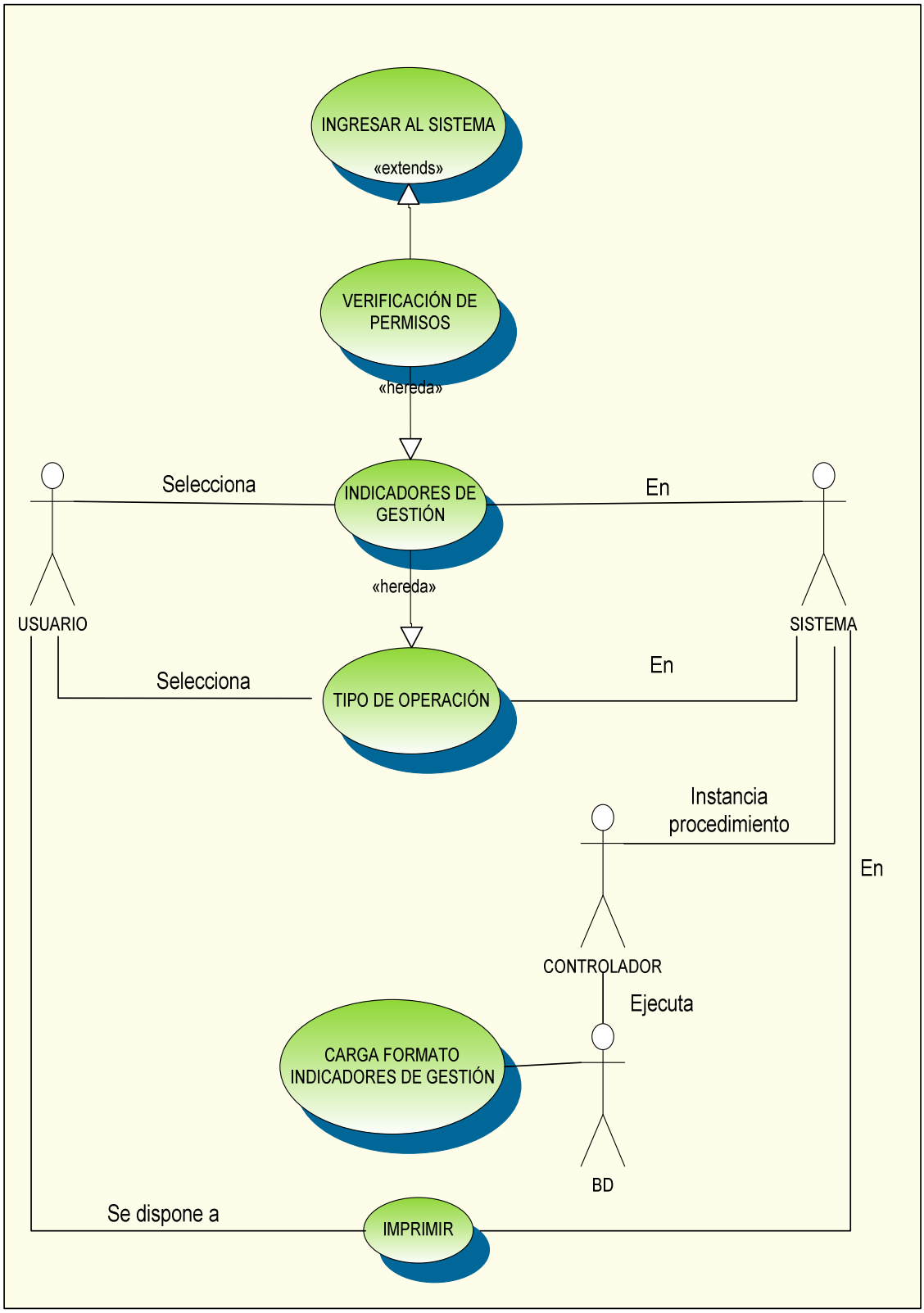
- **Actores:** Usuario de tipo Administrador o usuario registrado.

- ***Flujo Básico de Eventos:***

ACTOR	SISTEMA	CONTROLADOR	BASE DE DATOS
1. Selecciona el ítem de Indicadores de gestión			
	2. Captura la selección **3.** Solicita el tipo de operación a realizar		
4. Efectúa la selección			
	5. Instancia procedimiento almacenado		
		6. Busca y ejecuta package	**7.** Inicia el proceso interno indicadores de gestión
			8. OK
	9. Carga el formato de indicadores de gestión presentando los siguientes datos: nivel de mitigación, nivel de avance del plan de acción, eficiencia del plan de acción.		

Tabla 43. Caso de Uso 2.4, Indicadores de Gestión

FIGURA 33. CASO DE USO INDICADORES DE GESTIÓN

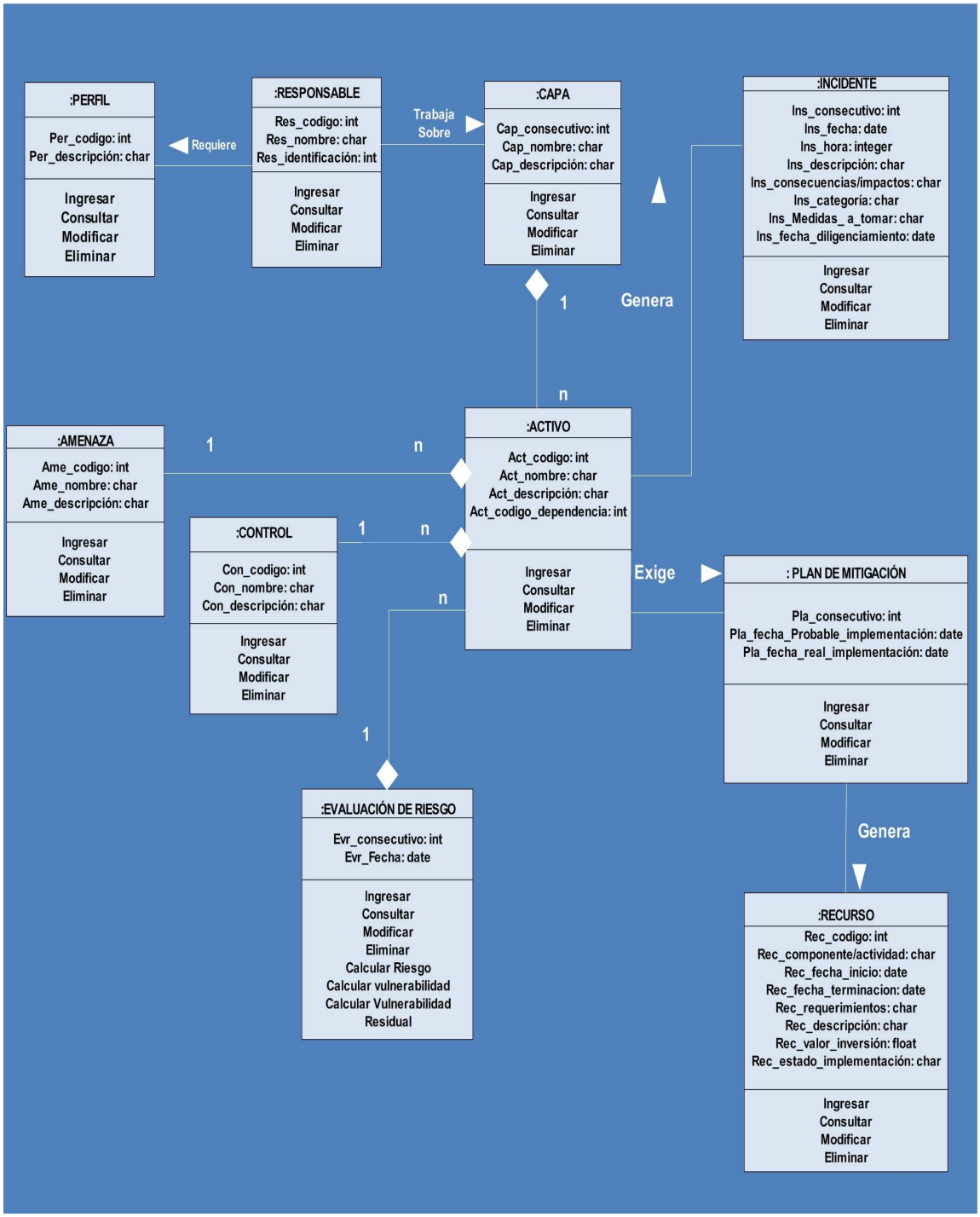


ACTIVIDAD 2. MODELO ESTÁTICO

- **DIAGRAMA DE CLASES**

Define la estructura del sistema que se va a modelar mediante un diagrama de clases que dispone el comportamiento general del SGSI.

FIGURA 34. DIAGRAMA DE CLASES



- **DICCIONARIO DE CLASES**

PERFIL		
Atributo	**Descripción**	**Tipo de dato**
per_codigo	Código que permite identificar el conjunto de permisos que posea el usuario	Integer
per_descripcion	Explica detalladamente la clasificación de los permisos de un usuario, existen 3 tipos: Administrador, Usuario Registrado u Otro Usuario	Char
RESPONSABLE		
Atributo	**Descripción**	**Tipo de dato**
res_codigo	Código que permite identificar personas que tienen a su cargo activos determinados	Integer
res_nombre	Nombre de la persona que tiene activos a su cargo	Char
res_identificacion	Cédula de ciudadanía del responsable	Integer
CAPA		
Atributo	**Descripción**	**Tipo de dato**
cap_consecutivo	Número sucesivo que permite la identificación de cada una de los niveles en los que esta dividida la empresa	Integer
cap_nombre	Denominación dada a cada una de las capas, estas son: Ambiente Instalaciones Tecnológicas, Ambiente Operativo de Escritorio y Red, Ambiente de Bases de Datos, Ambiente de Aplicativos, Datos, proceso de Negocio, Energía.	Char

cap_descripcion	Explicación detallada de cada una de las capas su importancia y utilidad dentro de la empresa	Char
ACTIVO		
Atributo	**Descripción**	**Tipo de dato**
act_codigo	Número único que permite identificar el activo al que se haga referencia	Integer
act_nombre	Denominación dada a los activos que se encuentran dentro de la empresa	Char
act_descripcion	Explicación detallada del activo que presta servicio a la empresa	Char
act_codigo_ dependencia	Número único que permite identificar a que activo padre se encuentra asociado el activo al que se hace referencia	Integer
CONTROL		
Atributo	**Descripción**	**Tipo de dato**
con_codigo	Número que permite identificar el control al que se haga referencia	Integer
con_nombre	Denominación dada a cada uno de los controles que están establecidos en la empresa	Char
con_descripcion	Explicación detallada de los controles específicos que implementa la empresa	Char
AMENAZA		
Atributo	**Descripción**	**Tipo de dato**
ame_codigo	Número que permite identificar la amenaza a la cual se encuentran expuestos los	Integer

	activos	
ame_nombre	Denominación dada a cada una de las amenazas que han sido identificadas en la empresa	Char
ame_descripcion	Explicación detallada de las amenazas específicas encontradas	Char
EVALUACIÓN DE RIESGO		
Atributo	**Descripción**	**Tipo de dato**
evr_consecutivo	Número sucesivo que permite la identificación de cada una de las evaluaciones que han sido realizadas para activos específicos a lo largo del tiempo	Integer
evr_fecha	Especificación del tiempo o momento en el que ha sido realizada la evaluación del riesgo	Date
RECURSO		
Atributo	**Descripción**	**Tipo de dato**
rec_codigo	Número único que permite identificar un recurso específico	Integer
rec_componente/actividad	Identifica y describe las tareas o procedimientos que se tendrán en cuenta si existe una amenaza	Char
rec_fecha_inicio	Especificación del tiempo o momento en el que ha sido iniciado el recurso	Date
rec_fecha_terminacion	Especificación del tiempo o momento en el que ha sido finalizado el recurso	Date
rec_requerimientos	Define las características solicitadas que son necesarias para el recurso	Char

rec_descripción	Explica detalladamente cual es la utilidad y beneficio que puede traer el recurso	Char
rec_valor_inversión	Expone el capital probable que debe ser invertido para la correcta implementación del recurso	Float
rec_estado_implementación	Manifiesta el estado en el que se encuentra la implementación del recurso	Char
PLAN DE MITIGACIÓN		
Atributo	**Descripción**	**Tipo de dato**
pla_consecutivo	Número sucesivo que permite la identificación de cada uno de los planes de mitigación que han sido propuestos para mitigar los riesgos de un activo	int
pla_fecha_probable_implementación	Especificación del tiempo o momento probable en el que se pondrá en funcionamiento algún tipo de plan de mitigación	date
pla_fecha_real_implementación	Especificación del tiempo o momento concreto en el que se pondrá en funcionamiento algún tipo de plan de mitigación	date
INCIDENTE		
Atributo	**Descripción**	**Tipo de dato**
ins_consecutivo	Número sucesivo que permite la identificación de cada uno de los incidentes que han sido reconocidos en la empresa o que probablemente puedan afectar la empresa	int
ins_fecha	Especificación del tiempo o momento en el que se ha presentado un incidente	date

ins_hora	Especificación del tiempo o momento en el que se ha presentado un incidente	integer
ins_descripción	Explicación detallada de cuales son los perjuicios y problemas que trae consigo el incidente	char
ins_consecuencias /impactos	Define los hechos o acontecimientos que intervienen en la aparición del incidente	char
ins_categoría	Define los grupos básicos en los que pueden ser divididos los incidentes de una forma global	char
ins_medidas_ a_tomar	Determina las decisiones que serán implantadas para combatir el incidente	char
ins_fecha_diligenciamiento	Especificación del tiempo o momento en el que se gestiona la información concreta del incidente presentado	date

Tabla 44. Diccionario de Clases

ACTIVIDAD 3. MODELO DINÁMICO

- **DIAGRAMA DE SECUENCIA**

Muestra las interacciones de un usuario con el sistema. Interacción es una cadena de mensajes enviados entre los objetos en respuesta a un evento generado por el usuario sobre la aplicación.

El Diagrama de Secuencia es uno de los diagramas más efectivos para modelar la interacción entre objetos en un sistema. Un diagrama de secuencia se modela para cada caso de uso, este contiene detalles de implementación, incluyendo los mensajes pasados entre los objetos, para lograrlo se examina la descripción de un caso de uso y se determinan los objetos necesarios para la implementación del escenario. Si se tiene modelada la descripción de cada caso de uso como una secuencia de varios pasos, el movimiento a seguir es recorrer estos pasos y así descubrir los objetos necesarios para seguir dichos pasos.

FIGURA 35. DIAGRAMA DE SECUENCIA ESTANDAR CONSULTAR

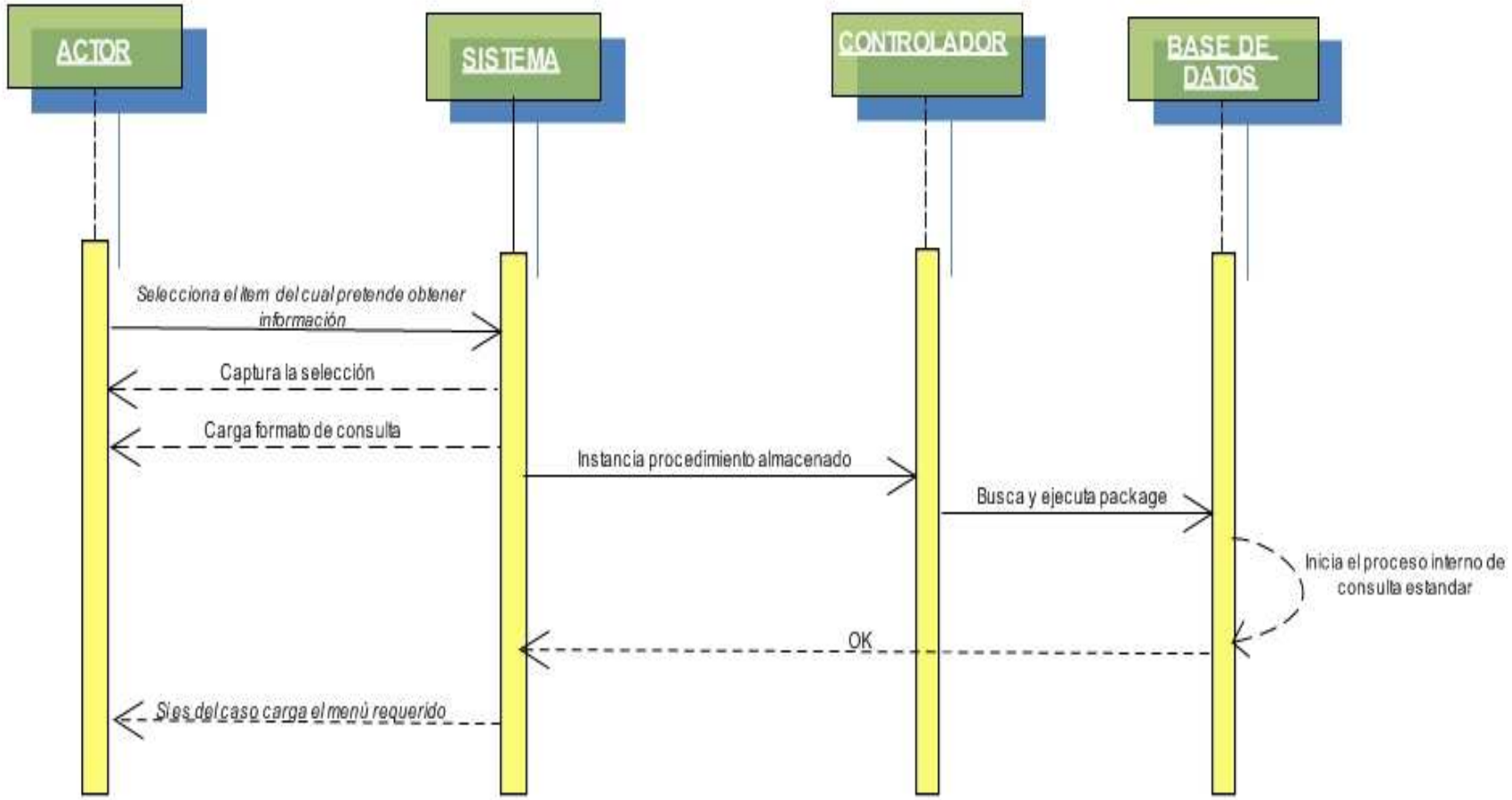


FIGURA 36. DIAGRAMA DE SECUENCIA ESTANDAR INGRESAR

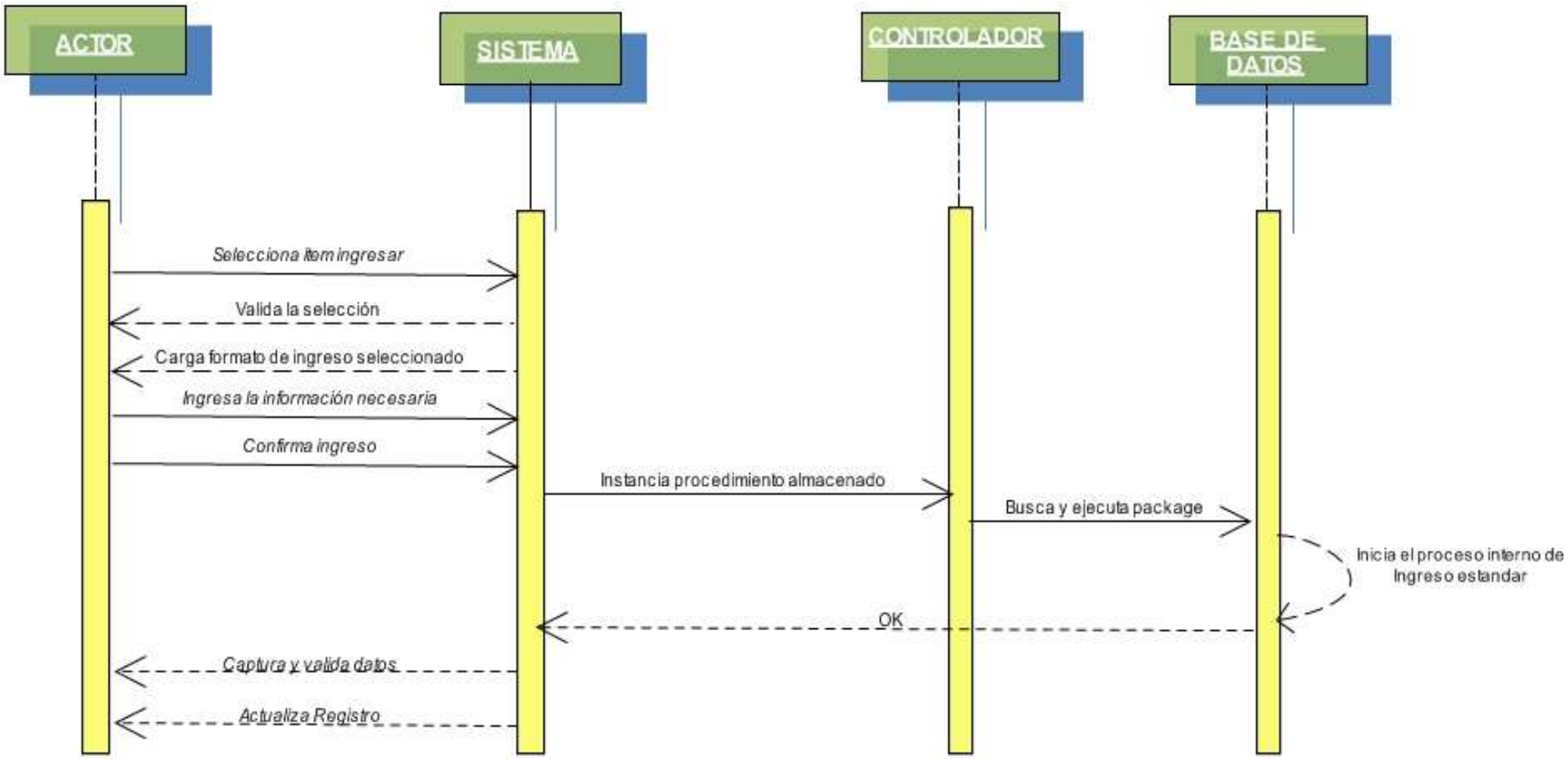


FIGURA 37. DIAGRAMA DE SECUENCIA ESTÁNDAR MODIFICAR

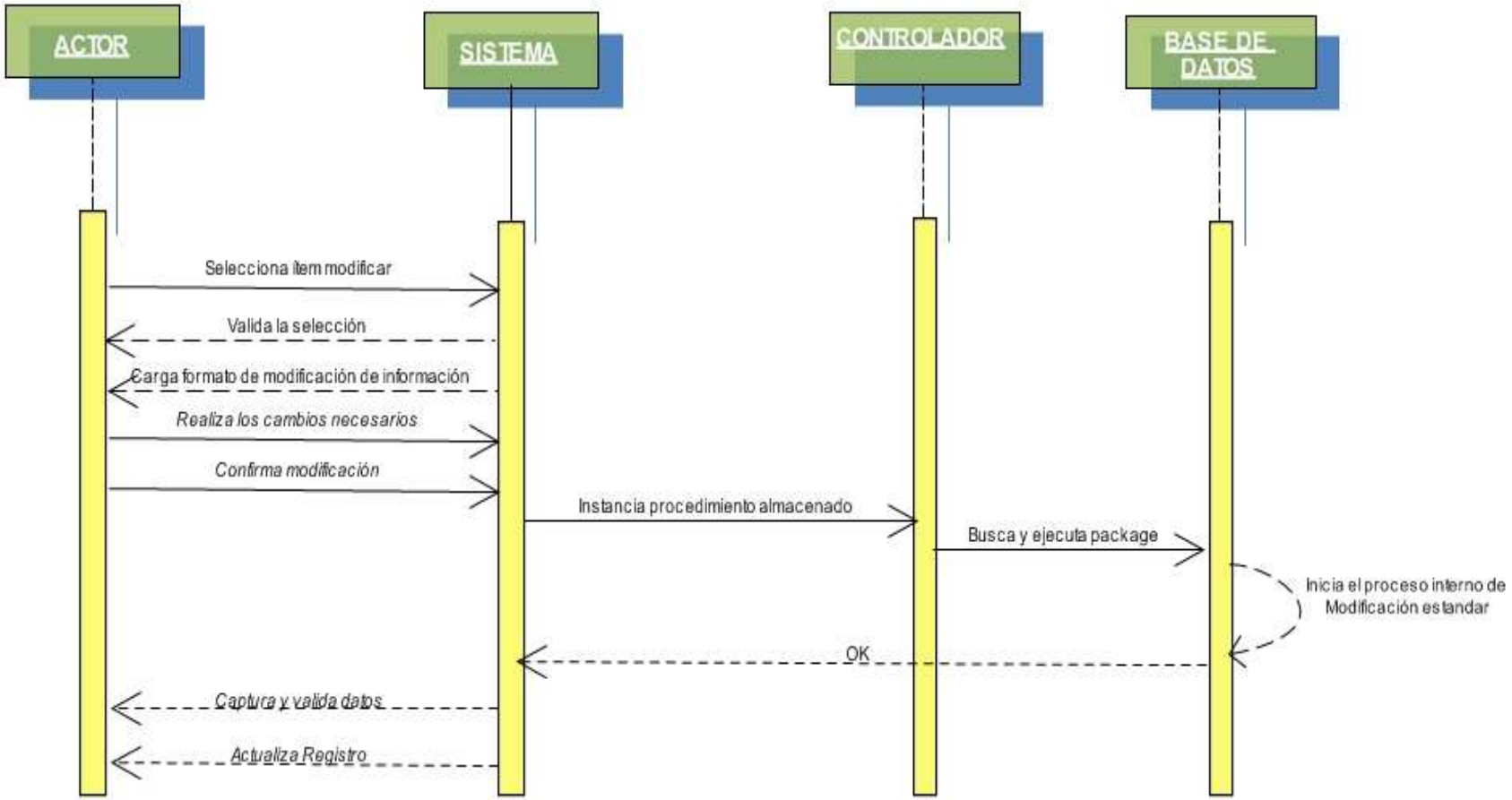


FIGURA 38. DIAGRAMA DE SECUENCIA ESTÁNDAR ELIMINAR

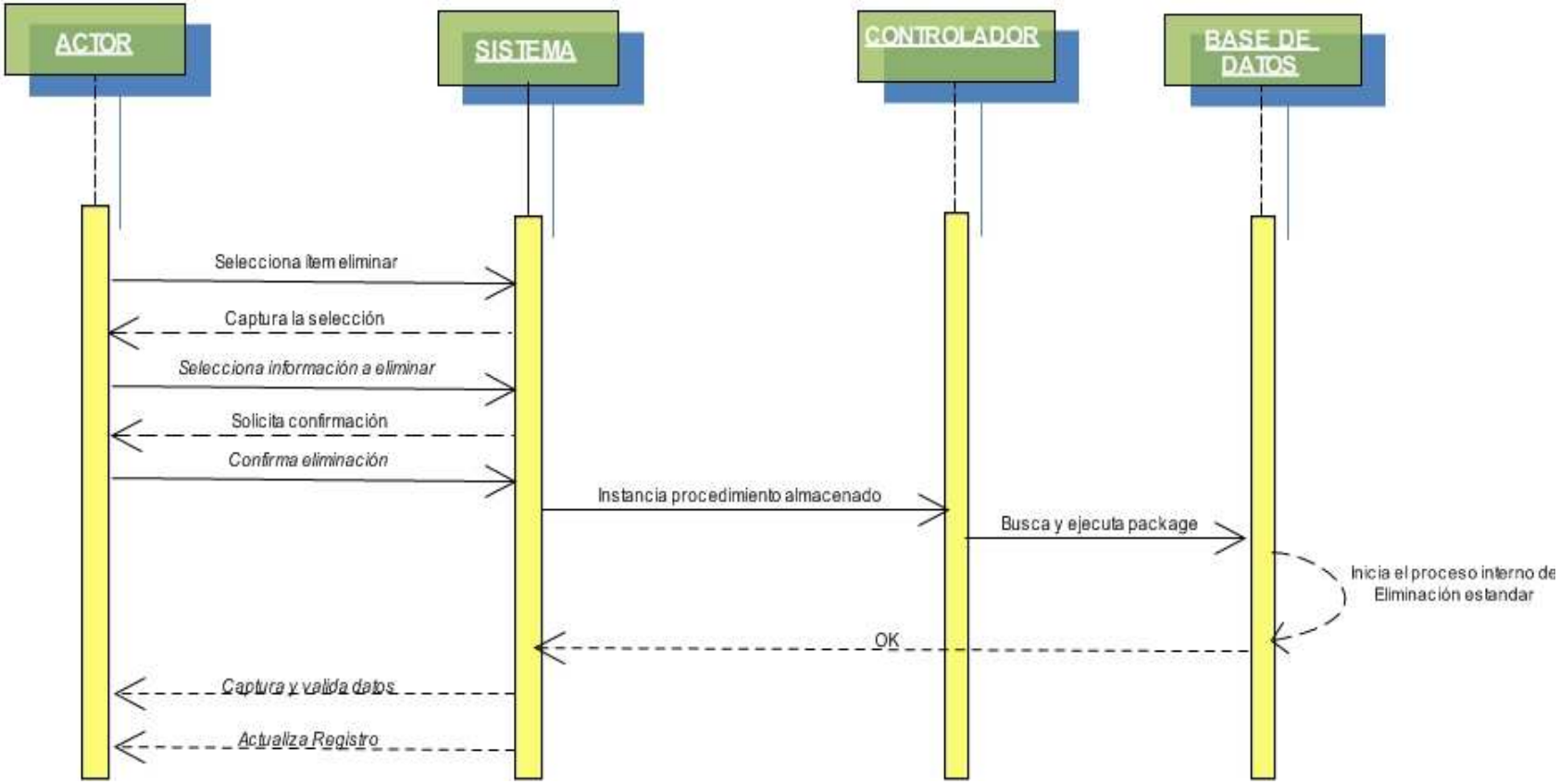


FIGURA 39. DIAGRAMA DE SECUENCIA INGRESAR AL SISTEMA

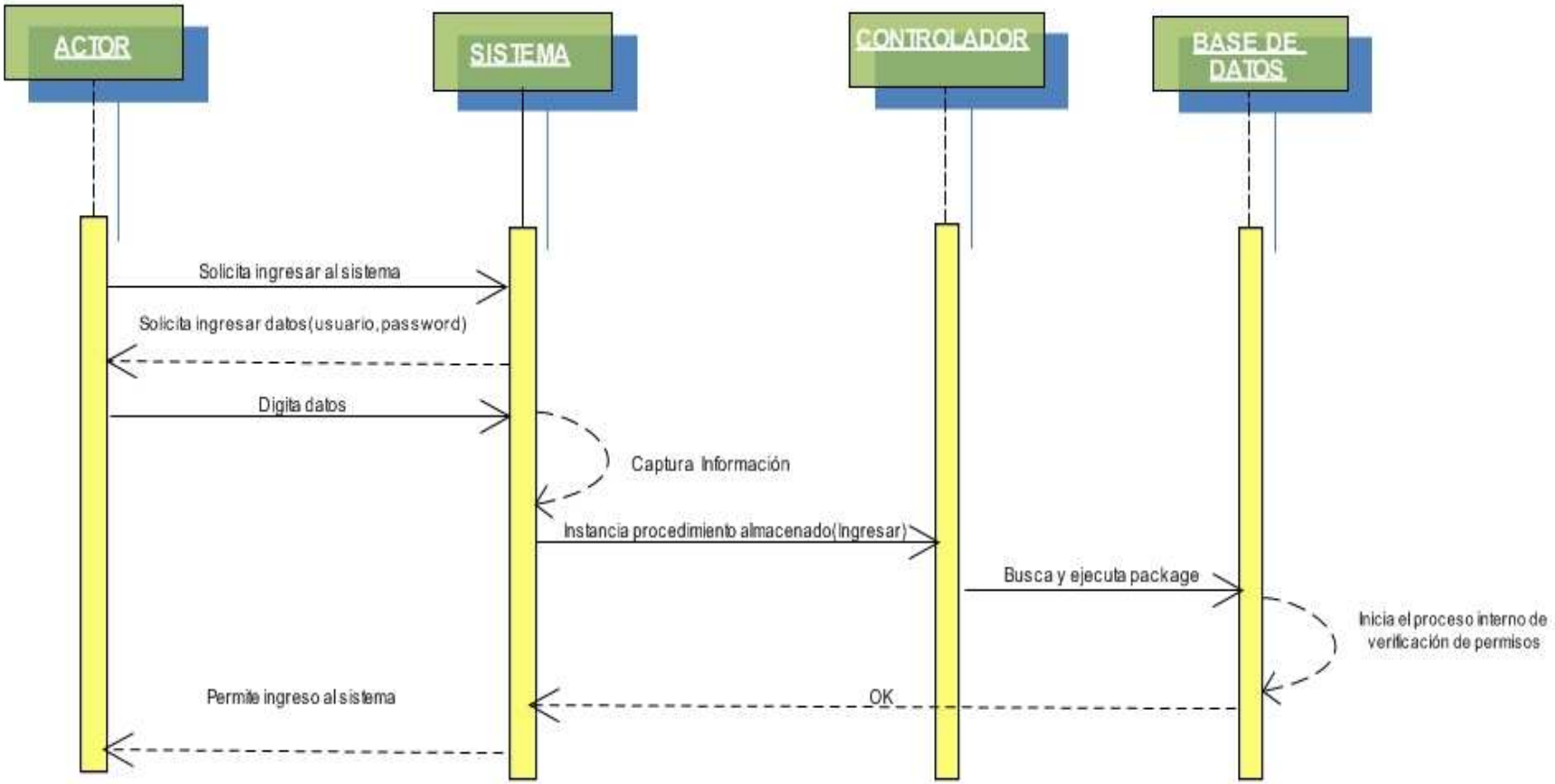


FIGURA 40. DIAGRAMA DE SECUENCIA VERIFICACIÓN DE PERMISOS

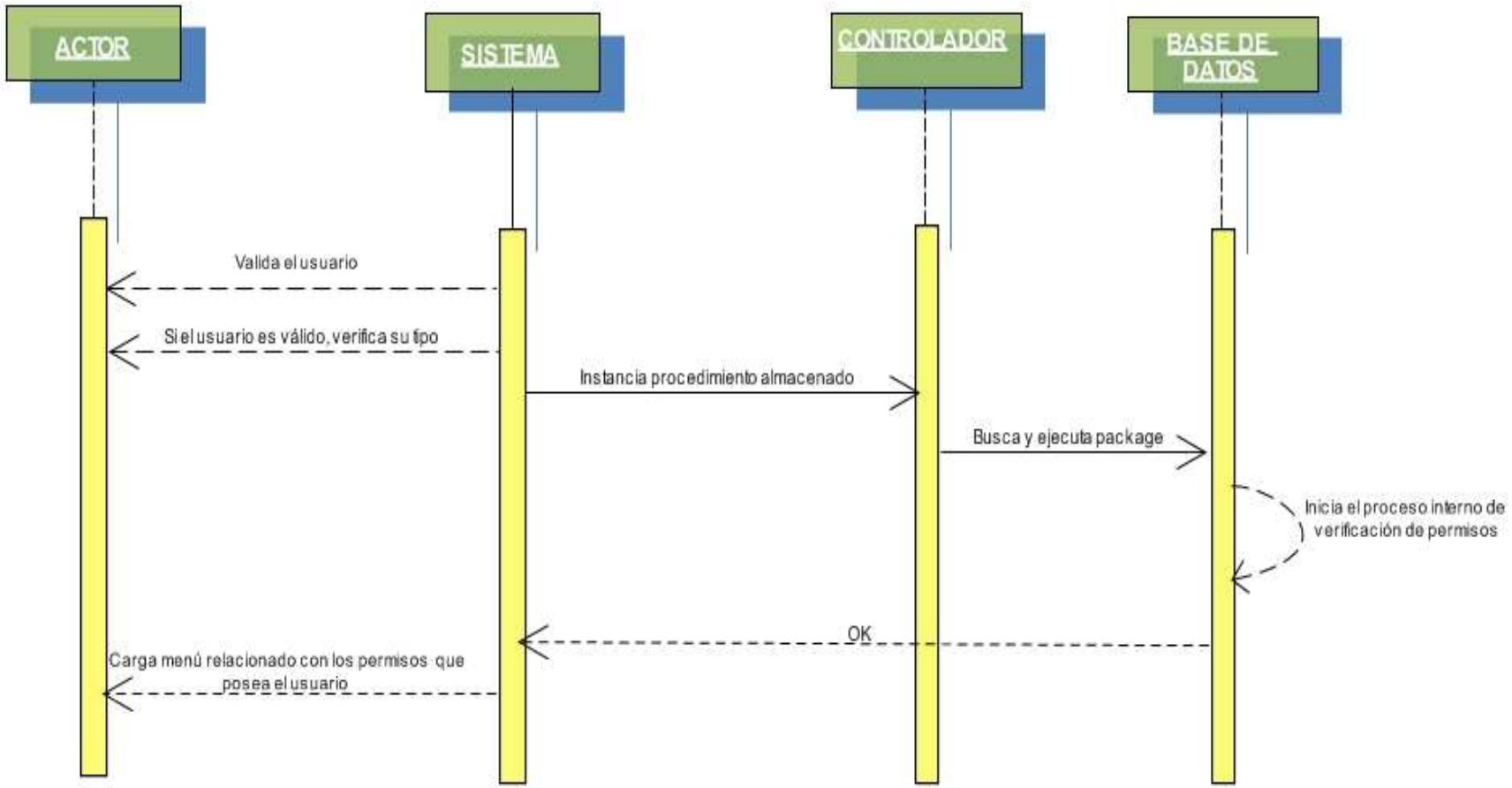


FIGURA 41. DIAGRAMA DE SECUENCIA MANEJO DE ACTIVOS

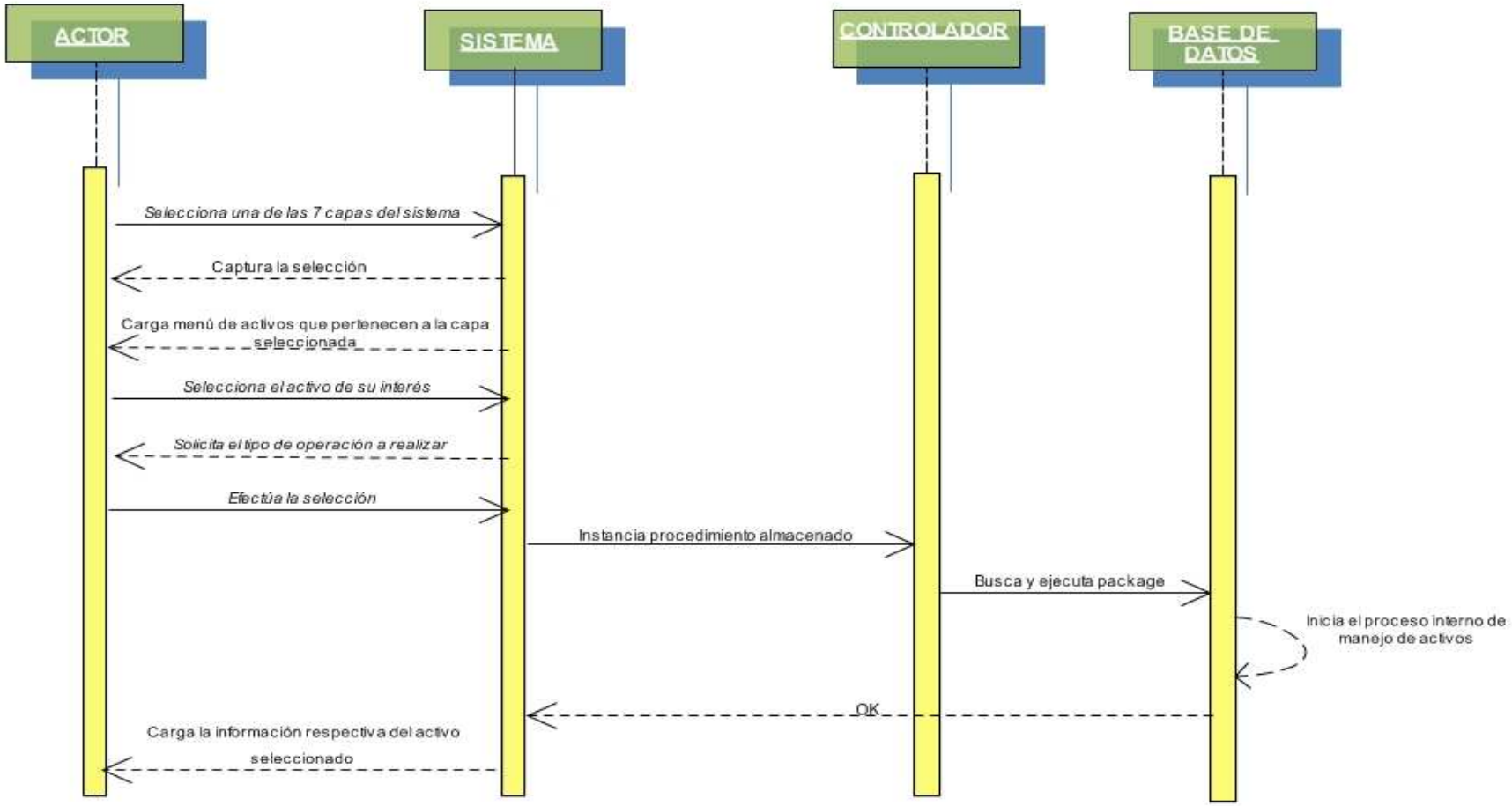


FIGURA 42. DIAGRAMA DE SECUENCIA DIAGNOSTICO AMENAZA- RIESGO

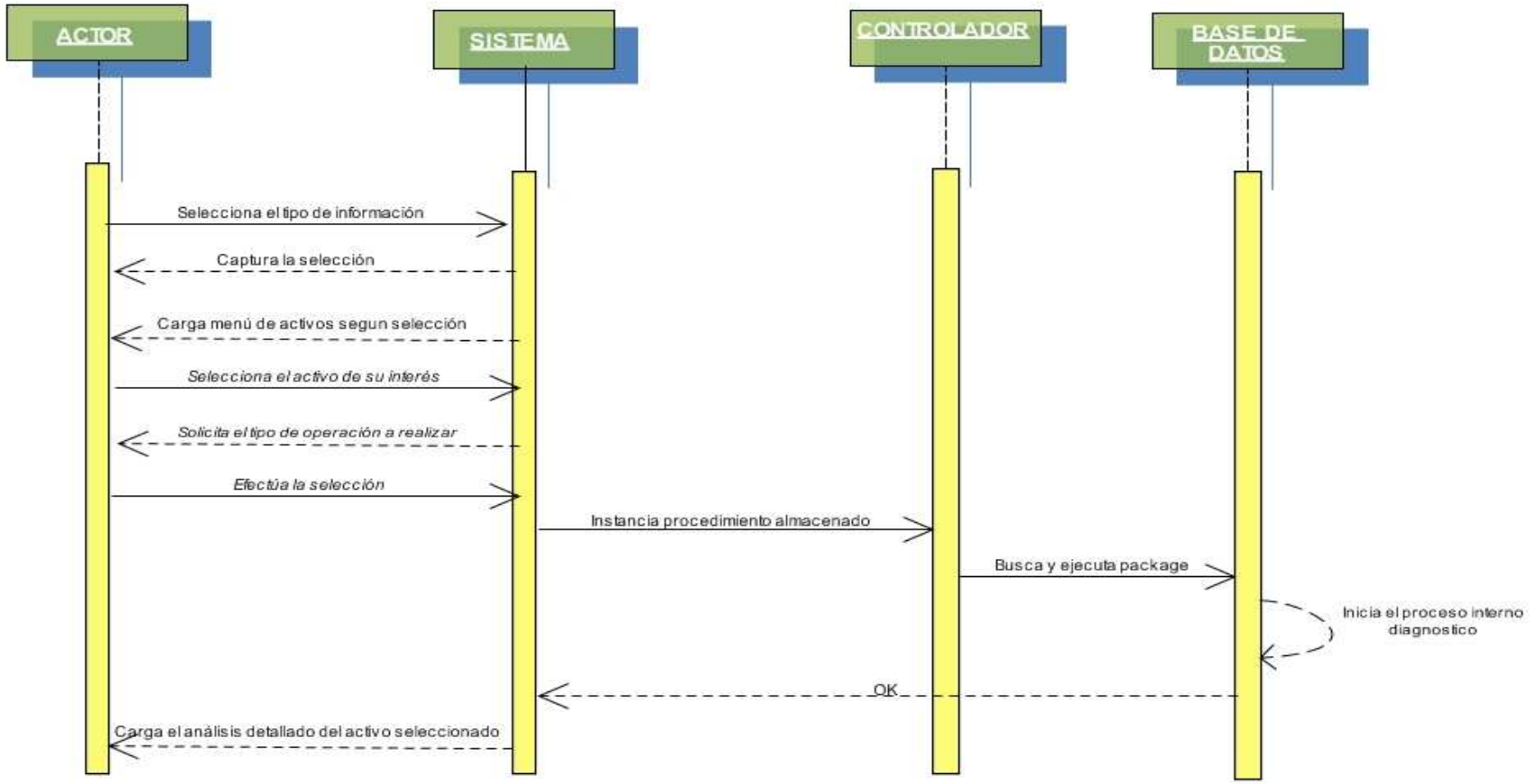


FIGURA 43. DIAGRAMA DE SECUENCIA INFORMACIÓN AMENAZA

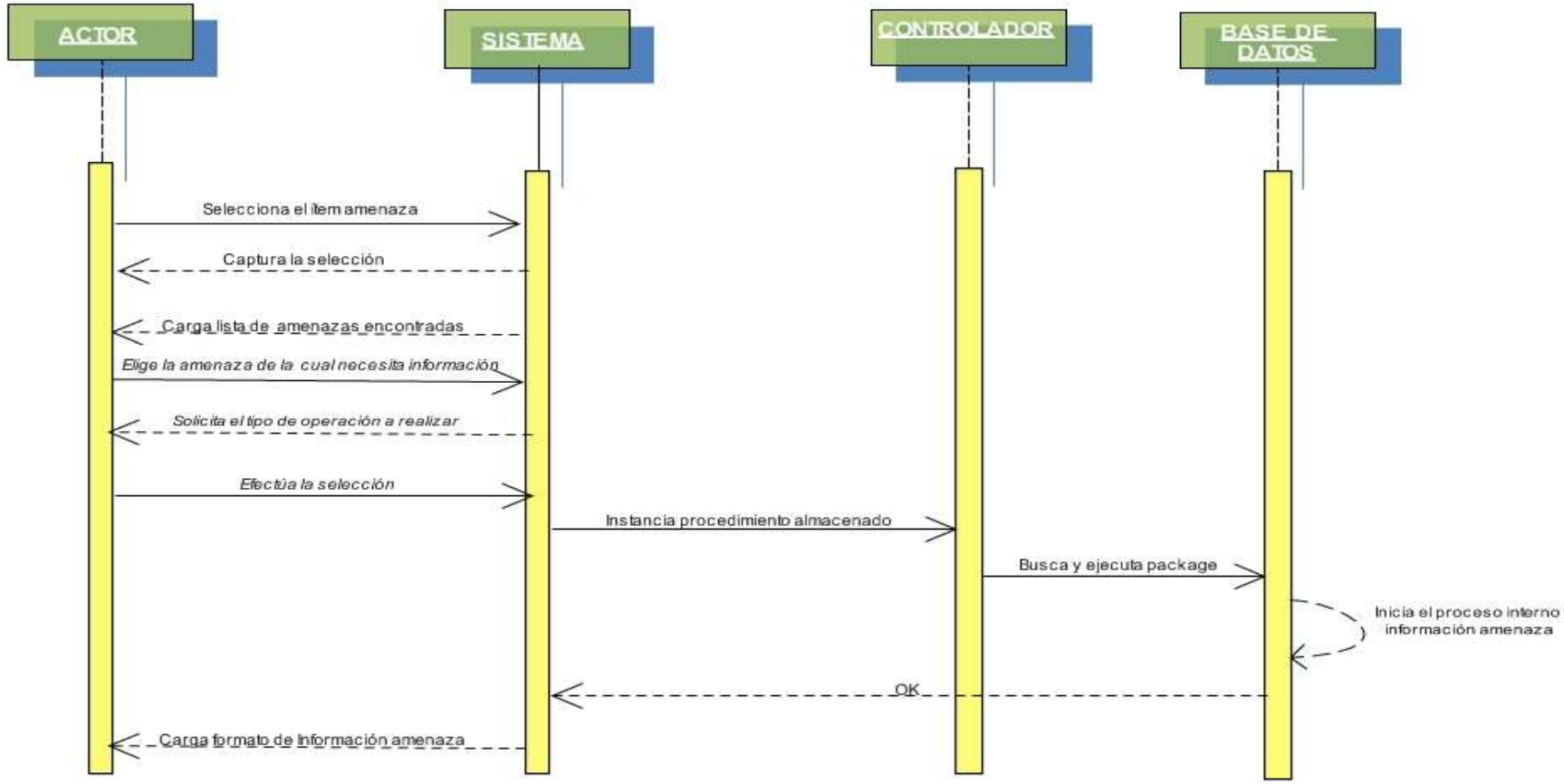


FIGURA 44. DIAGRAMA DE SECUENCIA INFORMACIÓN CONTROL

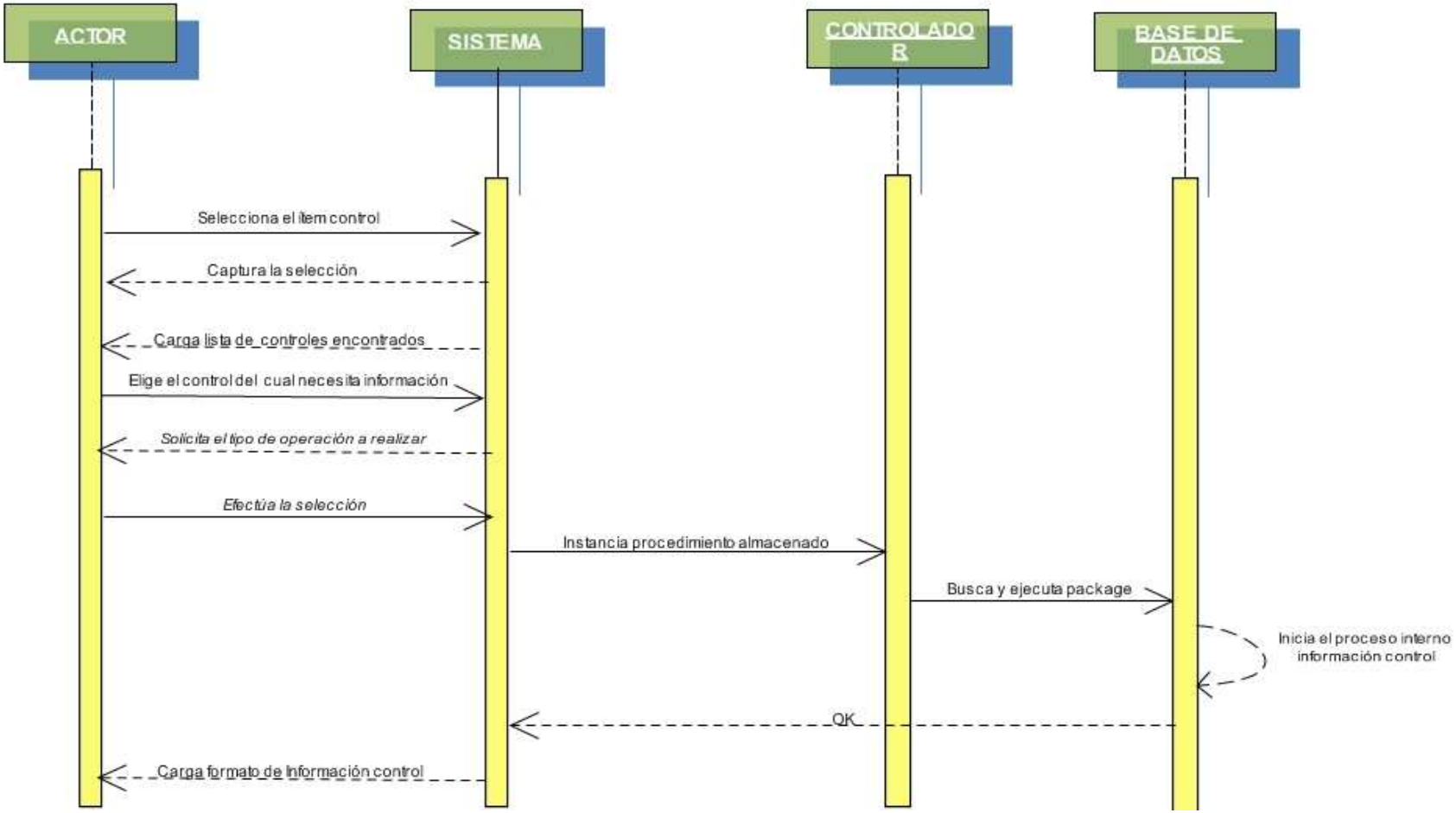


FIGURA 45. DIAGRAMA DE SECUENCIA EVALUACIÓN DE RIESGO

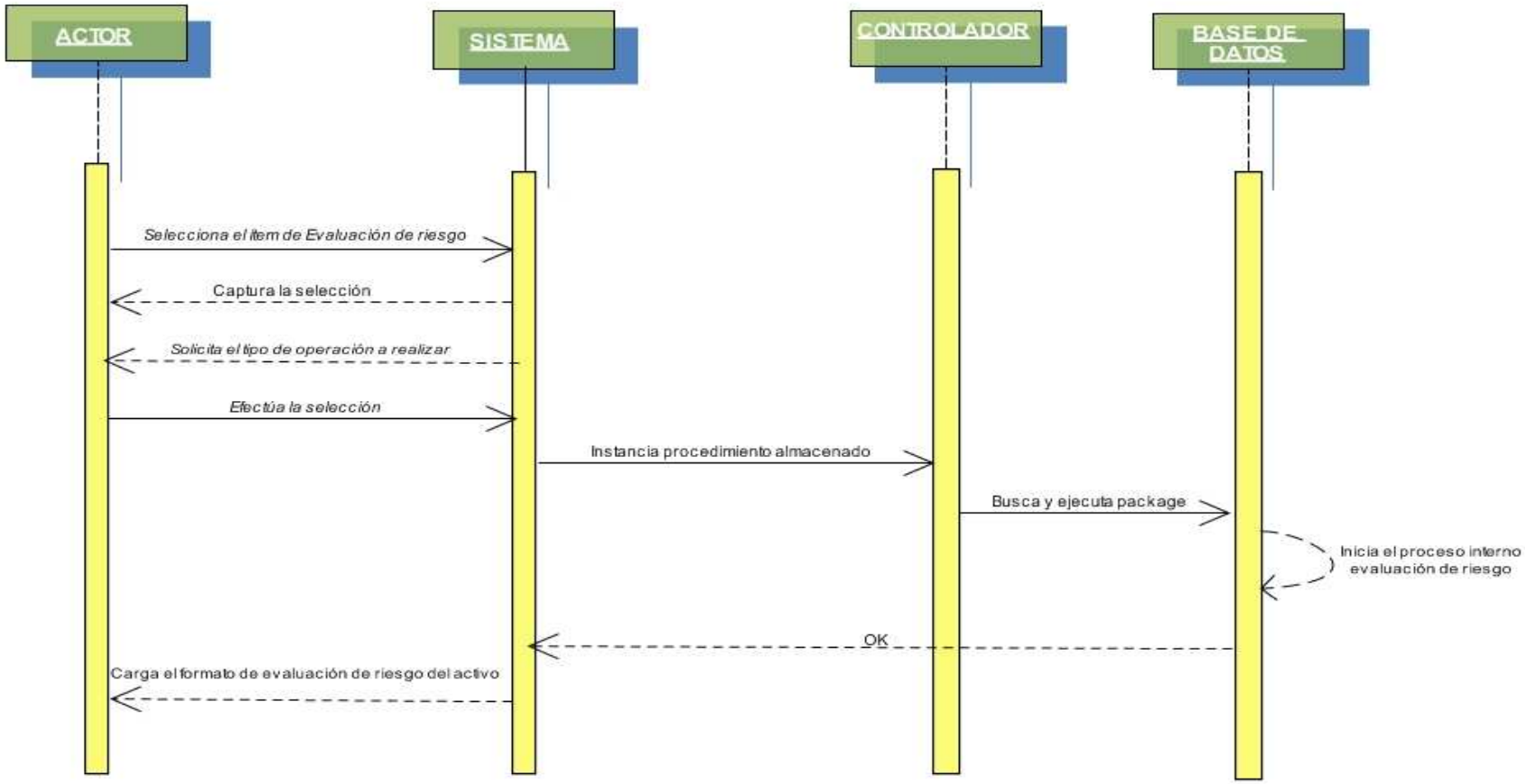


FIGURA 46. DIAGRAMA DE SECUENCIA VALORACIÓN PROBABILIDAD

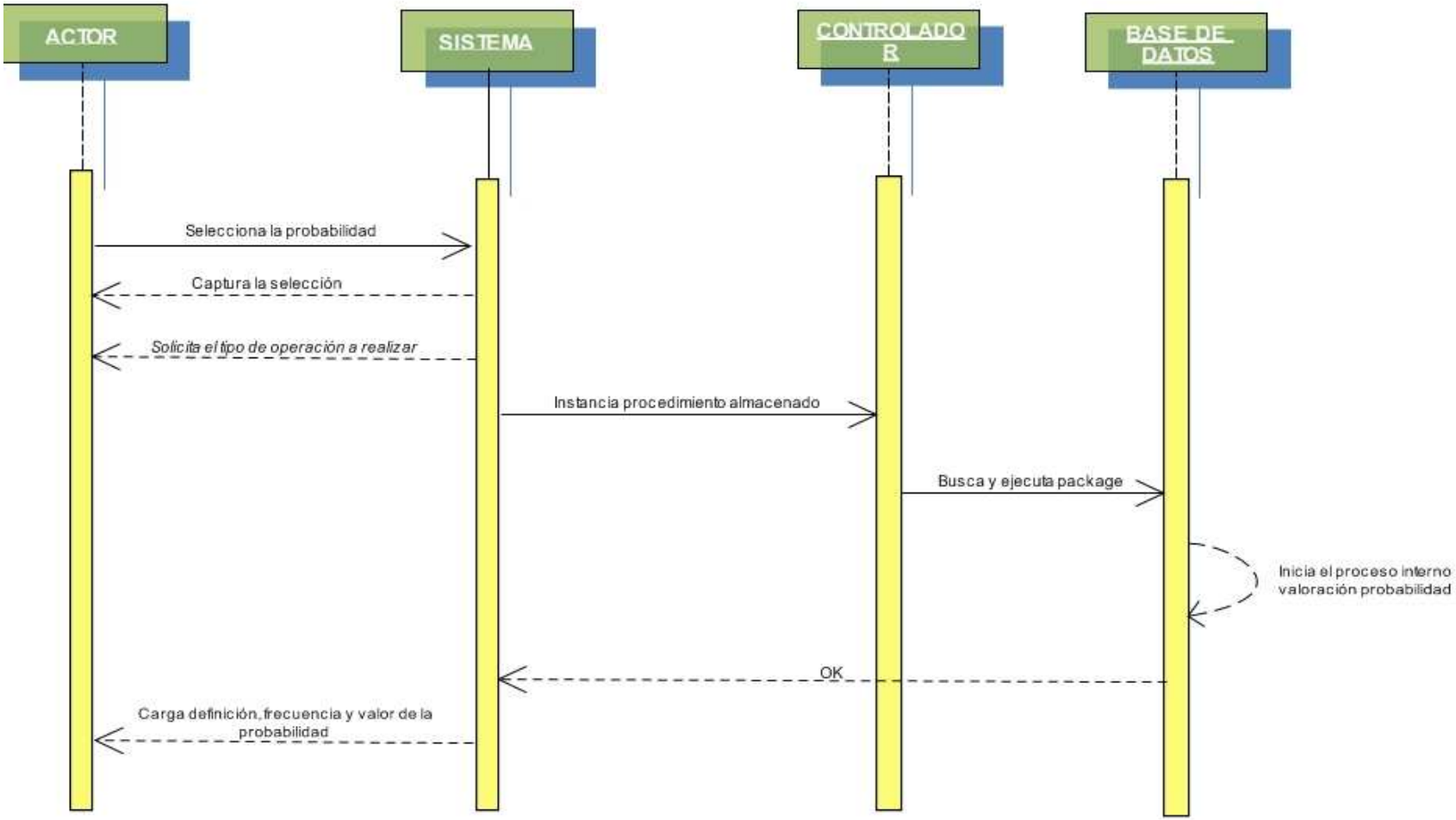


FIGURA 47. DIAGRAMA DE SECUENCIA VALORACIÓN IMPACTO

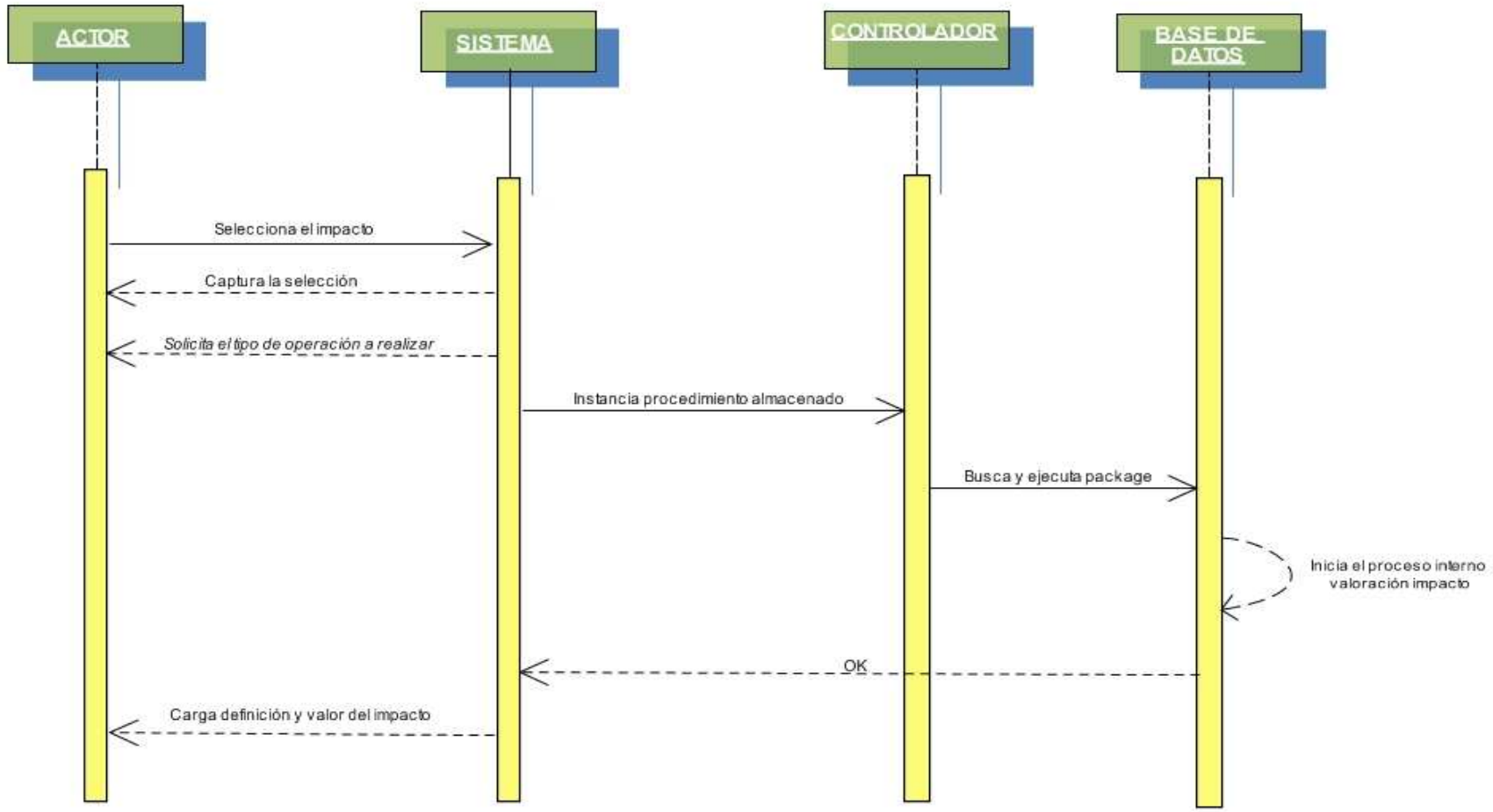


FIGURA 48. DIAGRAMA DE SECUENCIA VALORACIÓN VULNERABILIDAD

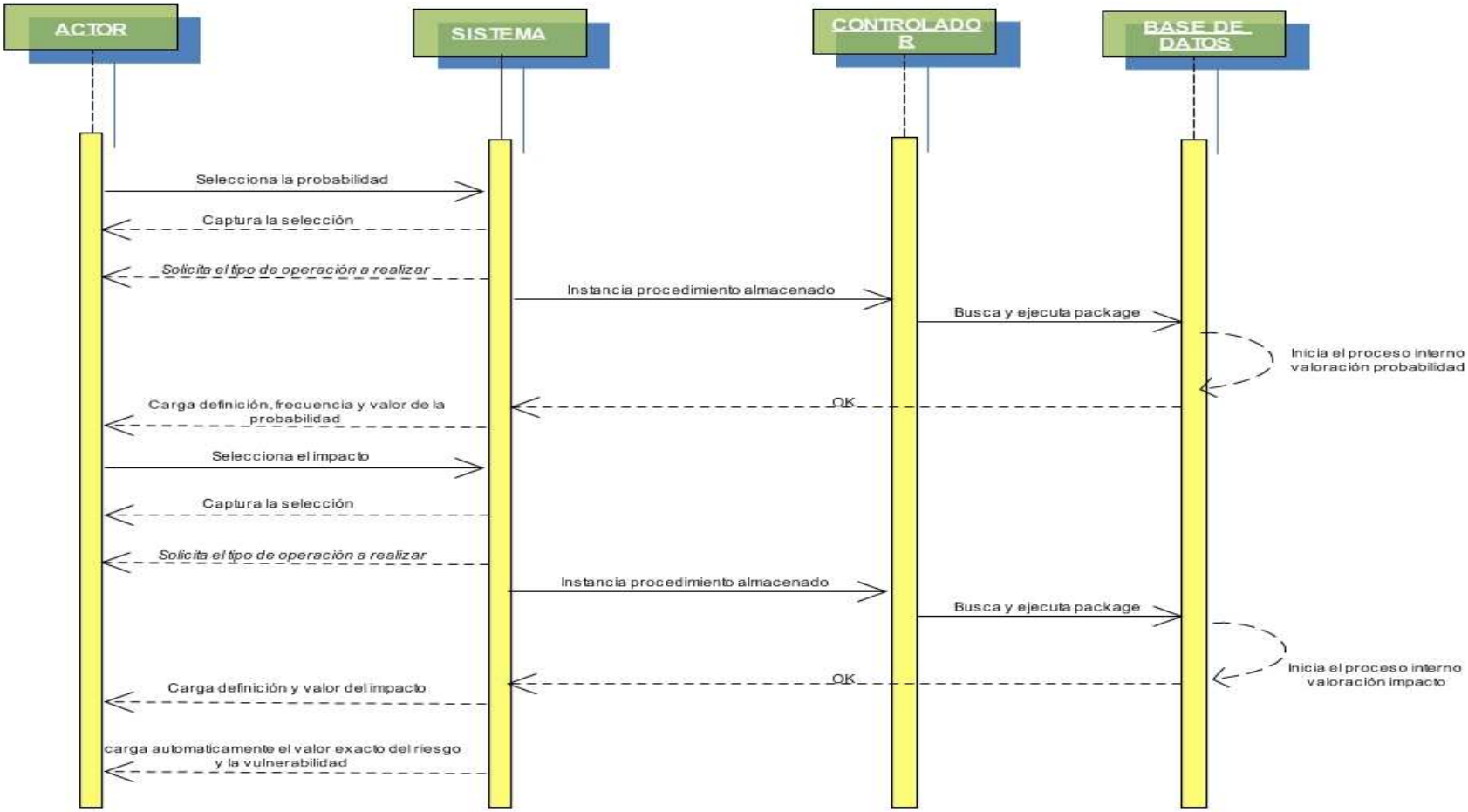


FIGURA 49. DIAGRAMA DE SECUENCIA VALORACIÓN VULNERABILIDAD RESIDUAL

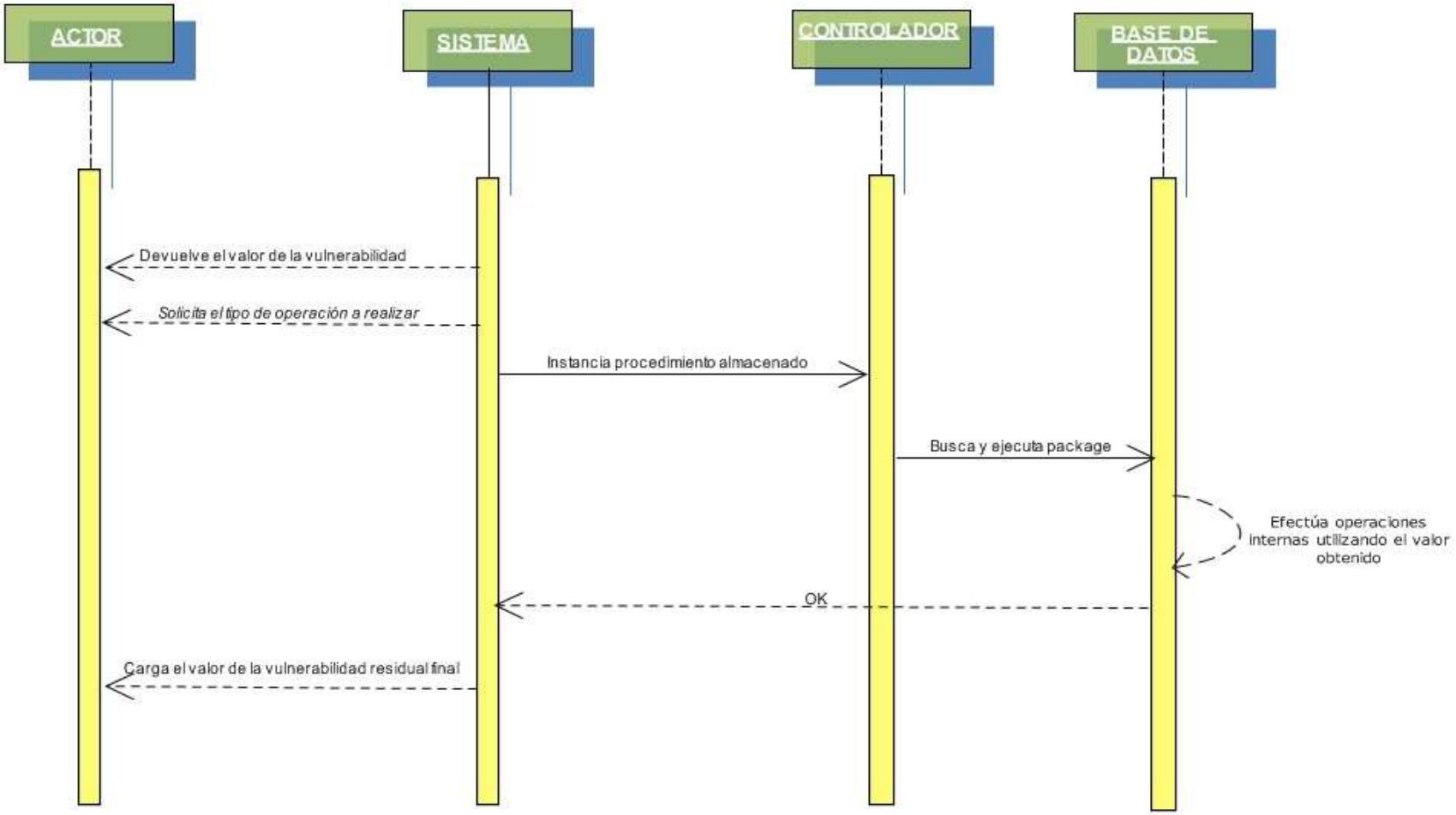


FIGURA 50. DIAGRAMA DE SECUENCIA VALORACIÓN CALIFICACIÓN

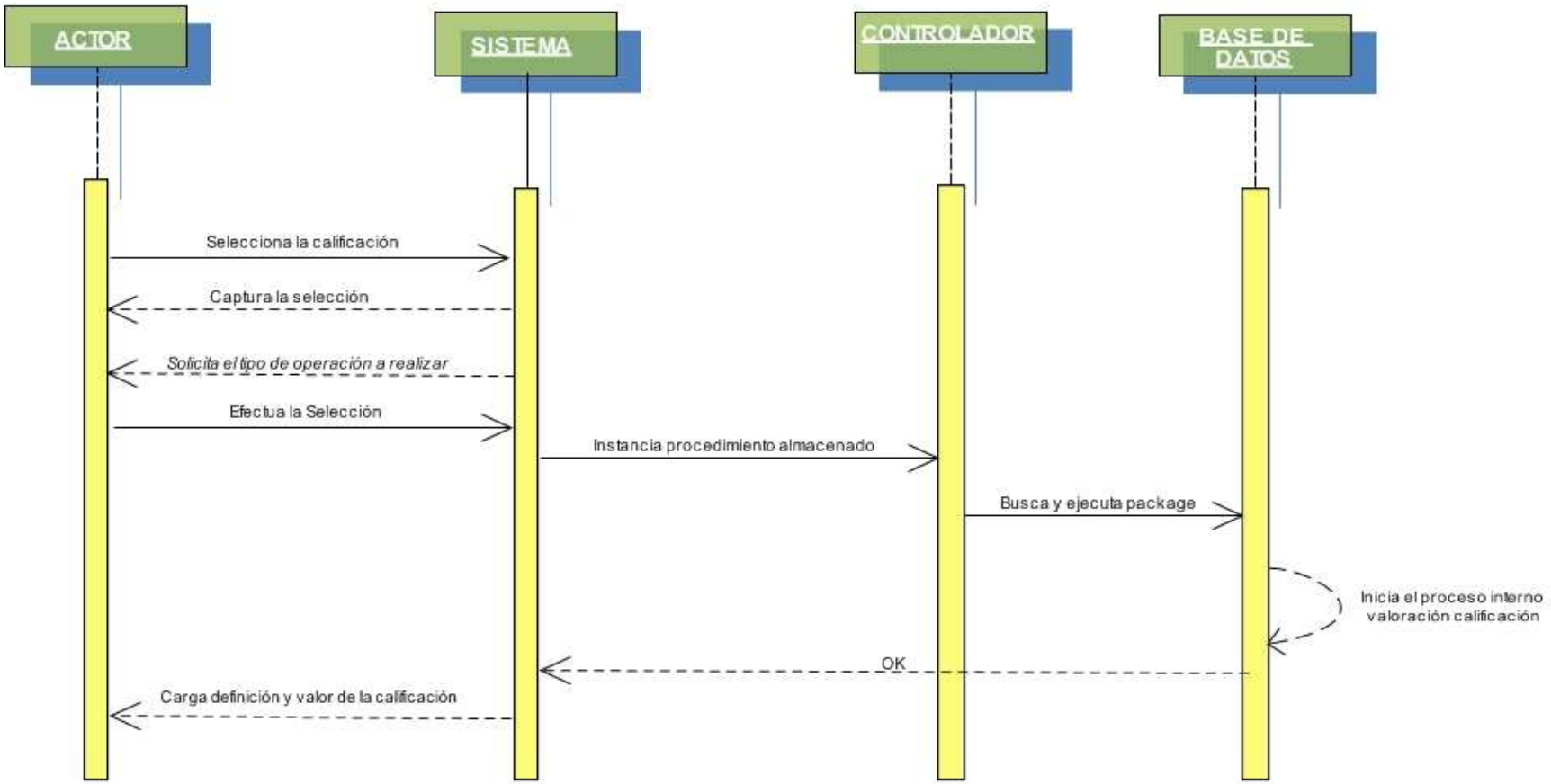


FIGURA 51. PLAN DE MITIGACIÓN

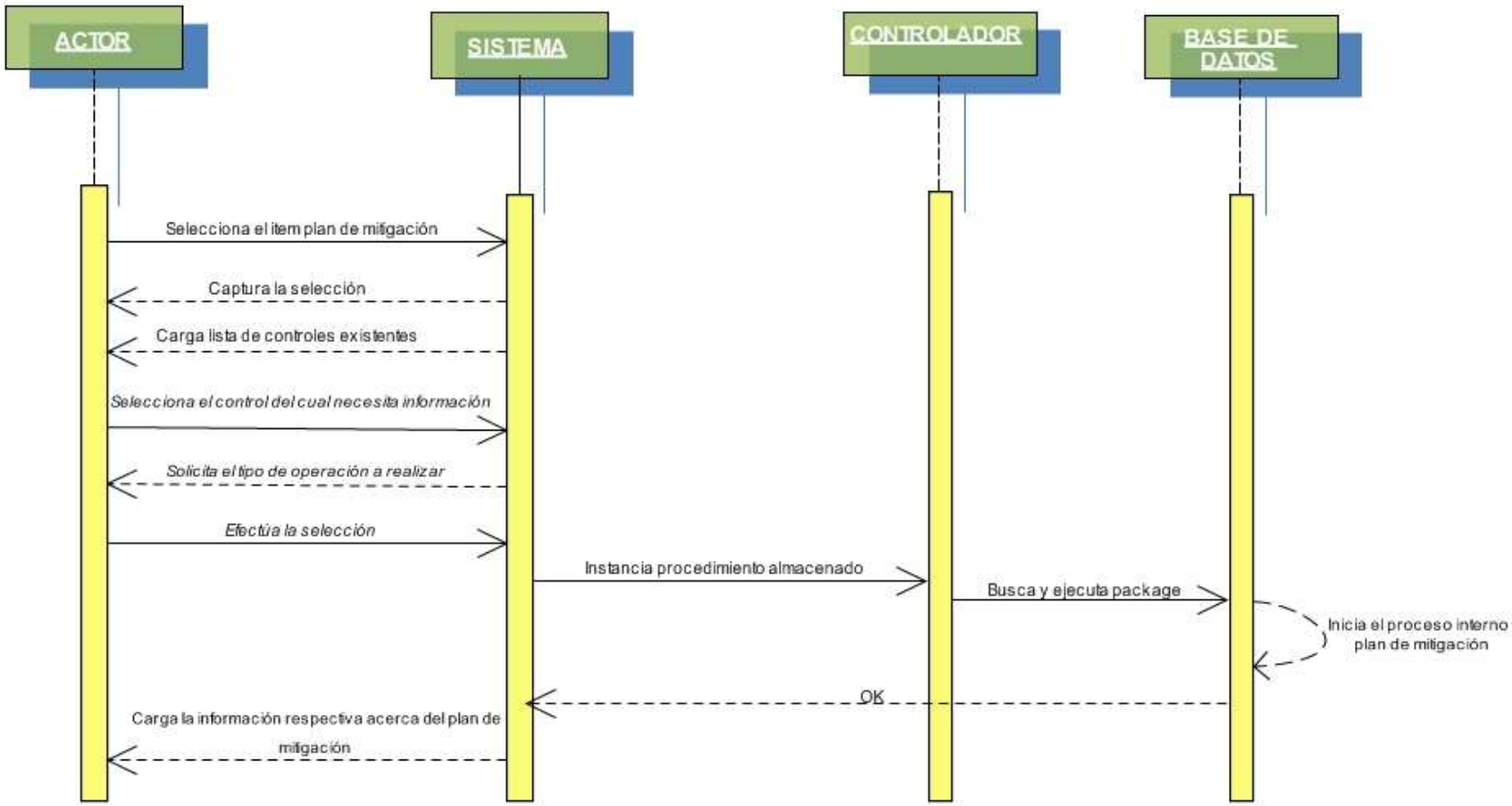


FIGURA 52. DIAGRAMA DE SECUENCIA CONTROL NORMA

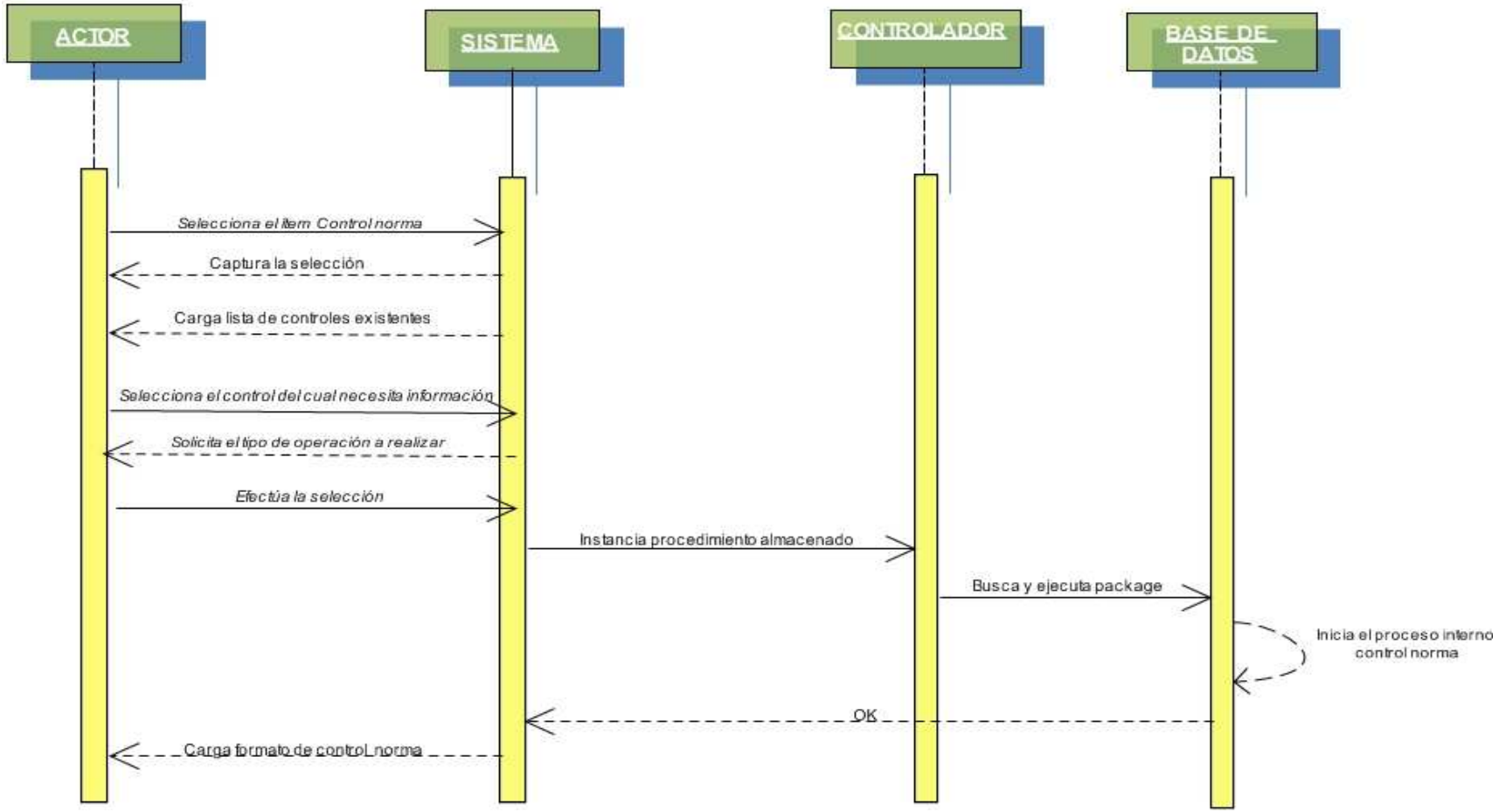


FIGURA 53. DIAGRAMA DE SECUENCIA DISPOSICIÓN DE RECURSOS

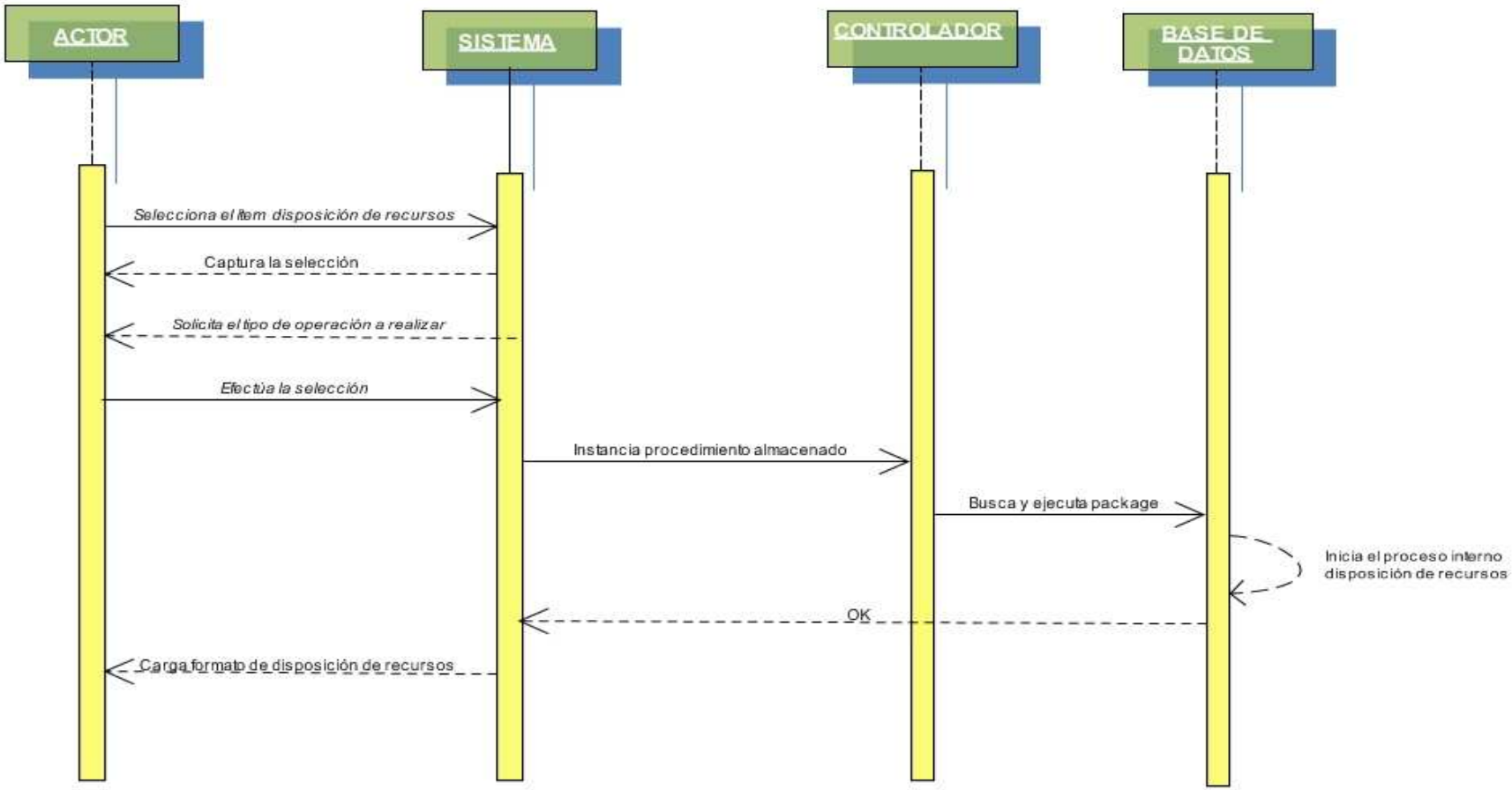


FIGURA 54. DIAGRAMA DE SECUENCIA RESPONSABLE ACTIVO

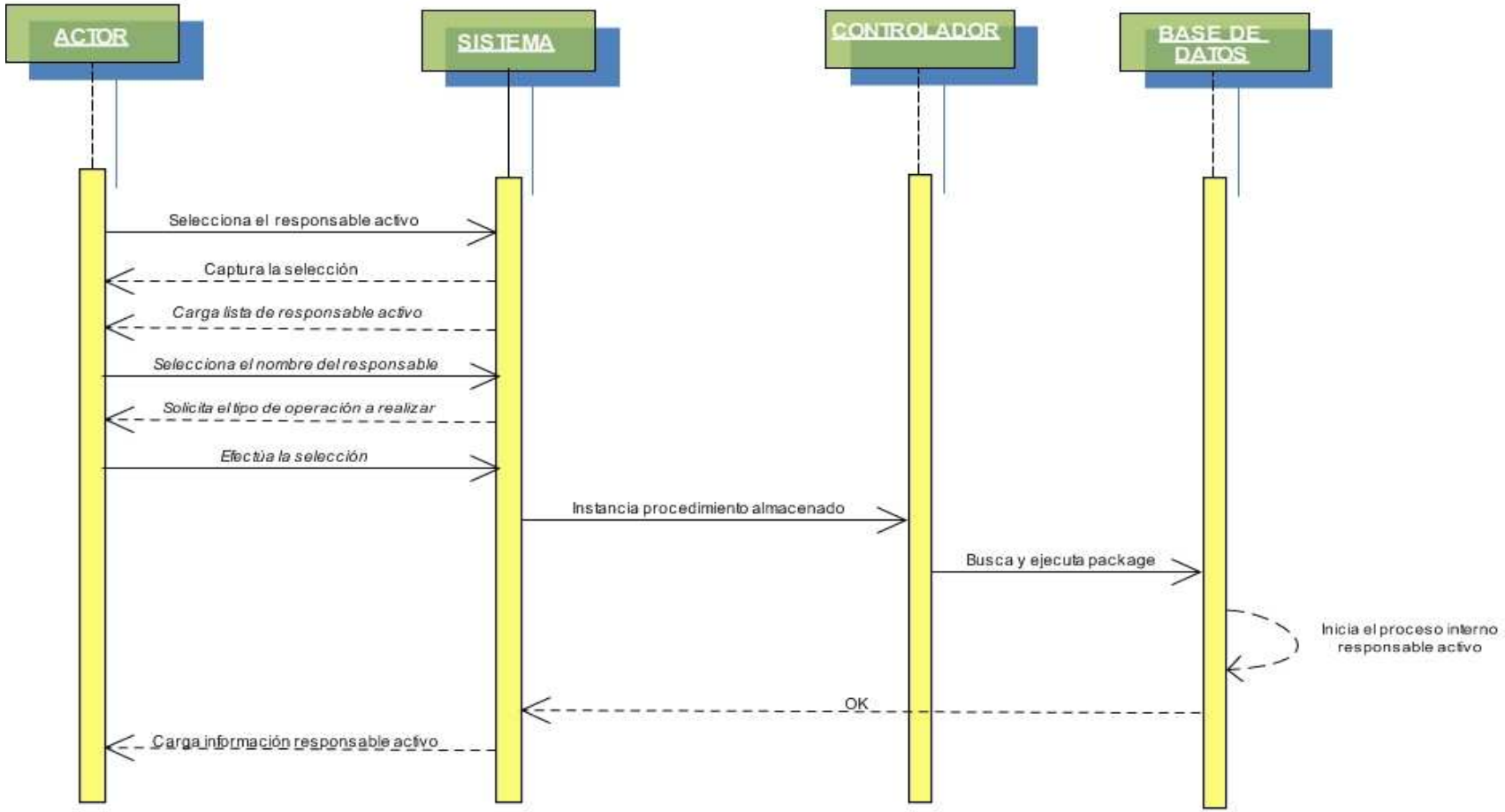


FIGURA 55. DIAGRAMA DE SECUENCIA ADMINISTRACIÓN DE INCIDENTES

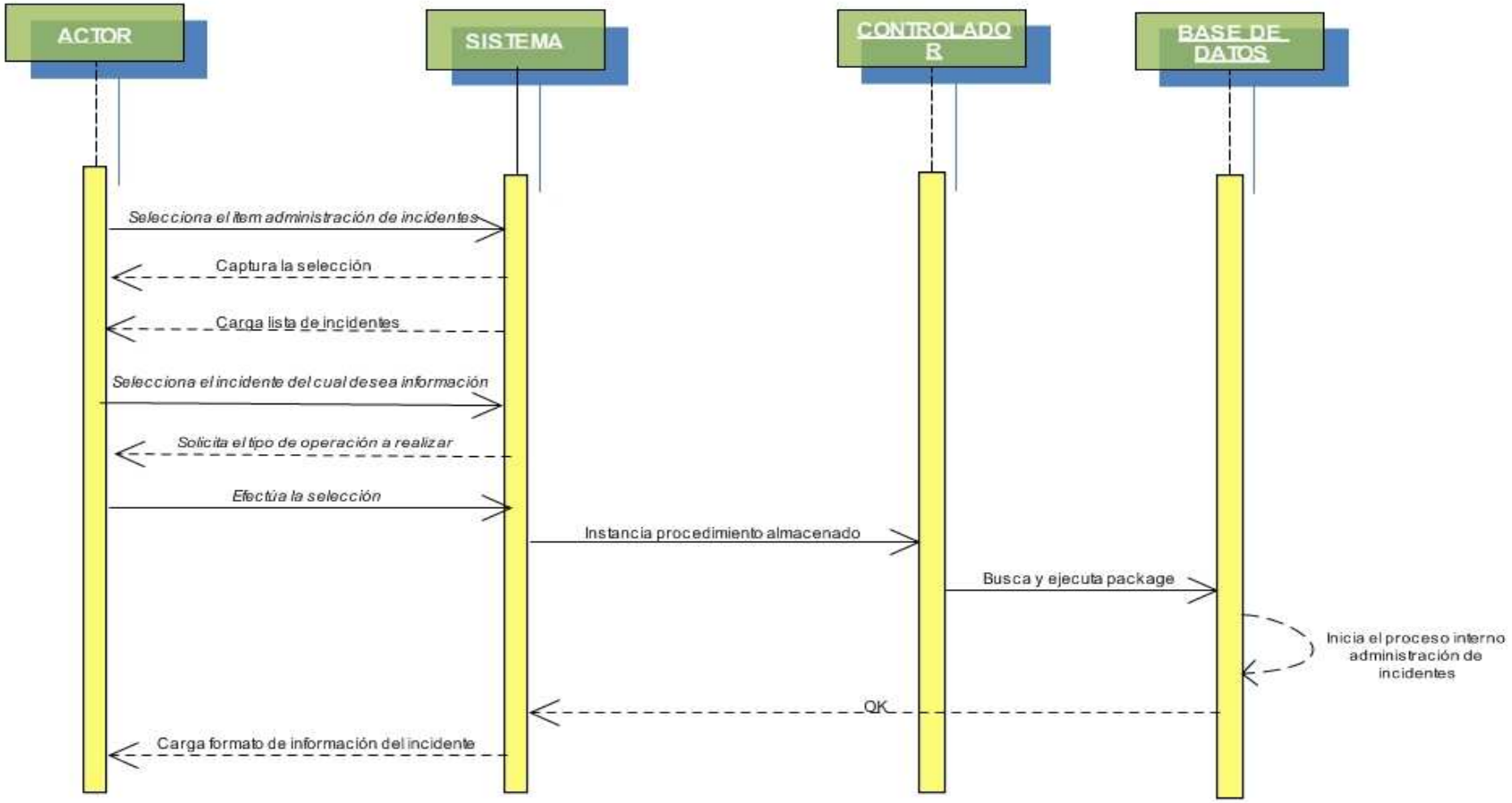
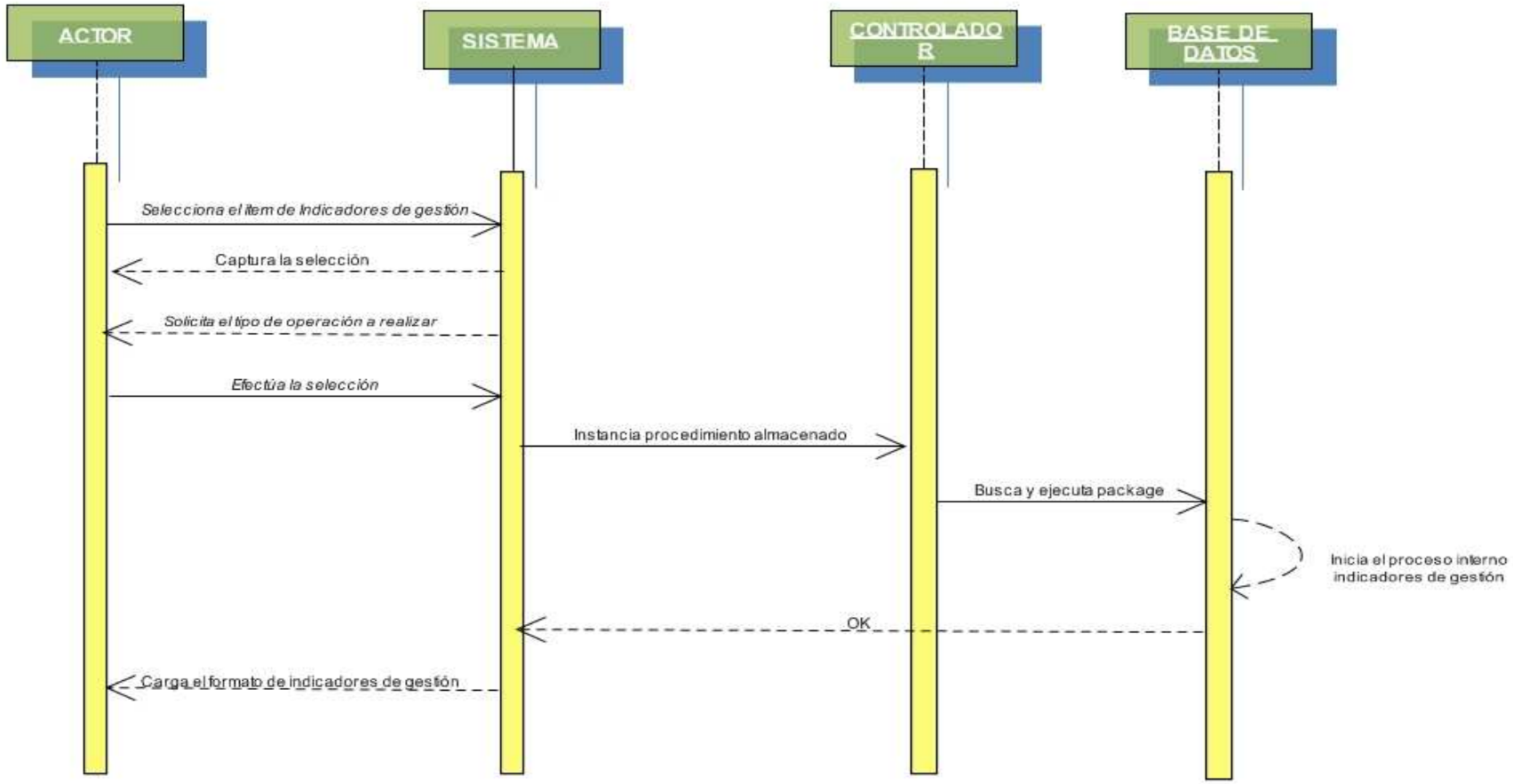


FIGURA 56. DIAGRAMA DE SECUENCIA INDICADORES DE GESTIÓN



- **DIAGRAMAS DE ACTIVIDADES**

FIGURA 57. INFORMACIÓN AMENAZA

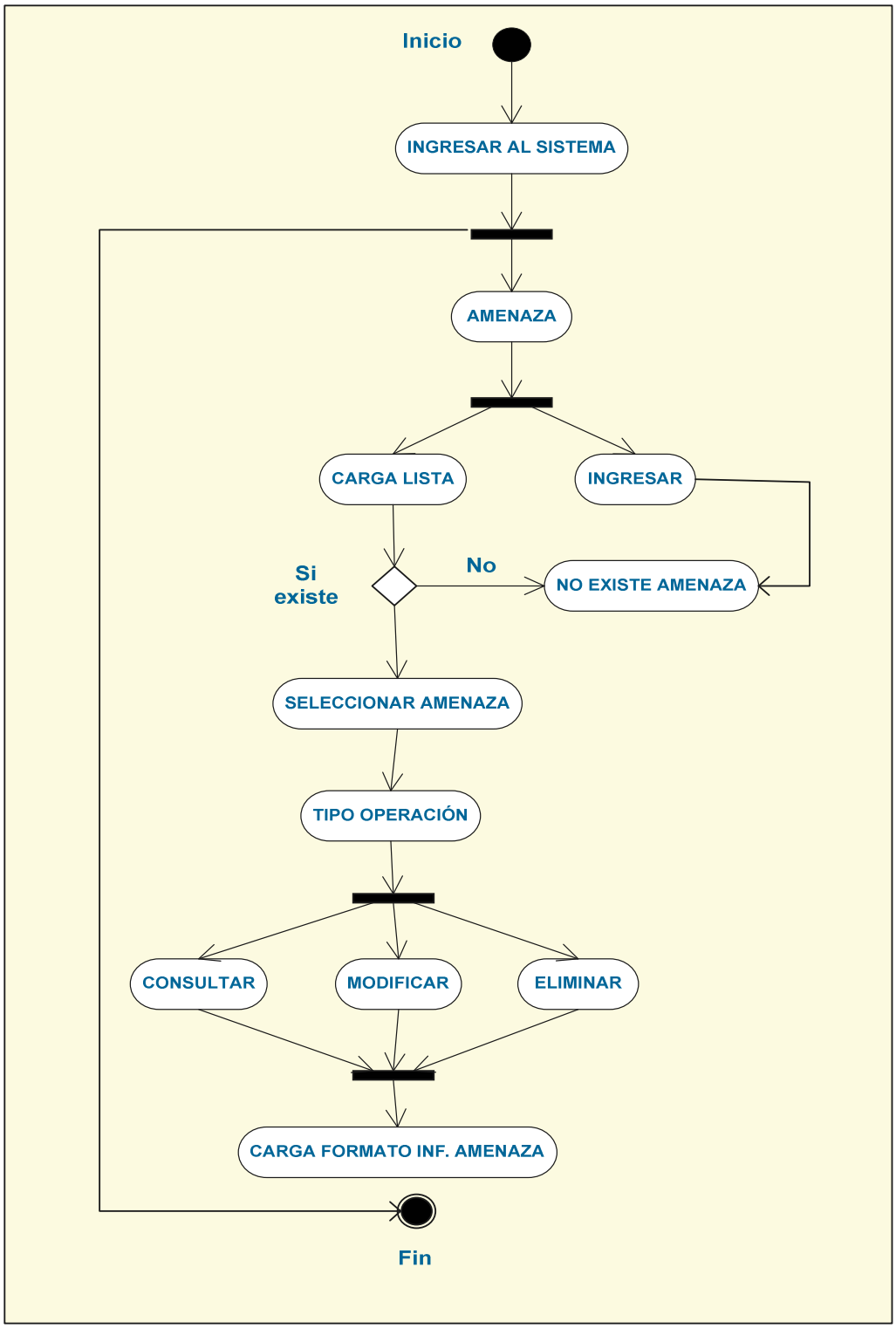


FIGURA 58. INFORMACIÓN CONTROL

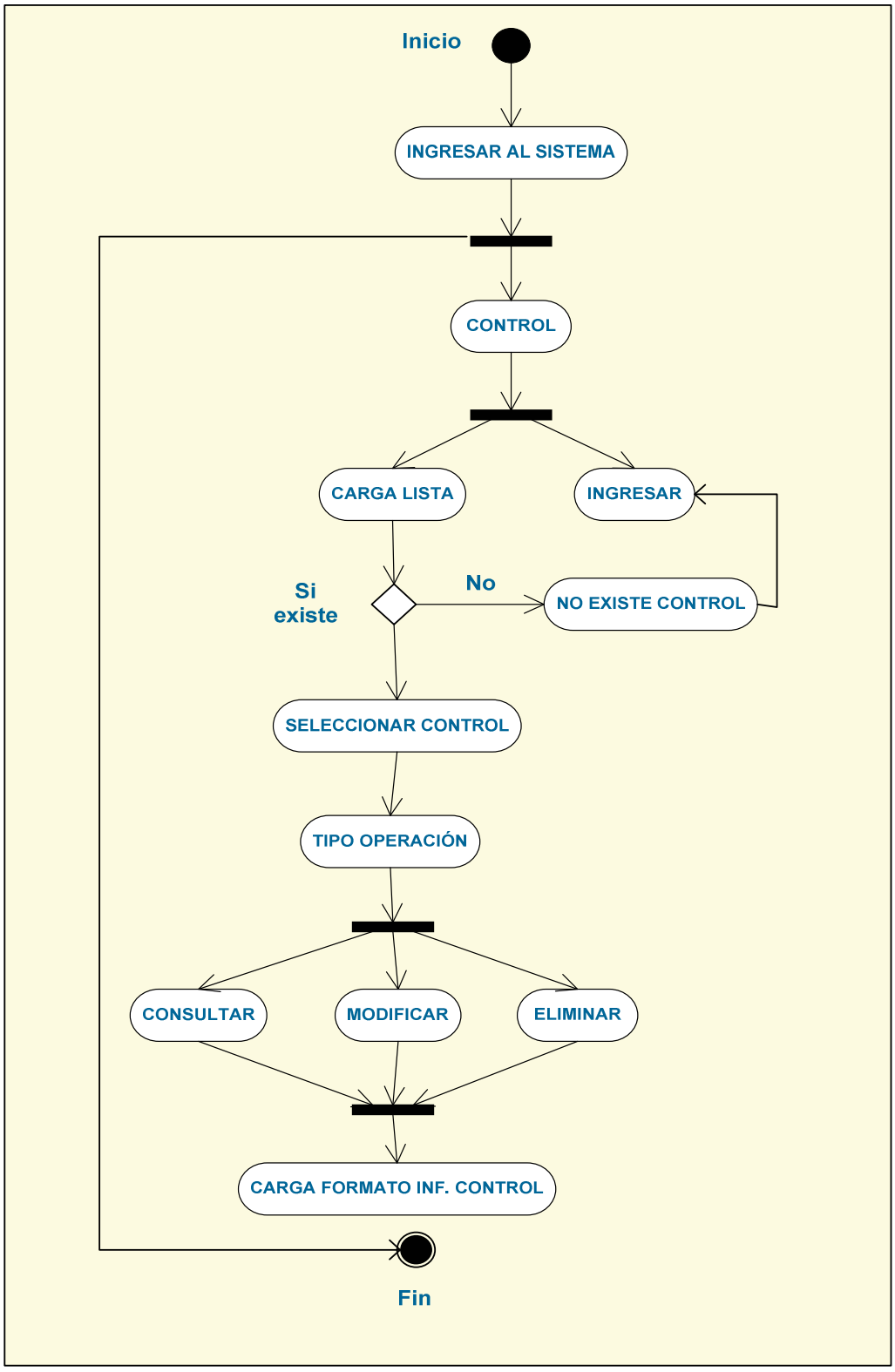
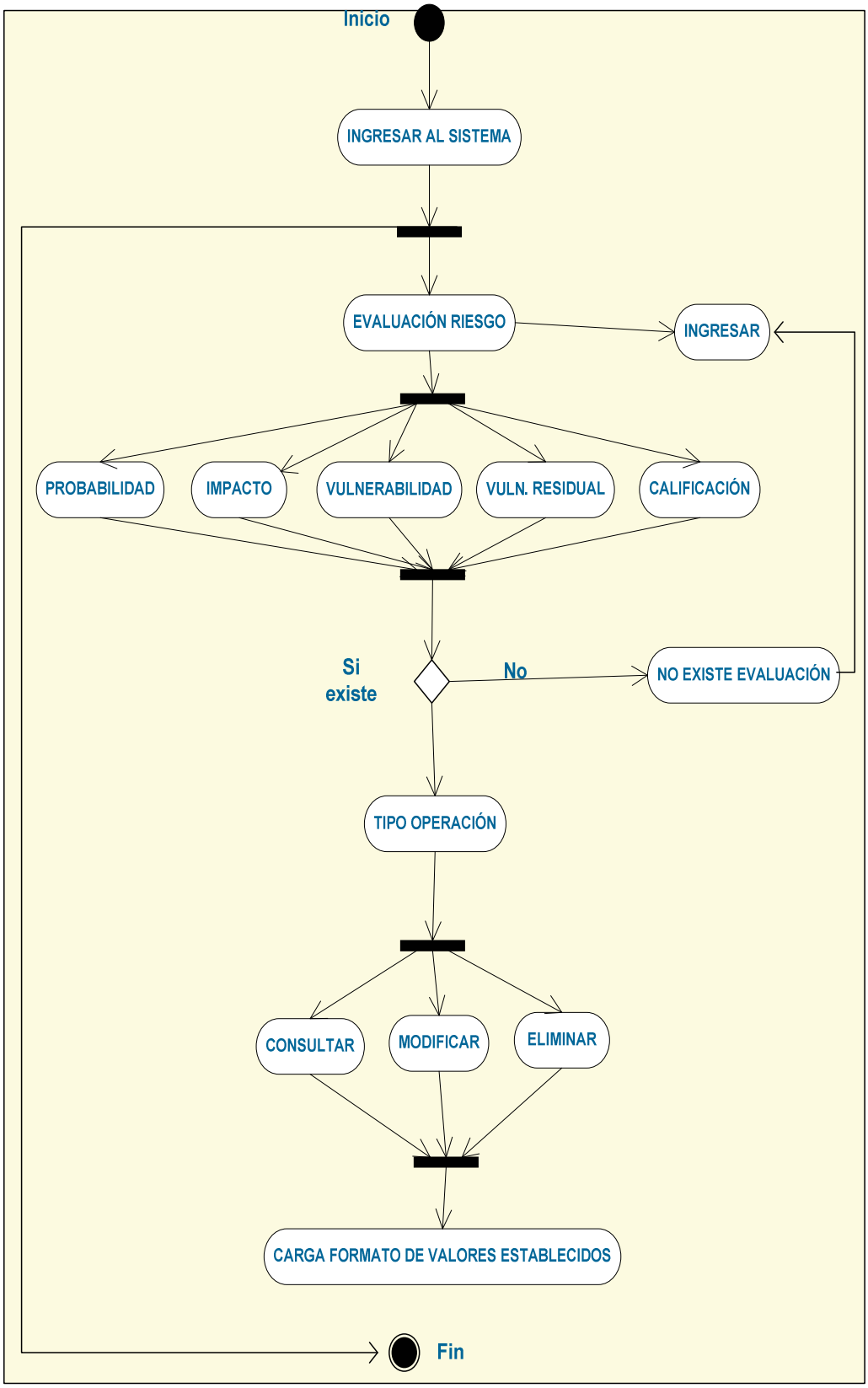


FIGURA 59. EVALUACIÓN DE RIESGO



5.2.4 FASE 4. DE DISEÑO DE OBJETOS

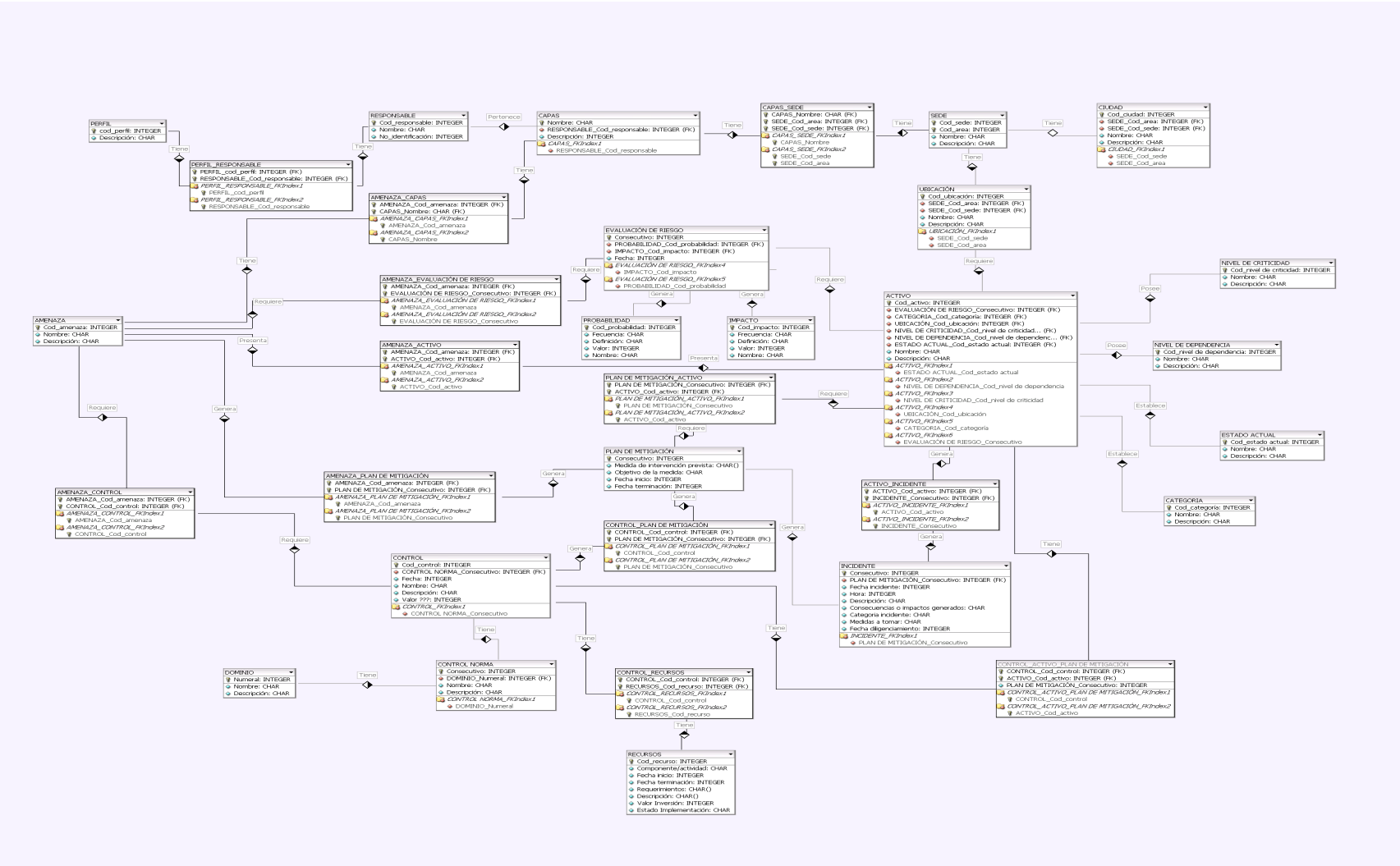
ACTIVIDAD 1. DIAGRAMA ENTIDAD- RELACIÓN

Este modelo fue propuesto a mediados de los años setenta como medio de representación conceptual y global de los problemas, esto con el fin de representar la percepción que se tenga de un sistema de forma general. Físicamente adopta la forma de un gráfico al que se denomina diagrama Entidad-Relación.
Sus elementos fundamentales son las entidades y las relaciones.

Las entidades son representaciones de una cosa, concepto u objeto que es distinguible del mundo real, las entidades están establecidas por uno o más atributos.
Dentro del diagrama entidad- relación existe la entidad fuerte (posee atributos claves) y la entidad débil (no poseen atributos claves propios).

Las relaciones son asociaciones, relaciones o vínculos entre diferentes entidades y describen el vínculo entre las mismas.

FIGURA 60. DIAGRAMA ENTIDAD- RELACIÓN



ACTIVIDAD 2. BASE DE DATOS EN ORACLE

Haciendo uso de todas las especificaciones que surgen a raíz de la definición detallada del diagrama entidad- relación, se establece un sistema de gestión de base de datos que soportará el aplicativo, se crean tablas definidas por atributos y estas a su vez administradas por medio de procedimientos almacenados (package) que estarán comunicados con el código del sistema y permiten la reutilización de código.

FIGURA 61. INTERFAZ ÁRBOL DE TABLAS

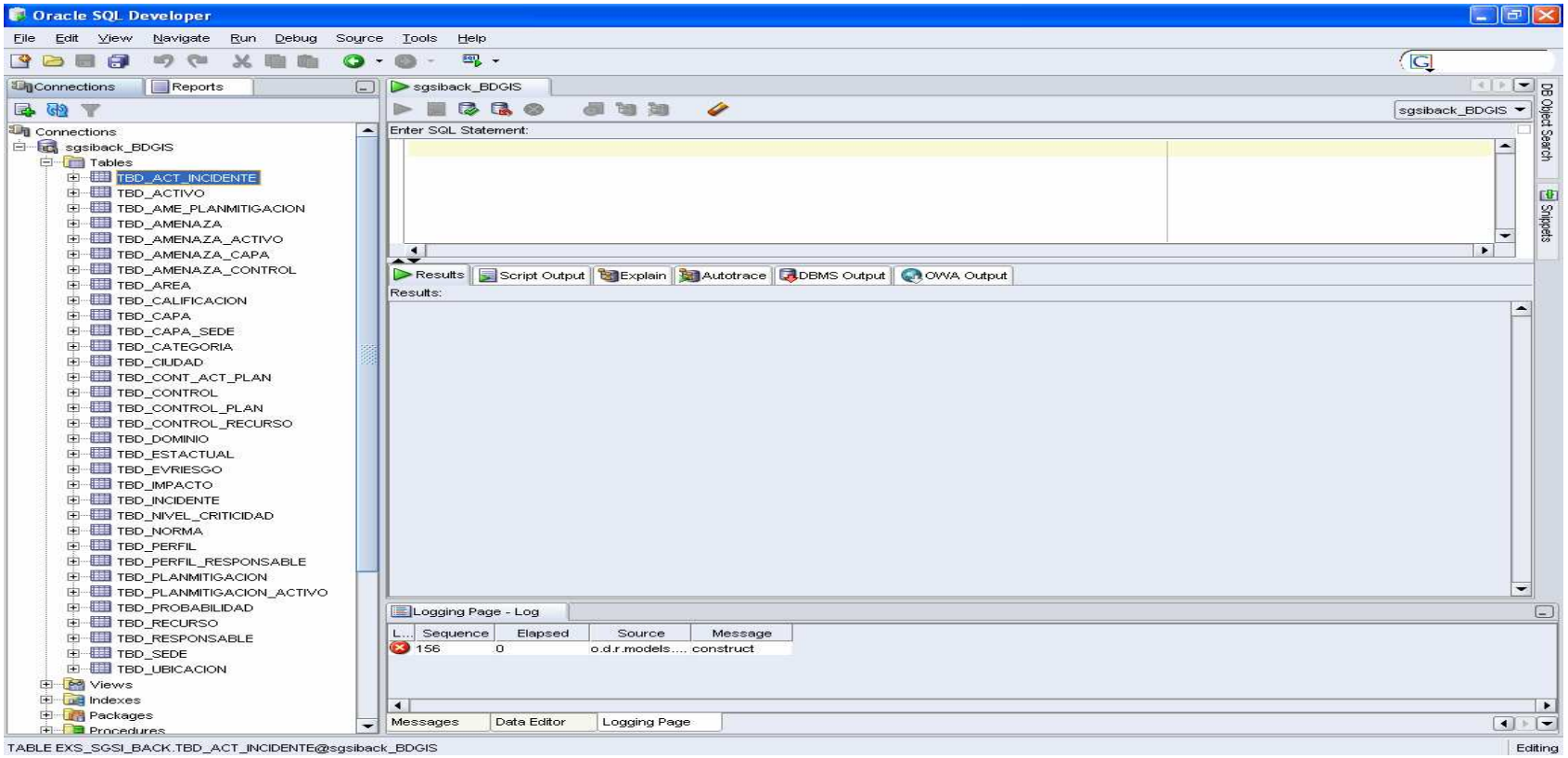


FIGURA 62. PACKAGE ESTABLECIDOS PARA SGSI

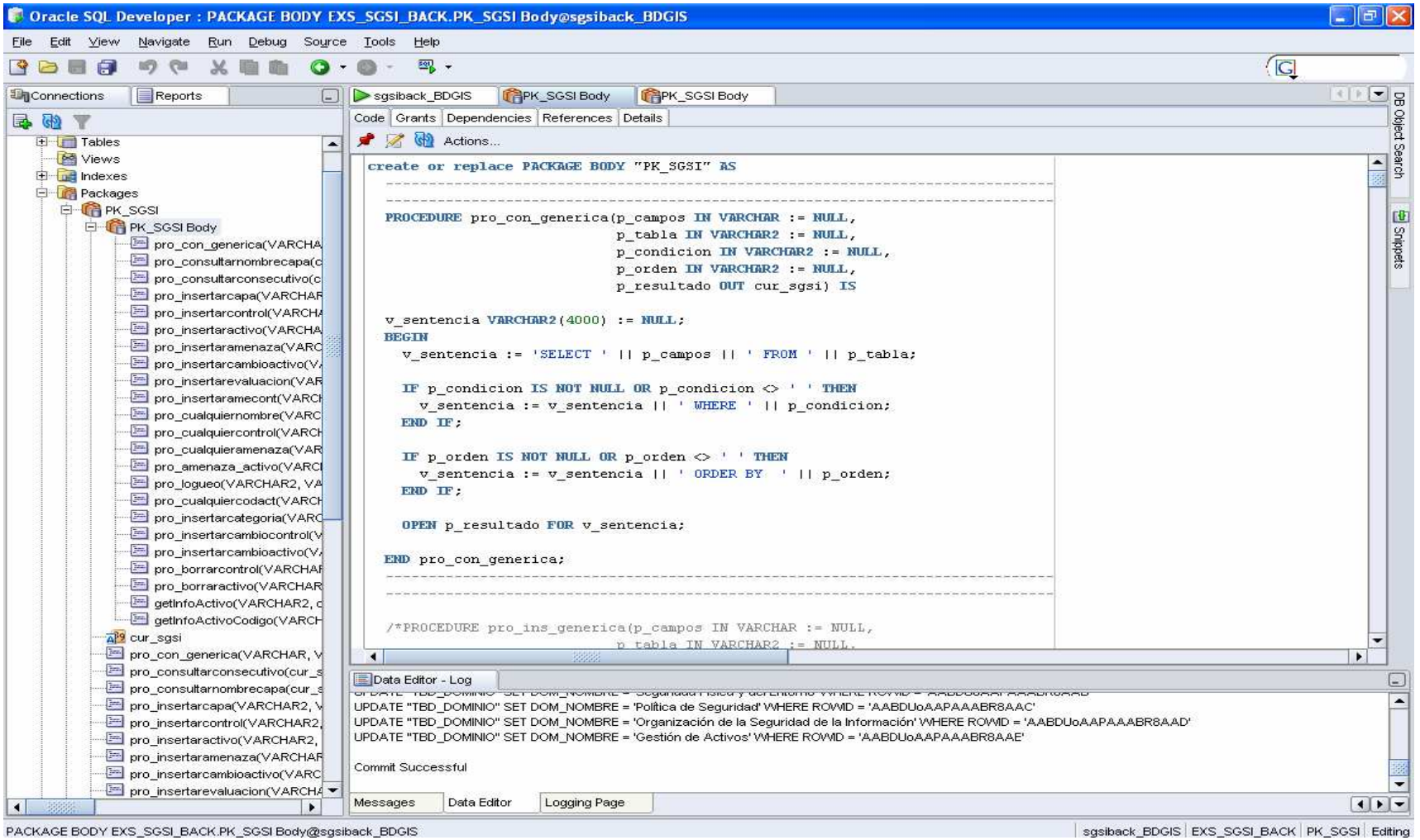


FIGURA 63. DEFINICION DE ESQUEMA/ATRIBUTOS EN UNA TABLA (TABLA ACTIVO)

Se encuentran definidos como datos principales el nombre de la columna, su tipo, si es un dato que permite nulos y si es llave primaria de la tabla.

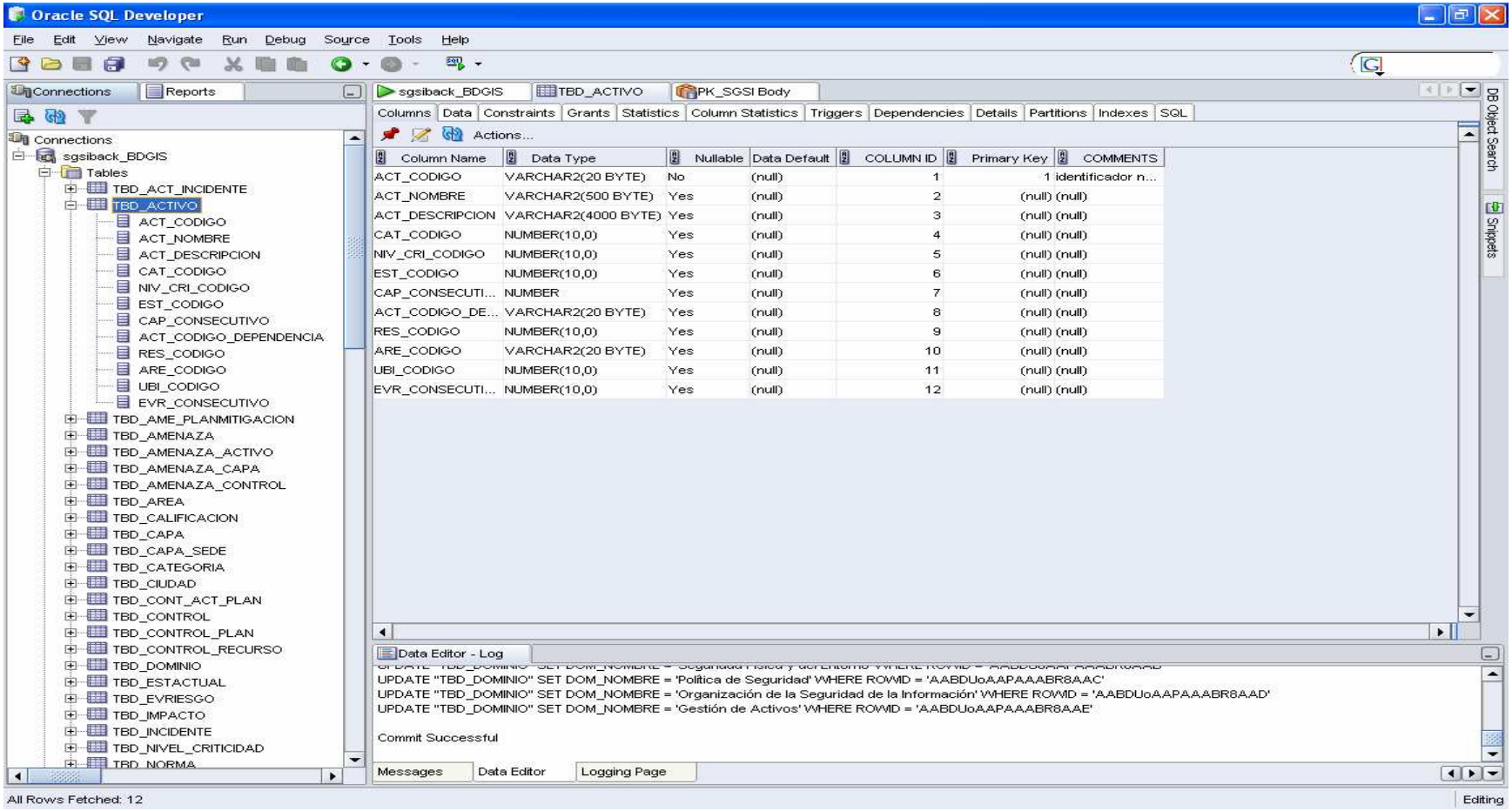
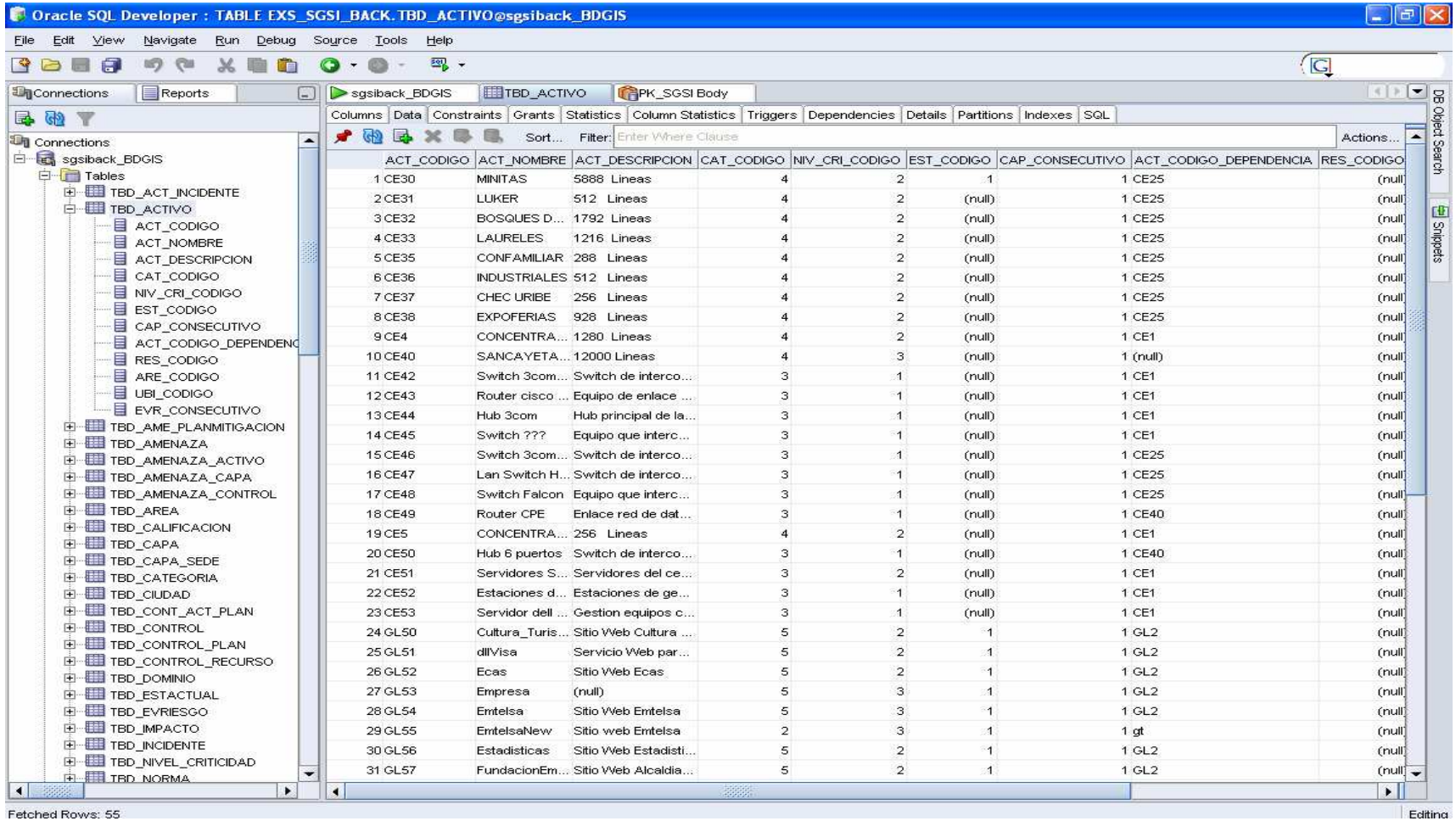


FIGURA 64. VISTA DE DATOS AL INTERIOR DE UNA TABLA (TABLA ACTIVO)

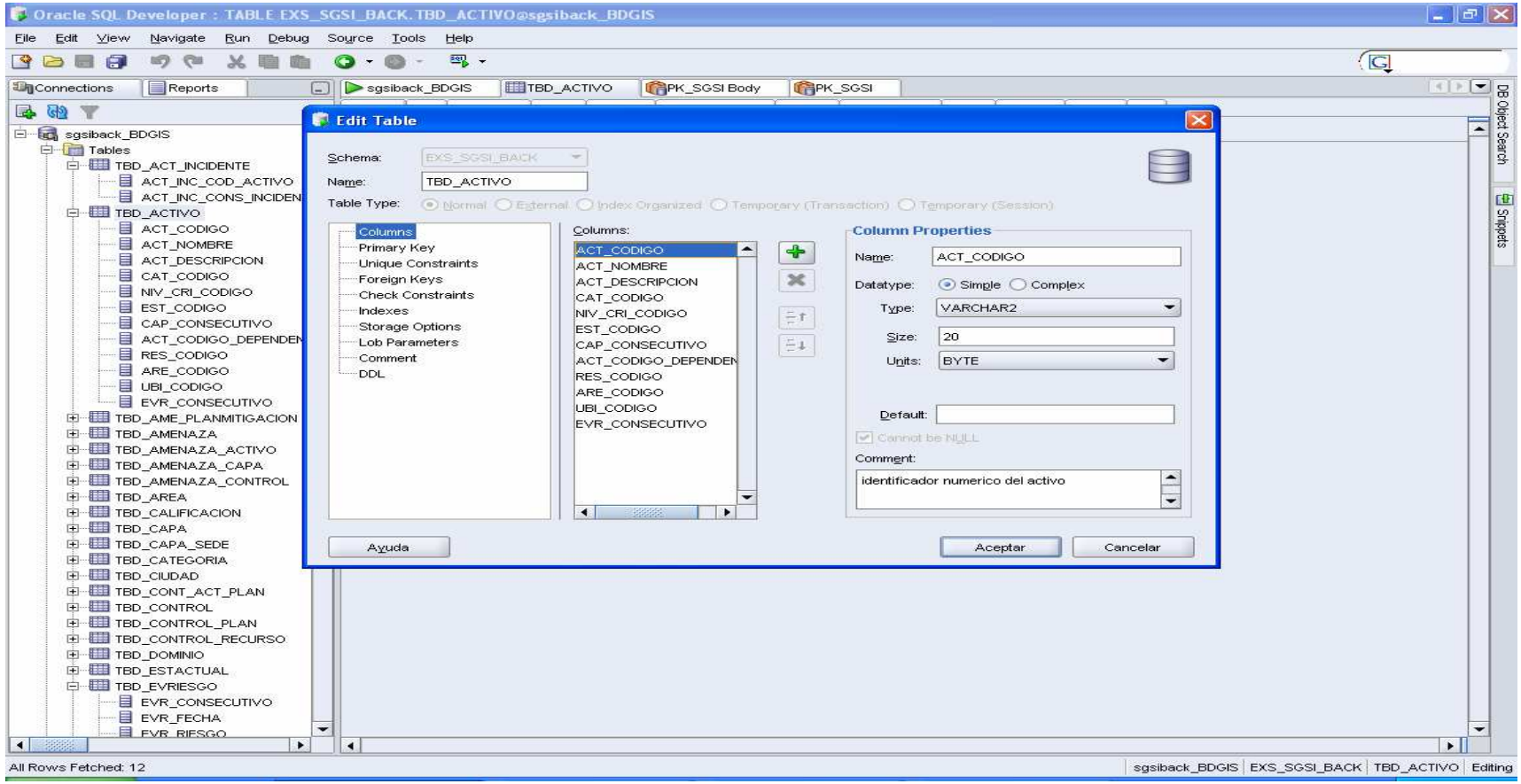
Listado de datos que se encuentran disponibles en el sistema organizados específicamente de la forma establecida por el diagrama entidad- relación



	ACT_CODIGO	ACT_NOMBRE	ACT_DESCRIPCION	CAT_CODIGO	NIV_CRI_CODIGO	EST_CODIGO	CAP_CONSECUTIVO	ACT_CODIGO_DEPENDENCIA	RES_CODIGO
1	CE30	MINITAS	5888 Lineas	4	2	1	1	CE25	(null
2	CE31	LUKER	512 Lineas	4	2	(null)	1	CE25	(null
3	CE32	BOSQUES D...	1792 Lineas	4	2	(null)	1	CE25	(null
4	CE33	LAURELES	1216 Lineas	4	2	(null)	1	CE25	(null
5	CE35	CONFAMILIAR	288 Lineas	4	2	(null)	1	CE25	(null
6	CE36	INDUSTRIALES	512 Lineas	4	2	(null)	1	CE25	(null
7	CE37	CHEC URIBE	256 Lineas	4	2	(null)	1	CE25	(null
8	CE38	EXPOFERIAS	928 Lineas	4	2	(null)	1	CE25	(null
9	CE4	CONCENTRA...	1280 Lineas	4	2	(null)	1	CE1	(null
10	CE40	SANCAYETA...	12000 Lineas	4	3	(null)	1	(null)	(null
11	CE42	Switch 3com...	Switch de interco...	3	1	(null)	1	CE1	(null
12	CE43	Router cisco ...	Equipo de enlace ...	3	1	(null)	1	CE1	(null
13	CE44	Hub 3com	Hub principal de la...	3	1	(null)	1	CE1	(null
14	CE45	Switch ???	Equipo que interc...	3	1	(null)	1	CE1	(null
15	CE46	Switch 3com...	Switch de interco...	3	1	(null)	1	CE25	(null
16	CE47	Lan Switch H...	Switch de interco...	3	1	(null)	1	CE25	(null
17	CE48	Switch Falcon	Equipo que interc...	3	1	(null)	1	CE25	(null
18	CE49	Router CPE	Enlace red de dat...	3	1	(null)	1	CE40	(null
19	CE5	CONCENTRA...	256 Lineas	4	2	(null)	1	CE1	(null
20	CE50	Hub 6 puertos	Switch de interco...	3	1	(null)	1	CE40	(null
21	CE51	Servidores S...	Servidores del ce...	3	2	(null)	1	CE1	(null
22	CE52	Estaciones d...	Estaciones de ge...	3	1	(null)	1	CE1	(null
23	CE53	Servidor dell ...	Gestion equipos c...	3	1	(null)	1	CE1	(null
24	GL50	Cultura_Turis...	Sitio Web Cultura ...	5	2	1	1	GL2	(null
25	GL51	dllVisa	Servicio Web par...	5	2	1	1	GL2	(null
26	GL52	Ecas	Sitio Web Ecas	5	2	1	1	GL2	(null
27	GL53	Empresa	(null)	5	3	1	1	GL2	(null
28	GL54	Emtelsa	Sitio Web Emtelsa	5	3	1	1	GL2	(null
29	GL55	EmtelsaNew	Sitio web Emtelsa	2	3	1	1	gt	(null
30	GL56	Estadisticas	Sitio Web Estadisti...	5	2	1	1	GL2	(null
31	GL57	FundacionEm...	Sitio Web Alcaldia...	5	2	1	1	GL2	(null

FIGURA 65. EDICION DE UNA TABLA (TABLA ACTIVO)

Permite hacer cambios en los atributos de la tabla como el nombre, tipo, hacer comentarios de importancia etc.



6. RESULTADOS

Aunque el capítulo previamente desarrollado describe la aplicación SGSI, resultado principal del presente proyecto, es importante destacar puntualmente los resultados obtenidos.

Teniendo en cuenta todos los parámetros establecidos desde un principio sobre el proyecto y siguiendo los lineamientos que propone la ISO 27001 se implementó un modelo de control tecnológico, que garantiza el óptimo cumplimiento de los objetivos empresariales dentro de una adecuada relación costo- beneficio con una seguridad razonable, esto permite garantizar tanto al negocio como a sus clientes la confidencialidad, integridad y disponibilidad de la información que constituye a EMTELSA S.A E.S.P. como empresa y que es el motor vital por el cual está fundamentado el manejo y control de la misma.

El correcto funcionamiento del aplicativo bajo la norma fortalece las auditorias venideras y prepara a la empresa para enfrentar adecuadamente los cambios futuros ofreciendo como valor agregado a todos los negocios de la organización un adecuado nivel de seguridad de la información

Una vez determinados los activos tecnológicos, las amenazas por cada uno de los activos, los controles existentes y la calificación del riesgo, se tiene una certeza de cuales son los riesgos que realmente es importante atenuar; ya detectada la enfermedad y categorizada, se debe actuar de forma inmediata para mitigarla y reducir el impacto que podría representar para la organización; por medio del aplicativo y una correcta administración de éste se consolida un plan con actividades concretas, con el objetivo de poder actuar sobre los riesgos, definiendo medidas preventivas, detectivas y correctivas y de esta forma llevar las amenazas que actúan sobre los activos tecnológicos a un nivel aceptable del riesgo evitando así daños en los activos lo cual se vería representado en pérdida de dinero y tiempo para la organización.

7. CONCLUSIÓN

Como experiencia el desarrollar un sistema de SGSI aporta bastantes conocimientos no solo de la norma ISO/IEC 27001 sino de la forma correcta en que ésta se debe poner en funcionamiento para lograr resultados óptimos, además la implantación de un desarrollo global como éste que abarca todos los procesos de la empresa, permite enfocar conocimientos en todas las áreas de una organización y entender de forma estratégica el orden actual de la misma, lo cual amplia el enfoque inicial del proyecto y lo hace lucir más como un proceso de negocio, de inversión interno en la organización ya que de esta forma se hace visible sistemáticamente la certeza de destinar recursos al punto neurálgico de quiebre que es necesario atacar.

No se debe olvidar que para desarrollar con éxito esta norma en cualquier empresa es necesario enfrentarse primero al análisis diseño e implantación que difiere notablemente en todas las empresas dependiendo de sus definiciones internas de seguridad, estándares de procesos que posiblemente nunca se habían evaluado y en los cuales todos los interesados deben aportar y aprobar para poder homogenizar el proceso global de seguridad de la empresa.

Un proceso de este tipo en cualquier negocio es un proyecto que apunta directamente a mejorar la seguridad y cuanto mayores sean las exigencias de seguridad con mucha más facilidad será posible alcanzar niveles precisos de capacidad, cumplimiento de leyes y normas de seguridad específicas que permitirán a futuro certificaciones de calidad en la correcta normalización de técnicas de seguridad.

8. RECOMENDACIONES

Actualmente la Información hace parte de los activos más importantes que posee cualquier empresa y es deber de esta mantenerla a salvo, es decir, protegerla de cualquier forma de acceso, uso, divulgación, modificación o destrucción no autorizada, por lo tanto es necesario invertir en recursos de seguridad que permitan garantizar el correcto funcionamiento de los activos de una empresa teniendo en cuenta que a futuro la inversión que será hecha en tiempo y recursos será notablemente incrementada enfocando globalmente la gestión de la seguridad y creando conciencia en todos los miembros de la empresa de la importancia del proceso.

Es probable que se vea incrementada la rentabilidad de la empresa ya que al implantar esta norma se está enfocando directamente en la búsqueda soluciones a los problemas graves que pueden generar pérdidas; igualmente la implantación del proceso mejorara notablemente la seguridad de la empresa frente a amenazas o fallos ya que permite activar controles que implementados correctamente reducen el riesgo al que puede estar expuesta la empresa y esto a nivel general le imprime al negocio imagen de confianza y tranquilidad para sus clientes.

Una vez el aplicativo se encuentre implantado y totalmente funcional, el paso a seguir es la obtención de la certificación ISO/IEC 27001, la cual cerraría el primer ciclo en la entidad.

BIBLIOGRAFÍA

CALDER, Alan. Nueve Claves Para el Éxito. Una visión General de la Implementación de la Norma NTC –ISO/IEC 27001. IT Goverment Publishing. Londres. 2005. 61 p.

CIBSI05. Hacia una Implementación Exitosa de un SGSI. [En Línea]. Chile. 2005. Disponible en: http://cibsi05.inf.utfsm.cl/presentaciones/sesion11/HaciaUnaImplementacionExitosaDeUnSGSI.pdf

EMTELSA S.A. E.S.P. Documentación Interna. Colombia. 2007

FIRMA-E. Guía para la Elaboración del Marco Normativo de un Sistema de Gestión de Seguridad de la Información (SGSI). [En Línea]. España. 2007. Disponible en: http://www.firma-e.com/documentos/Gu%EDa%20para%20la%20elaboraci%F3n%20del%20marco%20normativo-Creative%20common.pdf

ISO27000. Sistema de Gestión de la Seguridad de la Información. [En Línea]. España. 2005. Inicio>Portada Disponible en: http://www.iso27000.es

NEXTEL. S.A. Certificación de la Calidad de la Información. [En Línea]. España. 2008. Inicio>Empresa>Seguridad de la Información. Disponible en: http://www.nextel.es/anw/web/cas/empresa/seguridad/index.jsp

OZSU, Tamer. Principles of distributed database systems. Prentice Hall. New Jersey. 1991. 562 p.

SIGEA. Que es SIGEA. [En línea]. España, 2007. Inicio>Empresa. Disponible en: http://www.sigea.es/index.php

START-UP. Normas en Sistema de Gestión de Seguridad de la Información. [En Línea]. Oviedo (Asturias), España. 2007. Inicio>Portada. Disponible en: http://www.seguridadinformacion.com/seguinfo.php

ANEXO A

MANUAL DE USUARIO

COTENIDO

Pág.

Para ingresar al sistema, el usuario (empleado de EMTELSA asociado a un perfil) carga el aplicativo desde la Intranet de la empresa. Se carga la interfaz de inicio al sistema, allí el empleado debe diligenciar los campos Nombre de Usuario y Contraseña y a continuación oprime el botón Ingresar, que le permitirá acceder a la información.

FIGURA A1. INICIO DE SESIÓN

Si los datos de ingreso son correctos, el sistema despliega el formulario que contiene el menú principal del SGSI, el cual permitirá al usuario seleccionar opciones como: Activo, Amenaza, Control, Evaluación de riesgo, plan de Mitigación, administración de incidentes, informes.

FIGURA A2. INTERFAZ MENÚ PRINCIPAL

ACTIVO
Al seleccionar la opción del menú principal ACTIVO, este despliega un submenú que contiene 2 opciones: El usuario puede seleccionar Ingresar Activo o Actualizar Activo según sea su interés.

- **INGRESAR ACTIVO**

Al seleccionar la opción Ingresar Activo, el sistema despliega el formulario de Ingreso de Activo y pone a disposición del usuario los campos que debe diligenciar con el fin de ingresar un nuevo activo en el sistema.

FIGURA A3. DESPLIEGUE SUBMENÚ ACTIVO (INGRESAR ACTIVO)

El usuario deberá diligenciar los campos:
Nombre (Nombre del activo a ingresar), Código (Identificación única del nuevo activo), Descripción (Especificación en detalle del activo).

FIGURA A4. INTERFAZ FORMULARIO INGRESAR ACTIVO

CAPA

El usuario desplegara un DropDownList que le permitirá elegir la capa a la cual se encontrara asociado el activo[5]

FIGURA A5. SELECCIÓN CAPA

[5] La definición específica de cada una de las capas de la empresa, se encuentra en la pág. XX

DOMINIO

El usuario podrá elegir el ámbito bajo el cual se encuentra el activo a ingresar, este puede ser:

- Gestión de activos
- Organización de la Seguridad de la Información
- Política de Seguridad
- Seguridad Física y del Entorno
- Seguridad de los Recursos Humanos

FIGURA A6. SELECCIÓN DOMINIO

ESTADO ACTUAL

El usuario deberá elegir el estado actual del activo, este puede ser:

- Permanente: Activo que es manejado continuamente
- Rotatorio: El manejo de este activo alterna constantemente
- En producción: Activo que es usado actualmente
- Fuera de Producción: Activo que ha sido retirado y no esta en uso
- De Terceros: Activo que pertenece a otros

FIGURA A7. SELECCIÓN ESTADO ACTUAL

CATEGORIA

El usuario debe elegir la categoría en la cual quedara seleccionado el activo, estas pueden ser:

- Personas: Todas los perfiles de personas que tengan que ver con la capa o dominio y que en un momento dado pueda estar expuesta a alguna amenaza.
- Datos: Todos los datos considerados críticos dentro de la capa o dominio.
- Tecnología: Toda la tecnología informática y de comunicaciones de la capa o dominio que puede llegar a estar expuesta a alguna amenaza.
- Aplicaciones: Todos aquellos sistemas de información manuales o automáticos que son considerados críticos en el negocio.
- Instalaciones: recursos que albergan otros recursos tecnológicos.

FIGURA A8. SELECCIÓN CATEGORÍA

NIVEL DE CRITICIDAD

Cada uno de estos activos, deberá tener una calificación del nivel de criticidad en la empresa, el usuario elegirá Dicho nivel de criticidad y este tendrá tres escalas a saber:

- Muy Critico
- Critico
- Normal[6]

FIGURA A9. SELECCIÓN NIVEL DE CRITICIDAD

[6] La definición específica de cada uno de los niveles de criticidad de la empresa, se encuentra en la pág. 30

UBICACIÓN

La ubicación física del activo esta limitada en 3 aspectos: Ciudad, Sede, Piso.
El usuario elegirá la ciudad en la cual se encuentra el activo.

FIGURA A10. SELECCIÓN UBICACIÓN

Al momento de elegir la ciudad, por ejemplo Buga (como se muestra a continuación), el sistema automáticamente le mostrara al usuario las sedes que se encuentran en esta ciudad y le permitirá escoger una de ellas, al igual que los pisos con los que esta cuenta, permitiéndole también escoger el piso donde se encuentra el activo.

FIGURA A11. SELECCIÓN SEDE Y PISO

NIVEL DE DEPENDENCIA

Le permite al usuario definir el activo del cual depende este nuevo activo que esta ingresando, es decir, define el "activo padre" y el "activo hijo" dentro del sistema

El sistema autoriza al usuario hacer una búsqueda por nombre o código de este "activo padre" o simplemente seleccionarlo de una lista de activos ya ingresados en el sistema.

FIGURA A12. SELECCIÓN NIVEL DE DEPENDENCIA

RESPONSABLE

Le permite al usuario definir el encargado del activo que desea ingresar

El sistema autoriza al usuario hacer una búsqueda por nombre o código de los empleados que tengan activos a su cargo o simplemente seleccionarlo de una lista de responsables ya existentes.

FIGURA A13. SELECCIÓN RESPONSABLE

De esta forma debe lucir un formulario del ingreso de un activo completa y correctamente diligenciado, ahora el usuario deberá seleccionar la opción Ingresar Activo con el fin de finalizar el ingreso.

FIGURA A14. FORMULARIO INGRESO ACTIVO COMPLETAMENTE DILIGENCIADO

A continuación el sistema presentará al usuario un mensaje que le notificara el éxito o fracaso de su ingreso según el diligenciamiento del formulario.
Posteriormente el usuario seleccionará el ítem Aceptar y el Sistema lo ubicara de nuevo en el menú principal del SGSI.

FIGURA A15. CONFIRMACIÓN INGRESO ACTIVO

- **ACTUALIZAR ACTIVO**

FIGURA A16. DESPLIEGUE SUBMENÚ ACTIVO (ACTUALIZAR ACTIVO)

A continuación el sistema le dará la posibilidad al usuario de buscar por código o nombre el activo al cual se le harán algunas modificaciones o el activo que desea borrar definitivamente del sistema, una vez seleccionado el activo el sistema carga los datos del mismo con el fin de permitir al usuario visualizar sus cambios y permitiendo editar los campos que sean necesarios o borrar el activo específico.

FIGURA A17. INTERFAZ FORMULARIO ACTUALIZAR ACTIVO

EDITAR ACTIVO

A continuación el usuario selecciona el ítem Editar Activo y el sistema muestra un mensaje que le confirma al usuario el éxito o fracaso de la operación realizada.

FIGURA A18. MENSAJE DE CONFIRMACIÓN MODIFICACIÓN DE ACTIVO

BORRAR ACTIVO

A continuación el usuario selecciona el ítem Borrar Activo y el sistema muestra un mensaje que le confirma al usuario el éxito o fracaso de la operación realizada.

FIGURA A19. MENSAJE CONFIRMACIÓN BORRADO DE ACTIVO

FIGURA A20. DESPLIEGUE SUBMENÚ AMENAZA (INSERTAR/ACTUALIZAR AMENAZA)

Le permite al usuario ingresar una nueva amenaza en el sistema, ingresando el código, nombre y descripción únicos de la nueva amenaza, al oprimir ingresar, el sistema muestra un mensaje de confirmación de ingreso de activo
También le permite buscar el activo que desea editar o borrar, al oprimir editar o borrar, el sistema muestra un mensaje que manifiesta el éxito o fracaso de la operación

FIGURA A21. INTERFAZ FORMULARIO INGRESO/ACTUALIZACIÓN AMENAZA

FIGURA A22. DESPLIEGUE SUBMEÚ CONTROL (INGRESAR/ACTUALIZAR CONTROL)

Le permite al usuario ingresar un nuevo control en el sistema, ingresando el nombre, código, descripción y numeral de la norma, únicos del nuevo control.

FIGURA A23. INTERFAZ FORMULARIO INGRESO/ACTUALIZACIÓN CONTROL

INGRESAR CONTROL

A continuación el usuario selecciona el ítem Ingresar Control y el sistema muestra un mensaje que le confirma al usuario el éxito o fracaso de la operación realizada.

FIGURA A24. MENSAJE CONFIRMACIÓN INGRESO CONTROL

EDITAR CONTROL

A continuación el usuario buscar el control que desea editar, una vez ubicado cambia los datos que considere necesarios y selecciona el ítem Editar Control

FIGURA A25. EDICIÓN CONTROL

En este punto el sistema muestra un mensaje que le confirma al usuario el éxito o fracaso de la operación realizada

FIGURA A26. MENSAJE MODIFICACIÓN CONTROL

ELIMINAR CONTROL

A continuación el usuario buscar el control que desea editar, una vez ubicado el control que desea borrar definitivamente del sistema selecciona el ítem Borrar Control

FIGURA A27. ELIMINACIÓN CONTROL

En este punto el sistema muestra un mensaje que le confirma al usuario el éxito o fracaso de la operación realizada

FIGURA A28. MENSAJE ELIMINACIÓN CONTROL

Esta figura muestra la búsqueda de un control que ha sido eliminado del sistema, no es posible recuperar el control, si se elimina un control equivocadamente deberá volver a ser ingresado al sistema por medio del formulario de ingreso de activos

FIGURA A29. BUSQUEDA CONTROL ELIMINADO

En este punto el sistema muestra al usuario un mensaje que manifiesta la inexistencia del registro en el sistema

FIGURA A30. MENSAJE BUSQUEDA FALLIDA

FIGURA A31. MENÚ EVALUACIÓN DE RIESGO

Le permite al usuario ingresar una nueva evaluación de riesgo en el sistema para una amenaza que afecta un activo específico, el sistema permite al usuario buscar por código o nombre un activo especifico, después de esto el usuario debe hacer la misma búsqueda pero esta vez de una amenaza específica (con el fin de entablar la relación) y el sistema desplegara los controles que se encuentran asociados a la amenaza.

FIGURA A32. INTERFAZ FORMULARIO EVALUACIÓN DE RIESGO

Con estos datos el usuario selecciona la probabilidad (obtiene su respectiva definición, frecuencia y valor) y el impacto (obtiene su respectiva definición y valor) que considere necesarios y recibe el valor del riesgo, la vulnerabilidad y la vulnerabilidad residual, estos datos le permiten seleccionar la calificación adecuada para ingresar esta evaluación

FIGURA A33. INGRESO EVALUACIÓN

Esta figura muestra la interfaz del formulario del plan de mitigación que se encuentra en construcción

FIGURA A34. INTERFAZ MENÚ PLAN DE MITIGACIÓN

Esta figura muestra la interfaz del formulario de administración de incidentes que se encuentra en construcción

FIGURA A35. INTERFAZ MENÚ ADMINISTRACIÓN DE INCIDENTES

FIGURA A36. DESPLIEGUE SUBMENÚ INFORMES

FIGURA A37. DESPLIEGUE SUBMENÚ INFORMES (INFORMACIÓN ACTIVO)

Permite al usuario hacer una búsqueda por código o nombre de un activo específico

FIGURA A38. INTERFAZ FORMULARIO INFORMACION ACTIVO

Una vez seleccionado el activo requerido, el sistema carga los datos completos y específicos del mismo, esto permite visualizar si el activo ha sido ingresado de forma incompleta (por ej en la siguiente figura falta información de ciudad, sede, responsable, estado y dominio), al igual que tener la información organizada en caso que sea necesario imprimir los datos.

FIGURA A39. INFORMACIÓN COMPLETA DEL ACTIVO

Esta figura muestra la interfaz del formulario de Indicadores de Gestión que se encuentra en construcción

FIGURA A40. INTERFAZ SUBMENÚ INDICADORES DE GESTIÓN

Esta figura muestra la interfaz del formulario de recursos que se encuentra en construcción

FIGURA A41. INTERFAZ SUBMENÚ RECURSOS

ANEXO B
MANUAL TÉCNICO

Las características técnicas que se deben tener en cuenta para operar el sistema son:

CARACTERÍSTICAS EQUIPO USUARIOS:

Hardware:

Procesador 1Gh en adelante
Tarjeta de red
64 en RAM en adelante
Disco duro de 10Gb en adelante
Monitor de 15 pulgadas

Software:

Internet Explorer
Mozilla Firefox
Sistema Operativo Windows.

CARACTERÍSTICAS DE EQUIPO SERVIDOR:

Hardware:

Servidor Web:
Procesador: PentiumIII 800 Mhz
Ram: 2.5GB
S.O.: Windows 2000 Server
Distribución de los Discos Duros:
Raid1, 16Gb, Sistema Operativo
Raid5, 50 Gb, Ejecutables

Software

Sistema gestor de Bases de datos: Oracle
Lenguaje de Desarrollo: Asp.net
Publicador Web: IIS (Internet Information Service)

CARACTERISTICAS BASICAS DE IMPLEMENTACIÓN EN EL SERVIDOR:

Esta aplicación fue diseñada bajo la plataforma .Net, con conexión de Bases de datos a Oracle, esta se hace por medio de Package.

Las aplicaciones ASP .NET y los servicios Web están diseñados para ejecutarse como componentes del servidor, que a menudo se ejecutan en un equipo central en algún lugar de una red local o remota. Para ejecutar estas aplicaciones y servicios, debe asegurarse de que se cumplan todos los requisitos previos.

Para asegurarse de que la aplicación de servidor .NET se ejecuta con un rendimiento adecuado, debe tener en cuenta los siguientes requisitos:

REQUISITOS DEL SERVIDOR PARA IMPLEMENTAR APLICACIONES .NET

Tipo	Requisitos
SISTEMA OPERATIVO ADMITIDO	Microsoft® Windows® 2000 Professional con Service Pack 2.0 Microsoft® Windows® 2000 Server con Service Pack 2.0 Microsoft® Windows® 2000 Advanced Server con Service Pack 2.0 Microsoft® Windows® XP Professional Microsoft® Windows® Server 2003, Web Edition Microsoft® Windows® Server 2003, Standard Edition Microsoft® Windows® .Server 2003, Enterprise Edition
EJECUTANDO ASP.NET	Microsoft IIS 5.0 o posterior (Windows XP Pro incluye la versión 5.1 y Windows .NET incluye la versión 6.0.)
PROCESADOR	El procesador mínimo necesario es Intel Pentium o equivalente a 133 MHz o superior, como requieren las versiones instaladas de Windows. Se recomienda utilizar Pentium III XEON en equipos multiprocesador si se esperan cargas de trabajo elevadas. Dado que los componentes de servidor .NET deben ejecutarse de forma repetida por parte de múltiples usuarios, la potencia de procesamiento debe adecuarse a esta carga de trabajo.
RAM	El mínimo necesario es 128 MB o superior,

	como requieren las versiones instaladas de Windows. Se recomienda disponer del máximo de memoria posible, para beneficiarse de las características avanzadas de almacenamiento en caché de .NET Framework.
ESPACIO DE ALMACENAMIENTO	No hay requisitos especiales acerca del espacio de almacenamiento, más que los requisitos típicos de la versión instalada de Windows y el tamaño de los archivos que componen la aplicación. Para optimizar el acceso al disco y para proporcionar capacidades de tolerancia a errores en el subsistema de almacenamiento, se recomienda utilizar discos SCSI de alta calidad y configuraciones RAID, si es posible. Los sistemas configurados como conjuntos de servidores Web con el servicio de equilibrio de carga de Windows (WLBS) pueden beneficiarse de los sistemas de almacenamiento en la red, como los dispositivos SAN o NAS.
RED	Los requisitos de red se basan en la utilización del ancho de banda y la carga de trabajo esperada. Los requisitos de red serán distintos para los clientes internos y para los clientes remotos. Sin embargo, la administración de estos requisitos se basa en una simple administración de red.

Tabla 45. Requisitos del Servidor para Implementar Aplicaciones .Net

Implementación en el cliente

Las aplicaciones ASP .NET y los servicios Web están diseñados para ejecutarse como componentes del servidor. El dispositivo cliente utiliza una aplicación host, como Internet Explorer, para ejecutar estas aplicaciones .NET, o ejecutará una aplicación .NET para utilizar estos servicios de forma remota. Los servidores que ejecutan los sistemas operativos Windows Server 2003 incluyen

todos los requisitos previos para ejecutar aplicaciones .NET como dispositivos cliente.

En algunos casos, las aplicaciones .NET requerirán la implementación de componentes del cliente, y en tal caso las consideraciones sobre la implementación serán muy parecidas a la implementación de las aplicaciones de servidor .NET.

Determinar los requisitos

Para asegurarse de que la aplicación de servidor .NET se ejecuta en el dispositivo cliente con un rendimiento y una funcionalidad adecuados, debe tener en cuenta los requisitos siguientes que aparecen en la Tabla 3:

REQUISITOS DEL CLIENTE PARA IMPLEMENTAR APLICACIONES .NET

Tipo	Requisitos
SISTEMA OPERATIVO ADMITIDO	Microsoft® Windows® 98 Microsoft® Windows® 98 Second Edition Microsoft® Windows® Millennium Edition Microsoft® Windows NT® 4.0 Workstation con Service Pack 6.0a o posterior Microsoft® Windows NT® 4.0 Server con Service Pack 6.0a o posterior Microsoft® Windows® 2000 Professional Microsoft® Windows® 2000 Server Microsoft® Windows® 2000 Advanced Server Microsoft® Windows® XP Home Edition Microsoft® Windows® XP Professional Microsoft® Windows® Server 2003, Web Edition Microsoft® Windows® Server 2003, Standard

	Edition Microsoft® Windows® .Server 2003, Enterprise Edition
EXPLORADOR DE INTERNET	Microsoft® Internet Explorer 5.01 o posterior
WINDOWS INSTALLER	Microsoft® Windows® Installer 2.0 o posterior
OBTENCIÓN DE ACCESO A LA INFORMACIÓN DE ADMINISTRACIÓN DEL SISTEMA	Windows Management Instrumentation (WMI) (instalado con el sistema operativo en Windows 2000, Windows Millennium Edition, Windows XP y Windows Server 2003)
SERVICIOS COM+	Windows 2000 Service Pack 2.0 o Windows XP o Windows Server 2003
PARA EJECUTAR APLICACIONES ASP .NET	Microsoft IIS 5.0 o posterior (Windows XP Pro incluye la versión 5.1 y Windows .NET incluye la versión 6.0.)
PROCESADOR	El procesador mínimo necesario es Intel Pentium o equivalente a 90 MHz o superior, como requieren las versiones instaladas de Windows. Cuando se ejecutan aplicaciones .NET que necesitan también la ejecución de componentes del cliente, se recomienda utilizar Pentium III/IV a una velocidad mayor que la mínima requerida.
RAM	El mínimo necesario es 32 MB o superior, como requieren las versiones instaladas de Windows. Se recomienda disponer del máximo de memoria posible, para beneficiarse de las características avanzadas de almacenamiento en caché de .NET Framework.
ESPACIO DE ALMACENAMIENTO	No hay requisitos especiales acerca del espacio de almacenamiento, más que los requisitos típicos de la versión instalada de Windows y el tamaño de los archivos que componen la aplicación.
RED	Los requisitos de red se basan en la utilización del ancho de banda esperado.

Tabla 46. Requisitos del Cliente para Implementar Aplicaciones .Net