Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Título

Ázzets: Definición de Sistema de Gestión de Activos de Información

Autor: Juan Alejandro Knight

Tutor: Gustavo Díaz

Cohorte 2010

Contenido

Azzets – Definición de Sistema de Gestión de Activos de Información

Resumen

El presente trabajo está enfocado en capturar los requerimientos, analizar, diseñar y planificar un proyecto para el desarrollo de un sistema web que permita la gestión de activos de información de una organización. La herramienta estará basada en la ISO 27002, en el dominio 7 “Gestión de Activos” [1].

Tomando como fundamento los principios teóricos acerca de la gestión de activos de información, se diseñó y planificó un sistema que permita enumerar a los activos, categorizarlos por departamento, detectar sus interrelaciones, asignar tiempos de respuesta ante un incidente, identificar riesgos, clasificar y priorizar los riesgos, identificar los controles, cuantificar la eficacia de cada control y armar informes de los mapas integrales de riesgos para cada activo.

La gestión integral de los activos permitirá ver la situación actual de cada activo y departamento, la eficacia de los controles actuales, priorizar en qué activos hace falta invertir en nuevos controles, identificar los posibles controles a aplicar y comparar el mapa integral de riesgos entre la situación actual y la planificada.

Palabras claves

Gestión de Activos de Información – Seguridad Informática – Riesgos – Controles – Plan de Recuperación – Mapa Integral de Riesgos

Propuesta

Introducción

La gestión de activos de información permite una visión integral de los riesgos desde el punto de vista de la seguridad informática. Es una plataforma que permite determinar cómo están protegidos cada uno de los activos de información de la organización, qué riesgos amenazan la continuidad operativa y qué controles se están implementando para minimizar la exposición a posibles amenazas.

Los activos de información ayudan a cumplir los objetivos estratégicos. En organizaciones grandes donde existen vastas cantidades de activos de información, se requiere de una metodología para poder gestionar la seguridad de forma exhaustiva y profunda. Los recursos son siempre limitados, ya sea dinero, tiempo, esfuerzo o personal capacitado, por lo que se debe adecuar un plan de acción incremental e iterativo para poder resguardar los activos según su prioridad. Esto permitirá cubrir de forma temprana los activos que más pérdidas podrían causar en la organización en caso de la materialización de un riesgo.

Problema

Los problemas de la seguridad informática en grandes corporaciones incluyen mantener un repositorio centralizado de los activos de información, identificar y clasificar sus riesgos, identificar los controles implementados y realizar un criterio para priorizar su resguardo. Otro escoyo es planificar qué controles se implementarán en un futuro cercano, calculando su costo asociado y cuán efectivos son aminorando los riesgos actuales.

Se debe mantener actualizados los activos, los riesgos y los controles aplicados, además de poder generar informes del estado actual de los riesgos. Un sistema diseñado para este propósito facilitaría enormemente la gestión de la seguridad informática y decisiones más eficaces y eficientes a la hora de resguardar la información.

Objetivos

El objetivo principal es realizar un análisis, diseño y planificación de un proyecto para desarrollar un sistema web que permita realizar un inventario de los activos de información de una empresa, relacionar dichos activos, asignar tiempos de recuperación para un plan de continuidad, clasificarlos, identificar y cuantificar los riesgos inherentes para cada activo, identificar los controles asociados y cuantificar la eficacia de la aplicación de dichos controles.

El producto final será la piedra angular para la ejecución de un proyecto de desarrollo de dicho sistema. La herramienta está basada en la ISO 27002, en el dominio 7 “Gestión de Activos” [1]. Éste estándar ofrece un compendio de técnicas y mejores prácticas para la gestión de la seguridad informática, incluyendo objetivos y controles.

La herramienta también utiliza fundamentos de gestión de riesgos basada en la metodología MAGERIT publicada por el Ministerio de Administraciones Públicas de España [2].

Alcance

En el presente trabajo se investigarán las necesidades que deberá cumplir un sistema que gestione la seguridad de los activos de información. El desarrollo e implementación del sistema está fuera del alcance.

El trabajo tiene los siguientes entregables:

A. Justificación del proyecto
B. Visión del proyecto
C. Análisis del sistema
D. Diseño del sistema
E. Planificación del proyecto

Hipótesis

Azzets permitirá gestionar la seguridad de la información de una organización para saber qué información debe ser resguardada, cómo se la está resguardando, qué activo son prioritarios y qué controles serán los de mayor costo-beneficio.

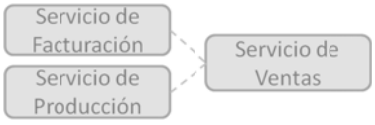
Gestión de activos de información

La herramienta estará basada en la ISO 27002, en el dominio 7 “Gestión de Activos” [1]. En esta sección se explayará el contenido teórico abordado para el diseño de ***Azzets***. El modelo de la solución se basa en el siguiente flujo de trabajo:

Inventario de activos

El primer paso en una gestión de activos de información es realizar un relevamiento y generar un inventario completo y exhaustivo de todos los activos de información en la organización. Los activos de información son los elementos que generan, procesan y utilizan con información de la organización. Los activos de información brindan valor a la organización y ayudan a cumplir sus objetivos estratégicos. Pueden incluir software, hardware, personal, sistemas, ambientes físicos, entre otros.

La dependencia entre activos será incluida dentro del inventario. La dependencia de un activo ocurre cuando se requieren datos o procesos de otro activo para que funcione correctamente un sistema. A modo de ejemplo se incluye un diagrama de dependencia de activos para una organización con una planta de producción.



Clasificación inicial de activos

La clasificación inicial de los activos debe ser realizada considerando las dimensiones de confidencialidad, disponibilidad y criticidad.

La clasificación por confidencialidad es la siguiente:

- **Pública**: No necesita de un control de acceso ya que la información está disponible de forma transparente.
- **Acceso autorizado**: La información es privada y requiere de un control de acceso.
- **Sensible**: Información crítica y altamente protegida.

La disponibilidad determina en cuánto tiempo debe recuperarse un activo que ha sufrido un siniestro para que la operación del área no se vea imposibilitada.

La clasificación por criticidad es la siguiente:

- **Monto**: Implica un costo asociado a un siniestro.
- **Transacción**: Repercute en la pérdida de transacciones.
- **Cliente**: Impacta directamente al cliente externo.
- **Estrategia**: Afecta la estrategia del mercado y el negocio.
- **Complejidad**: Impacto encadenado en varios activos.
- **Cumplimiento**: Disminución o anulación en el cumplimiento de aspectos regulatorios.

Identificación y evaluación de riesgos

A continuación, es necesario identificar todos los riesgos que afecten a cada activo. Los activos están expuestos a una serie de amenazas que podrían desencadenar daños en la disponibilidad, confidencialidad o criticidad.

Clasificación de riesgos

La evaluación de riesgos implica identificar con qué probabilidad de ocurrencia se puede materializar el riesgo y qué impacto tendrá considerando el daño que causaría. La probabilidad y el impacto pueden ser

clasificados, por ejemplo, en un nivel bajo, medio o alto y en una representación numérica de 1, 2 y 3 respectivamente.

El riesgo inherente se calcula multiplicando la probabilidad y el impacto. El riesgo inherente quedará clasificado en 3 niveles: alto (exposición entre 6 y 9), medio (exposición entre 3 y 4) y bajo (exposición entre 1 y 2).

Impacto				
	3	3	6	9
	2	2	4	6
	1	1	2	3
		1	2	3
		Probabilidad		

Clasificación de controles

La implementación de controles previene la materialización de los riesgos y las consecuencias de los mismos. Los controles pueden afectar a uno o más riesgos.

Los controles tienen dos formas de ejecución según su naturaleza:

- **Automática**: Son ejecutados por un sistema informático de forma programada, es decir, se dispara sin la interacción con un ser humano.
- **Manual**: Son ejecutadas por un ser humano y requieren de interacción.

Los controles tienen tres tipos de enfoques:

- **Preventiva**: Son acciones realizadas para evitar la ocurrencia de eventos no deseados. Simplemente previenen: ante la materialización del riesgo, estos controles no detectan ni minimizan sus efectos.
- **Detectiva**: Son acciones que detectan la materialización de un riesgo. Simplemente detectan el evento no deseado: no lo previenen ni pueden minimizar sus efectos.
- **Correctiva**: Son acciones que mitigan los efectos de un riesgo materializado para minimizar el daño.

Efectividad de controles

La efectividad de cada control dependerá de cuánto puedan reducir la probabilidad de ocurrencia y el impacto de un riesgo. La efectividad de un control se medirá según su naturaleza y tipo. Se asignarán tres niveles de efectividad: poco satisfactorio, satisfactorio y muy satisfactorio. El nivel de efectividad depende de la clasificación en el siguiente cuadro:

Naturaleza	Automático	Satisfactorio	Satisfactorio	Muy Satisfactorio
	Manual	Poco Satisfactorio	Satisfactorio	Muy Satisfactorio
		Correctivo	Detectivo	Preventivo
		Tipo		

Cada nivel de efectividad tiene un coeficiente multiplicador asignado entre cero y uno. Los coeficientes para cada nivel de efectividad son:

Nivel de Efectividad	Coeficiente
Poco Satisfactorio	1,00
Satisfactorio	0,50
Muy Satisfactorio	0,25

Mitigación de riesgos

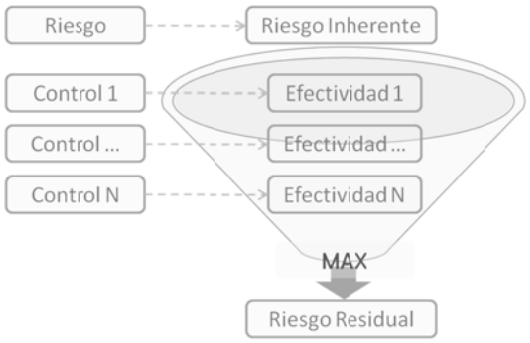
El riesgo residual es la apreciación del riesgo luego de haber aplicado un control. Es decir, el riesgo residual se calcula como la multiplicación entre el riesgo inherente y el coeficiente de efectividad del control, por lo que el riesgo residual siempre será igual o menor al riesgo inherente. Cuanto más satisfactorio sea el nivel de efectividad de un control, menor será el riesgo residual. Este comportamiento se resume en el siguiente cuadro:

Riesgo Inherente	9	2,25	4,50	9,00
	6	1,50	3,00	6,00
	4	1,00	2,00	4,00
	3	0,75	1,50	3,00
	2	0,50	1,00	2,00
	1	0,25	0,50	1,00
		0,25	0,50	1,00
		Efectividad del Control		

Para realizar un mejor análisis se agrupa el riesgo residual en las siguientes clasificaciones:

Clasificación	Riesgo Residual
Alto	3,00 - 9,00
Medio	1,50 - 2,25
Bajo	0,25 - 1,00

Un riesgo puede tener uno o varios controles asociados. Para poder aplicar más de un control a un riesgo es necesario establecer un criterio para determinar la efectividad global de todos los controles asignados a un riesgo. El criterio a tomar en estos casos es calcular la efectividad de un grupo de controles como la efectividad máxima de dichos controles.



Clasificación del activo según riesgos

Para poder saber cuán crítico es un activo según sus riesgos, es necesario establecer una clasificación. Dicha clasificación requiere que se hayan calculado previamente los riesgos residuales. Al mitigar un riesgo, su riesgo residual aparecerá en el cuadro “Riesgo Inherente / Efectividad del Control” expuesto anteriormente. Cada activo tendrá una distribución de riesgos residuales, algunas clasificadas como altas, otras como medias y el resto como bajas.

Se utilizará un ponderador del riesgo total del activo para poder clasificar los activos según sus riesgos. Para poder aplicar este ponderador, es necesario dividir el mapa en zonas.

Riesgo Inherente				
	9	XVI	XVII	XVIII
	6	XIII	XIV	XV
	4	X	XI	XII
	3	VII	VIII	IX
	2	IV	V	VI
	1	I	II	III
		0,25	0,50	1,00
		Efectividad del Control		

El ponderador tiene las siguientes clasificaciones para el activo:

- **Altamente crítico**: Existe al menos un riesgo en las zonas XV, XVII o XVIII.
- **Crítico**: Al menos un 50% están entre IX, XII y XIV.
- **Medio**: La distribución no es crítica ni moderada.
- **Moderado**: Al menos un 70% están entre las zonas I, II, III, IV, V, VII o X.
- **Bajo**: Todos los riesgos están entre las zonas I, II, III, IV, V, VII o X.

Este ponderador a su vez se ajustará según la clasificación inicial (confidencialidad, disponibilidad y criticidad) del activo. En casos de que los activos sean de gran relevancia, el ponderador podrá elevarse a un nivel superior.

Mapa integral de riesgos

El mapa integral de riesgos se basa en los resultados de la clasificación de activos según el riesgo. Cada activo del inventario tendrá una clasificación según el ponderador. El mapa integral permite mostrar de forma compacta y rápida el estado actual de todos los activos según la clasificación de sus riesgos. El mapa integral de riesgos permite enfocarse rápidamente en brindar recursos a los activos que requieren mayor atención.

Nivel	Activos
Altamente Crítico	Servicio de Facturación
Crítico	Servidor AR01
Medio	Servicio de Ventas
Moderado	Servicio de Producción, Centro de Cómputos
Bajo	Servidor AR02, Firewall

Justificación del proyecto

Justificación de la necesidad

El principal motivo que justifica este proyecto son es brindar un fundamento en la toma de decisiones estratégicas en la gestión de activos. El sistema propuesto permitirá saber cuál es la situación actual de cada activo en la empresa, si hay riesgos no mitigados, diseñar un plan de continuidad, revisar el histórico de siniestros en cada activo, evaluar la necesidad de implementar controles y evaluar el costo-beneficio de cada control.

Estos beneficios se ven altísimamente potenciados debido a que en la actualidad no existen herramientas con la visión integral propuesta, generando una ventana de oportunidad para aumentar la competitividad con respecto a la competencia.

El sistema no tiene ningún impacto directo sobre los sistemas de la empresa, ya que no es invasiva y no requiere integración de ningún tipo. Como resultado de la aplicación del sistema, se tendrá una mejor comprensión de los sistemas de la empresa y su nivel de resguardo.

Análisis del entorno del proyecto

Se realizó una investigación en el mercado y se hallaron una infinidad de productos enfocados en la gestión de activos de información. Existe una gran variedad de productos pero ninguna ofrece el enfoque brindado por ***Azzets***. Para más detalles sobre las soluciones actuales en el mercado, ver el Anexo A. ***Azzets*** será una herramienta estratégica con un alto valor diferencial.

Beneficios para el negocio

Los principales beneficios se listan a continuación:

N°	Ventaja	Descripción	Beneficio
1	Inventario centralizado	Se tiene un inventario único, centralizado y clasificado de los activos de información de la organización. Hay mayor conocimiento sobre los sistemas existentes	Alto

N°	Ventaja	Descripción	Beneficio
2	Detección de controles con bajo costo/beneficio	Se podrán reducir costos en controles poco eficientes o mal implementados	Alto
3	Análisis de sensibilidad de controles	Mejor información para la toma de decisiones a la hora de invertir en futuros controles evaluando el impacto de cada control en el sistema	Alto
4	Gestión de riesgos	Se identifican los riesgos y se clasifican. Los riesgos generan una base para tomar las decisiones y alterar la situación actual.	Alto
5	Histórico de siniestros	Se podrá revisar y analizar los tiempos de recuperación reales luego de la ocurrencia de siniestros. La aplicación correcta de controles deberían reducir los tiempos de recuperación en donde aplique por lo que se podría evaluar la eficacia de los controles una vez implementados.	Alto
6	Cumplimiento con ISO 27001	Si se busca certificarse con ISO 27001, el sistema permitirá controlar el dominio 7 “Activos de Información”	Medio
7	Planificación de continuidad optimizada	Al tener la inter-dependencia de los activos, se puede mejorar el plan para la recuperación de los activos y detectar inconsistencias	Medio

El retorno de la inversión será directo y rápido dado que podrá ahorrar dinero en controles innecesarios o poco efectivos.

Visión del proyecto

Visión

La visión del proyecto es diseñar un sistema de gestión estratégica de activos de información sin precedentes en el mercado. El eje central de este proyecto es planificar la construcción de un producto que ofrezca ventajas competitivas en materia de gestión de activos de información basada en riesgos, armando informes automáticamente, que permita analizar la sensibilidad al incorporar nuevos controles y fundamentar las decisiones a la hora de invertir capital en seguridad.

Equipo de Trabajo

El equipo de trabajo estará compuesto por tan sólo una persona, el autor de este trabajo. El tutor de este trabajo será el *sponsor* del proyecto.

FODA

Se utilizó la herramienta FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) para evaluar el panorama mercadotécnico del proyecto.

Fortalezas

- Generación de mapas integrales de riesgos por activo y por departamento.
- Detección de dependencias entre activos.
- Armado de escenarios con posibles controles a incorporar.
- Planes de recuperación ante siniestros más efectivos.
- Análisis de costo/beneficio de los controles a agregar.
- Revisión histórica de recuperación ante siniestros.
- Priorización al invertir en controles para activos y departamentos.
- No es invasivo ni tiene impacto en los sistemas existentes.

Oportunidades

- Los productos en el mercado actual no ofrecen el enfoque estratégico que brinda ***Azzets***.

Debilidades

- El sistema no incluye aspectos de cumplimiento con normas y estándares.

Amenazas

- Incorporación de una gestión de riesgos más estratégica en los productos del mercado.

Análisis del sistema

Requerimientos funcionales

En esta sección se enumerará la funcionalidad del sistema.

- Activos de información

1. Alta, baja y modificación de activos. El activo tiene un monto asociado.
2. Asignación del departamento al cual pertenece.
3. Clasificación de activos:
    - Confidencialidad (público, acceso autorizado o sensible).
    - Disponibilidad (tiempo de recuperación).
    - Criticidad (afecta por monto, transacción, cliente, estrategia, complejidad, cumplimiento).
4. Asignación de riesgos ya existentes a un activo seleccionado.
5. Gestión de los siniestros para un activo seleccionado.

- Plan de recuperación

6. Dependencia entre activos: seleccionar el mínimo estricto de activos requeridos por un activo seleccionado para que funcione correctamente. Un activo debe tener un tiempo de recuperación mayor o igual al máximo tiempo de recuperación entre los activos de los cuales depende. Deben evitarse dependencias cíclicas entre los activos.
7. Informe de disponibilidad de activos. Contiene un listado de los activos y su clasificación por disponibilidad, es decir, el tiempo de recuperación deseado.
8. Informe de dependencia de activos. Para cada activo, contiene un listado de los activos de los cuales depende. El informe puede ser graficado en un árbol.
9. Informe de plan de recuperación. Está basado en el árbol de dependencia de activos. Para cada activo, se enumera su tiempo de recuperación, los activos de los cuales depende y los tiempos de recuperación que le preceden.

- Siniestros

10. Histórico de tiempos de recuperación de activo ante siniestros. Se dan de alta siniestros con la fecha del suceso y el tiempo real en que se tardó en recuperar el activo.

11. Informe de siniestros. Se enumerarán los siniestros ocurridos en un rango de fechas y los tiempos de recuperación reales para cada siniestro. A modo de resumen, se promediarán los tiempos de recuperación reales para cada activo.

- Gestión de Riesgos

12. Alta, baja y modificación de riesgos. Los riesgos tienen un identificador y un texto descriptivo. Para cada riesgo se puede ver de forma gráfica su riesgo inherente, los activos a los que afecta y sus controles asociados.

13. Evaluación del riesgo. La probabilidad e impacto se medirán con las categorías alto (3), medio (2) y bajo (1).

14. El riesgo inherente se calculará multiplicando la probabilidad por el impacto. La clasificación por riesgo inherente es alta (entre 6 y 9), medio (entre 3 y 4) y bajo (entre 1 y 2).

15. Asignación de los activos afectados por un riesgo seleccionado.

16. Asignación de controles a un riesgo seleccionado.

- Gestión de Controles

17. Alta, baja y modificación de controles. Cada control tiene un texto descriptivo y un costo asociado. El control puede estar aplicado o planificado. Los controles aplicados mitigan los riesgos asociados, mientras que los controles planificados simplemente existen para analizar su implementación.

18. Clasificación por tipo de ejecución: manual o automática.

19. Clasificación por enfoque: preventiva, detectiva y correctiva.

20. Cálculo de coeficiente multiplicador de efectividad del control, basado en el tipo de ejecución y su enfoque.

21. Cálculo de riesgo residual al multiplicar el riesgo inherente y la efectividad del control.

22. Cálculo del ponderador del riesgo total del activo. El cálculo se realiza al analizar la distribución de riesgos residuales para cada riesgo del activo.

23. Ajuste del ponderador del riesgo total del activo según clasificación inicial del activo (confidencialidad, disponibilidad y criticidad).

24. Asignación de riesgos a mitigar para un control seleccionado.

- Mapa integral de riesgos

25. Mapa integral de riesgos de activos. Listado de los activos clasificados según sus riesgos.

26. Mapa integral de riesgos de activos agrupados por departamento. Listado de los activos agrupados por departamento y clasificados según sus riesgos.

27. Mapa integral de riesgos de departamentos. Listado de los departamentos y clasificados según los riesgos de todos sus activos.

28. Análisis de sensibilidad en adquisición de controles. Se basa en el mapa integral de riesgos actual (calculado con los controles aplicados) y los controles planificados (no aplicados). El análisis de sensibilidad se construye a partir de la selección de controles no aplicados pero que se desea adquirir y se estudia qué efecto causa en el mapa integral de riesgos y cuánto cuesta. En resumen, se hace un análisis de costo/beneficio para los controles que se desean aplicar en un futuro.

- Administración

29. Alta, baja y modificación de usuarios. Cada usuario tendrá un nombre de usuario, una contraseña, nombre y apellido.

30. Alta, baja y modificación de departamentos. Cada departamento tiene un texto descriptivo para su nombre.

31. Configuración de los criterios para el ajuste del ponderador del riesgo total del activo según la clasificación inicial del activo. Los criterios son condiciones que de cumplirse alguno de ellos, se elevará un nivel al ponderador.

    - Confidencialidad: Si el activo es de acceso autorizado o de información sensible.

- Disponibilidad: Si el activo tiene un tiempo de recuperación mayor a un umbral.
- Criticidad: Si el activo excede un monto, excede un porcentaje de transacciones, si tiene una alta complejidad o si afecta la relación con el cliente externo, información estratégica o de cumplimiento en cuestiones legales.

- Operación

32. Ingreso al sistema proporcionando un usuario y contraseña válidos. Los usuarios del sistema son los dados de alta por el administrador.

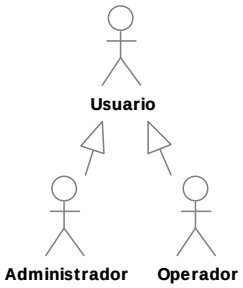
33. Cambio de contraseña por parte del usuario. Es un requisito obligatorio ingresar la contraseña actual antes de realizar el cambio.

Actores

Los actores son roles interpretados por una persona en un tiempo y lugar específicos. Los actores identificados en este sistema son:

- **Usuario**: Ingresa al sistema y puede acceder a cierta funcionalidad según el rol que tenga asignado (operador o administrador).
- **Operador**: Realiza las tareas principales del sistema, tales como dar de alta activos, administrar los riesgos y los controles.
- **Administrador**: Se encarga de las tareas administrativas del sistema, como dar de alta los usuarios del sistema.

La herencia entre actores es una propiedad para especificar una jerarquía entre los actores. Si un actor hereda de otro, está en verdad cumpliendo con ambos roles. De esta aclaración se desprende que tanto el actor operador como el actor administrador heredan del actor usuario, ya que ambos deben ingresar al sistema y acceder a funcionalidad. A continuación se grafica esta relación:



Análisis de datos

El análisis de los datos es crucial para entender y especificar la persistencia de la información. En todo sistema existen entidades las cuales agrupan atributos o datos propios de cada entidad. Las entidades también pueden estar relacionadas y dichas relaciones deben ser persistidas.

Según el análisis de requerimientos se pudieron identificar las siguientes entidades y sus respectivos atributos:

- **Departamento**: identificador y nombre.
- **Activo**: identificador, nombre de activo, identificador del departamento al que pertenece, monto asignado, nivel de confidencialidad (público, autorizado o sensible), nivel de disponibilidad (tiempo deseado en que debe estar recuperado el activo ante un siniestro) y nivel de criticidad (si tiene relación con el cliente, si contiene información estratégica o si afecta el cumplimiento con normas).
- **Siniestro**: identificador, identificador de activo, texto descriptivo, tiempo real de recuperación y fecha.
- **Riesgo**: identificador, descripción, probabilidad de ocurrencia (1, 2 ó 3) e impacto (1, 2 ó 3).
- **Control**: identificador, descripción, costo, estado (aplicado o planificado), forma de ejecución (manual o automática) y enfoque (preventivo, detectivo o correctivo).
- **Usuario**: identificador, nombre de usuario, contraseña, rol (usuario o administrador), nombre y apellido.

Las relaciones identificadas son:

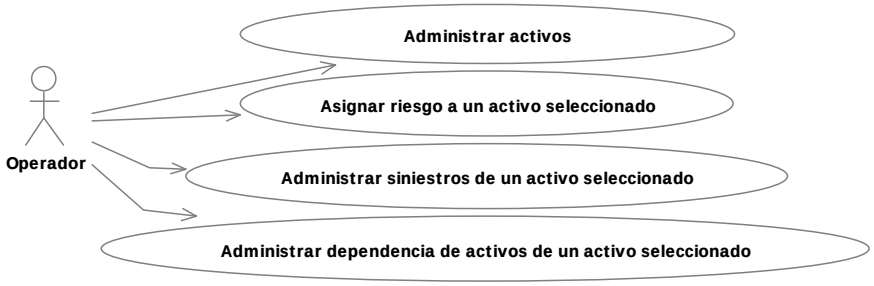
Relación	Entidades	Tipo	Atributos
Asignación de riesgos	Activo-Riesgo	Muchos a muchos	Identificador de activo, identificador de riesgo, fecha
Dependencia entre activos	Activo-Activo	Muchos a muchos	Identificadores de ambos activos relacionados, fecha
Asignación de controles	Control-Riesgo	Muchos a muchos	Identificador de control, identificador de riesgo, fecha

Casos de uso

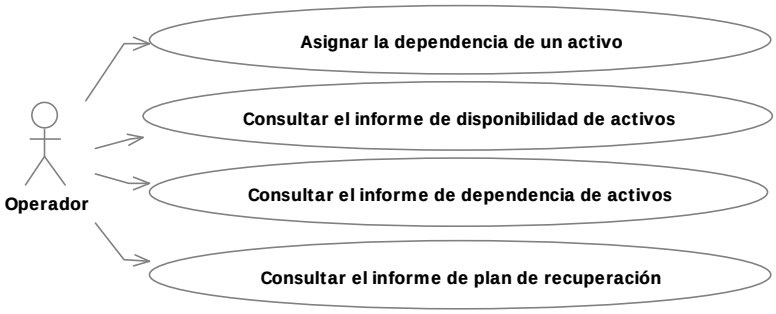
Un caso de uso es un escenario específico que representa la interacción entre un actor y el sistema. Por medio de los casos de uso, se pueden analizar las acciones que el usuario puede realizar en el sistema.

Los casos de uso son identificados claramente con verbos infinitivos. En esta sección, la palabra administrar representa la gestión administrativa en altas, bajas y modificaciones en el sistema.

- Activos de información

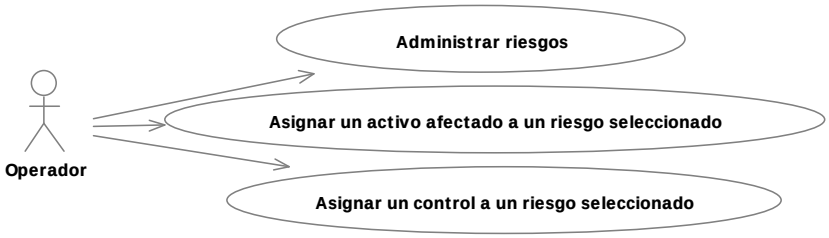


- Plan de recuperación

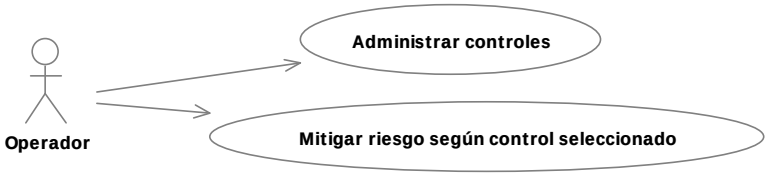


- Siniestros

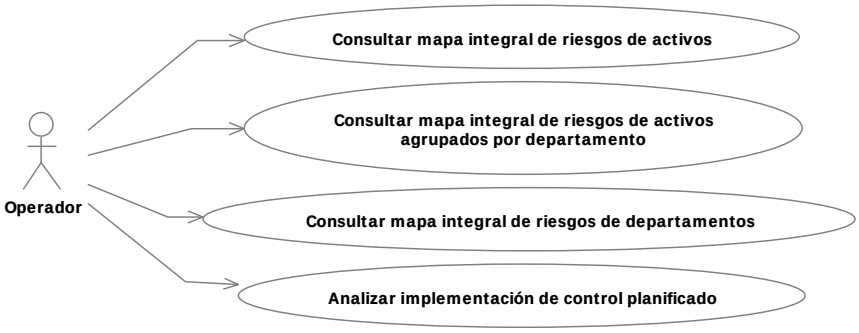
- Gestión de Riesgos



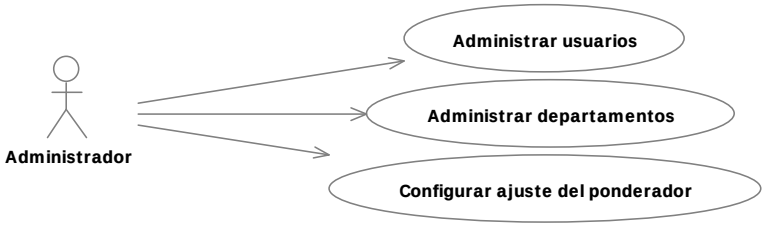
- Gestión de Controles



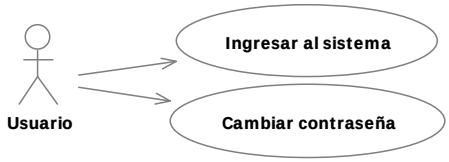
- Mapa integral de riesgos



- Administración



- Operación



Diseño del sistema

Modelo de despliegue

El modelo de despliegue es una representación de los nodos / equipos que interaccionan para que funcione el sistema en su totalidad.

Los nodos son los siguientes:

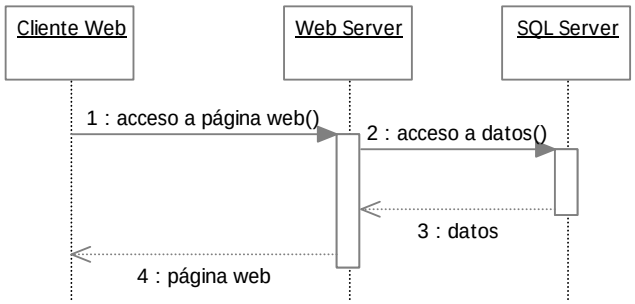
- **SQL Server**: En este equipo se alojará la base de datos Microsoft SQL Server 2005 para almacenar los datos del sistema.
- **Web Server**: Es el servidor que alojará la aplicación web que sustenta la interacción con el usuario final. Tendrá una interacción bidireccional con el SQL server.
- **Cliente Web**: Es el equipo con el cual el usuario final accede al sistema mediante un navegador.

Los protocolos de comunicación entre los nodos son:

- **HTTP (*Hyper Text Transfer Protocol*)**: Es un protocolo para el intercambio de información entre un navegador web y un servidor web.
- **SQL (*Structured Query Language*)**: Es un lenguaje que permite realizar altas, bajas, modificaciones y consultas a la información almacenada en la base de datos.

Modelo de procesos

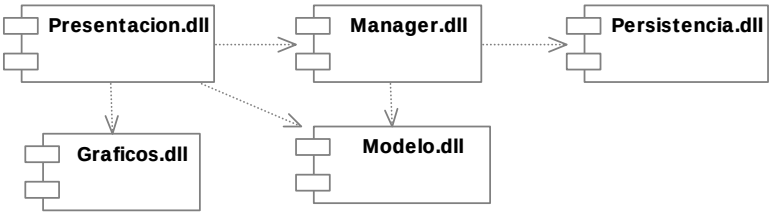
El modelo de procesos es una representación de la interacción entre los procesos involucrados. Este modelo está fuertemente ligado al modelo de despliegue.



El cliente web inicia una solicitud web al requerir una página web ofrecida por el servidor web. El servidor web recibe la solicitud, lo procesa y realiza una consulta a la base de datos. El servidor SQL recibe la consulta y realiza la transacción. El servidor web culmina el procesamiento devolviendo la página web al cliente. Finalmente, el cliente web muestra la página en el navegador.

Modelo de componentes

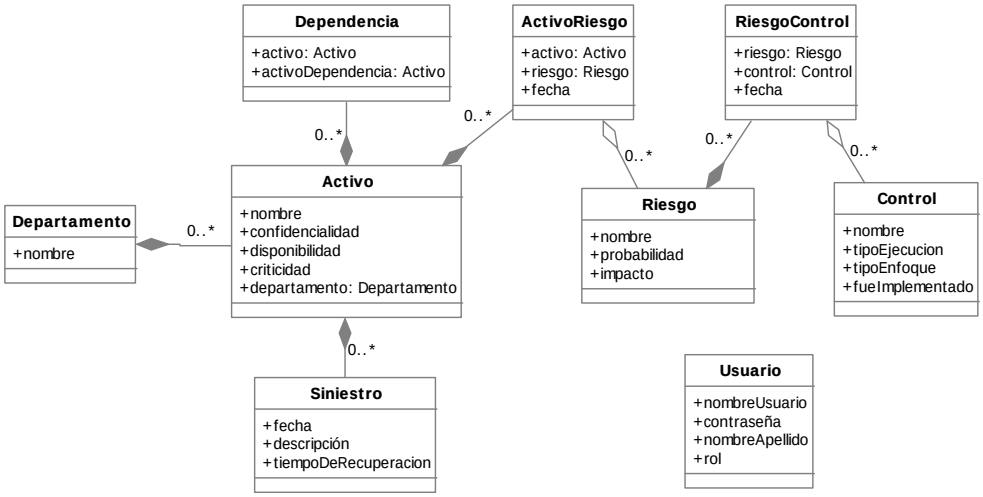
El modelo de componentes enumera los componentes (bibliotecas, ejecutables, etc.) y sus dependencias.



- **Presentación**: Representa la aplicación web a desplegar en el web server ofreciendo toda la funcionalidad del sistema a través de un portal y permitiendo la interacción con el usuario final.
- **Gráficos**: Se encarga de trazar y armar los gráficos a utilizar en los informes.
- **Modelo**: Contiene las entidades del negocio, sus datos intrínsecos y sus relaciones con otras entidades.
- **Manager**: Ofrece servicios para poder utilizar todos los beneficios de trabajar con un modelo inteligente y sincronizado con la base de datos.
- **Persistencia**: Encapsula toda la funcionalidad para acceder y hacer uso de la base de datos.

Diagrama de clases

El diagrama de clases es un modelo que permite ver las relaciones entre las clases / entidades del sistema, enfocándose en el estado (atributos almacenados) y comportamiento (métodos o servicios ofrecidos).



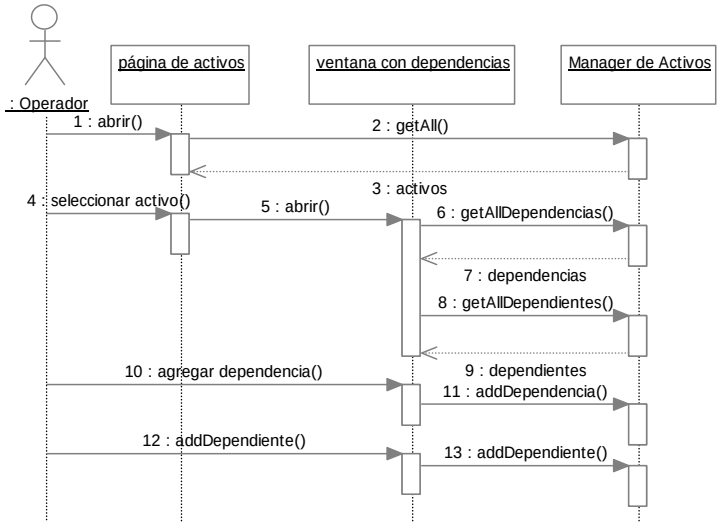
A continuación se analizan las clases:

- **Activo**: es la entidad neurálgica del sistema y representa un activo de información. Un activo tiene un nombre descriptivo y la clasificación inicial (confidencialidad, disponibilidad y criticidad). El activo está asociado a un departamento y posiblemente a varios otros activos de los cuales depende para su correcto funcionamiento. El activo también puede tener varios siniestros registrados y varios riesgos que amenacen su funcionamiento.
- **Departamento**: representa un departamento dentro de la organización y tiene un nombre descriptivo.
- **Siniestro**: modela una caída en el activo, es decir, un incidente en el cual el activo no prestó servicios durante un lapso de tiempo.
- **Riesgo**: contiene un nombre descriptivo, una probabilidad y un impacto.
- **ActivoRiesgo**: Representa la relación entre un activo y un riesgo.
- **Control**: contiene un nombre descriptivo, el tipo de ejecución, el tipo de enfoque y si el control está implementado o si es un control planificado.
- **RiesgoControl**: Representa la relación entre un riesgo y un control.
- **Usuario**: representa un usuario del sistema, conteniendo un nombre, contraseña y datos personales.

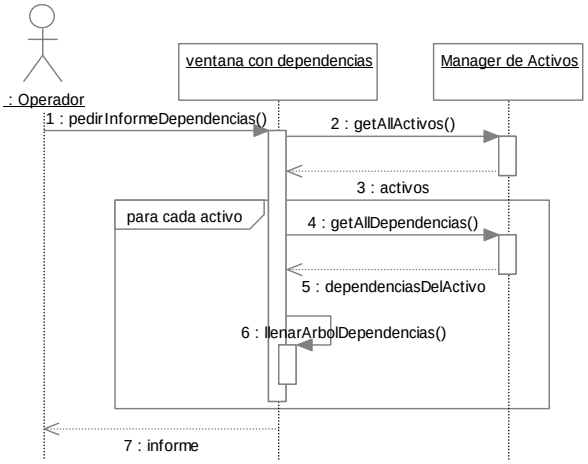
Diagramas de secuencia

Los diagramas de secuencia son representaciones del flujo de información entre los actores y las clases del sistema. Sirven para diagramar las operaciones realizadas, la recuperación y almacenamiento de información. En esta sección se analizarán los casos de uso más representativos o interesantes.

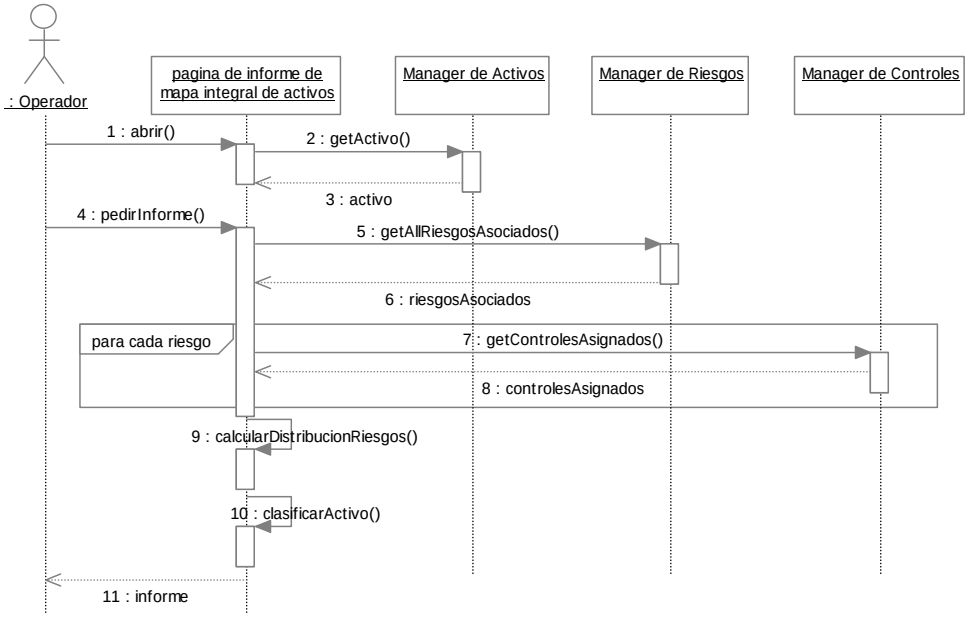
- **Administrar dependencia de activos**: Se puede establecer los activos de los cuales depende un activo seleccionado o también los activos que dependen del activo seleccionado.



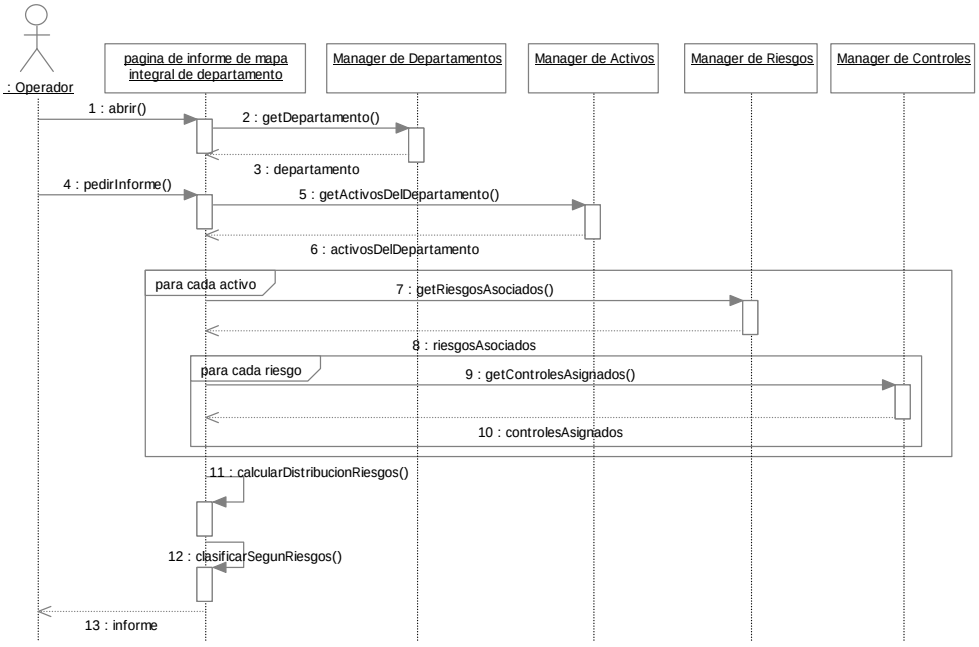
- **Consultar informe de dependencia**: En este caso de uso se arma un árbol según la dependencia de los activos y se establece la cadena de tiempos de disponibilidad.



- **Consultar mapa integral de riesgos de un activo**: Para un activo seleccionado, se genera un informe según la clasificación de riesgos del activo y los controles asociados.



- **Consultar mapa integral de riesgos de departamento**: Para un departamento seleccionado, se genera un informe según la clasificación de los riesgos de todos los activos dentro del departamento y los controles asociados.



Diseño de base de datos

En esta sección se enumeran las tablas que tendrá la base de datos del sistema:

- Departamento

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
Nombre	Cadena	No	-

- Activo

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
Nombre	Cadena	No	-
DepartamentoId	Entero	No	Id de Departamento
Confidencialidad	Entero	No	-
Disponibilidad (horas)	Entero	No	-
Monto	Decimal	No	-
AfectaRelacionCliente	Si/No	No	-
AfectaEstrategia	Si/No	No	-
AfectaCumplimiento	Si/No	No	-

- Siniestro

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
ActivoId	Entero	No	Id de Activo
Descripción	Cadena	No	-
Tiempo de Recuperación (horas)	Entero	No	-
Fecha	Fecha	No	-

- Riesgo

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
Descripción	Cadena	No	-
Probabilidad	Entero	No	-
Impacto	Entero	No	-

- Control

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
Descripción	Cadena	No	-
Aplicado	Si/No	No	-
FormaEjecucion	Entero	No	-
TipoEnfoque	Entero	No	-

- DependenciaActivo

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
ActivoId	Entero	No	Id de Activo
DependeDeActivoId	Entero	No	Id de Activo
Fecha	Fecha	No	-

- Activo-Riesgo

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
ActivoId	Entero	No	Id de Activo
RiesgoId	Entero	No	Id de Riesgo
FechaAsignación	Fecha	No	-

- Control-Riesgo

Columna	Tipo	Clave Primaria	Clave Foránea
Id	Entero	Si	-
ControlId	Entero	No	Id de Control
RiesgoId	Entero	No	Id de Riesgo
FechaAsignación	Fecha	No	-

- Usuario

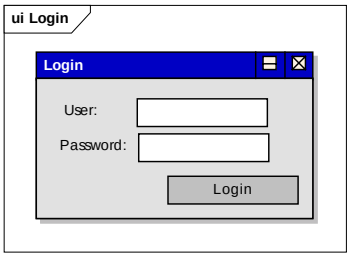
Columna	Tipo	Clave Primaria	Clave Foránea
Usuario	Cadena	Si	-
Contraseña	Cadena	No	-
Nombre y Apellido	Cadena	No	-
Rol	Entero	No	-

Prototipo de pantallas

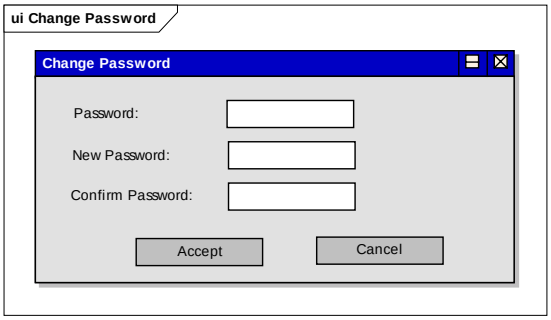
A continuación se mostrarán los prototipos de pantallas para la interfaz gráfica con el usuario. Se analizarán las pantallas basándose en los casos de uso propuestos en la etapa de análisis del proyecto.

Acceso al sistema

- **Ingresar al sistema**. Todo usuario deberá ingresar sus credenciales para acceder al sistema. El sistema identifica al usuario y redirige a un ambiente específico según su rol.

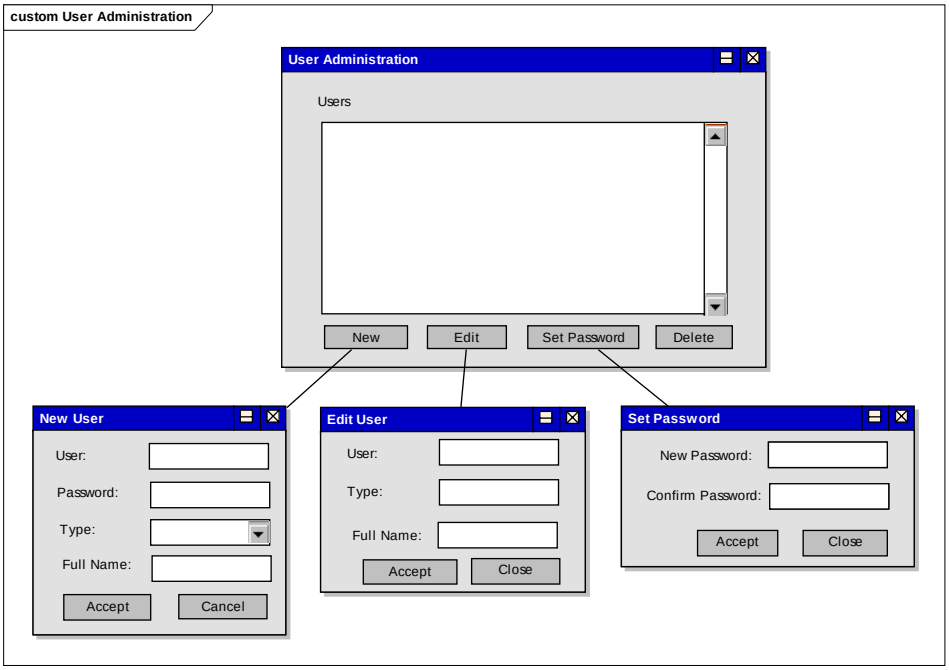


- **Cambiar contraseña**. Esta pantalla será accesible para todo usuario del sistema. Permitirá al usuario cambiar su contraseña cuando lo requiera.

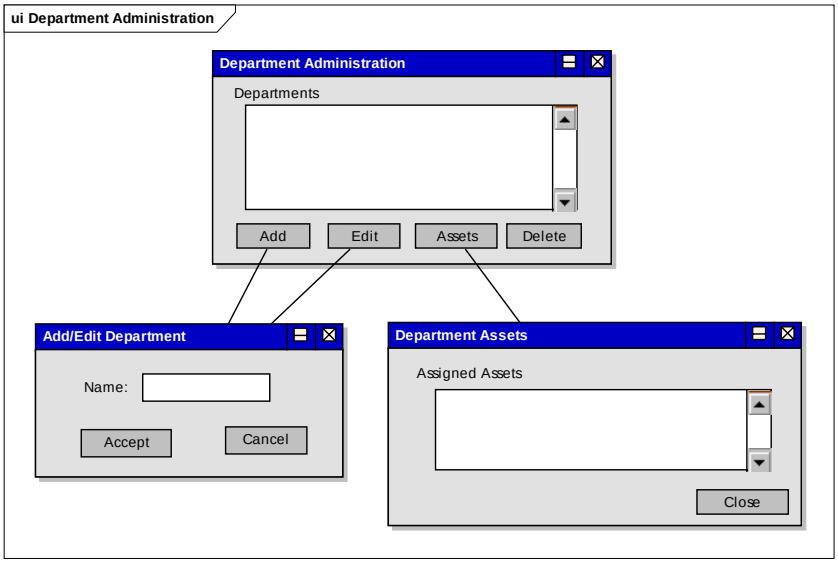


Administración del sistema

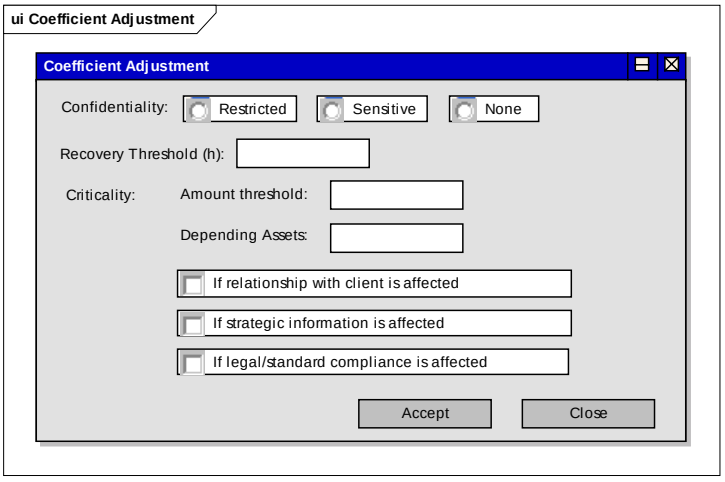
- **Administrar usuarios**. El administrador podrá dar de alta usuarios, modificarlos, eliminarlos o cambiar su contraseña.



- **Administrar departamentos**. El administrador podrá dar de alta, modificar y eliminar departamentos. Además, se podrán visualizar los activos asociados a un departamento seleccionado.

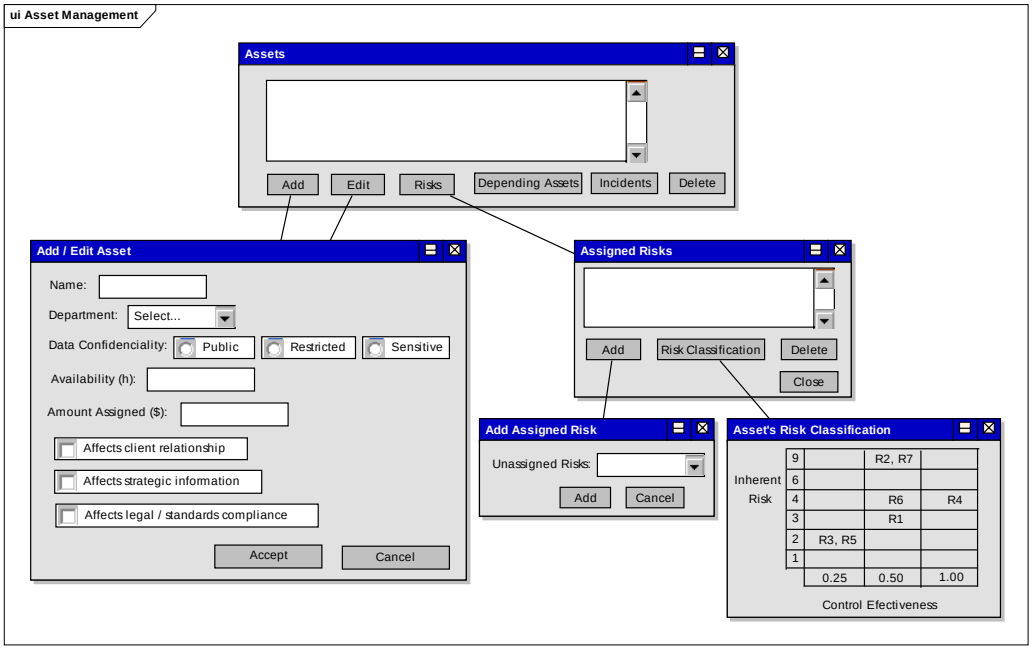


- **Configurar ajuste del ponderador**. El administrador podrá configurar los criterios que en caso de cumplirse causarán que el ponderador total de riesgos de un activo suba un nivel. Estos criterios se definen según la confidencialidad del contenido del activo, su tiempo de recuperación y su criticidad.

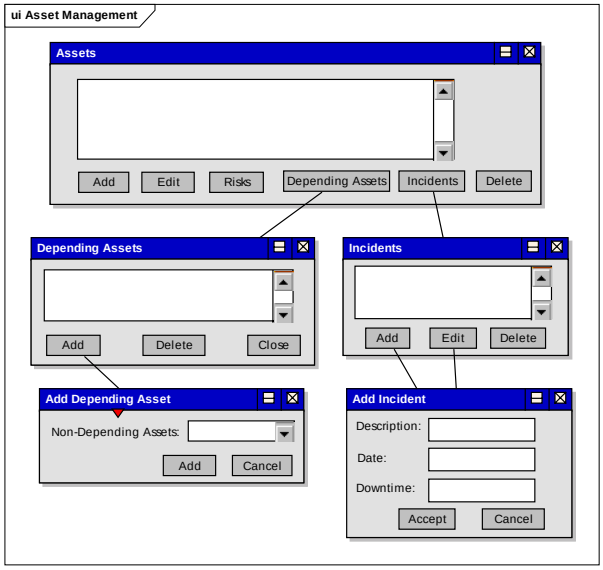


Activos de información

El operador podrá administrar los activos de la organización y asignar los riesgos que afectarán un riesgo seleccionado. Además, se podrá visualizar la clasificación de los riesgos del activo.



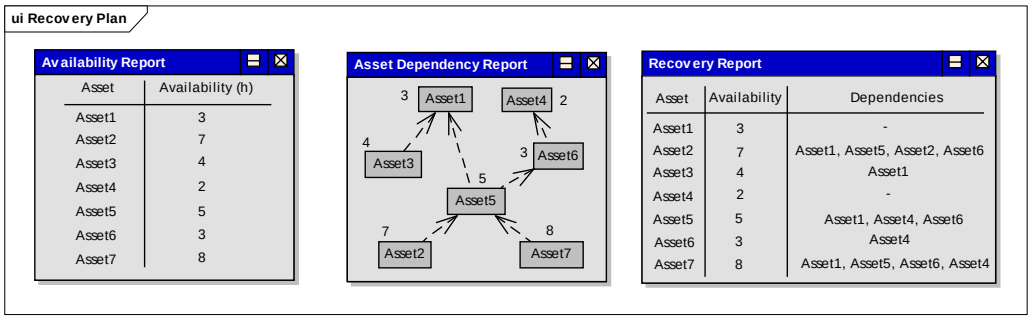
El operador también podrá establecer la dependencia de activos y registrar los incidentes.



Plan de Recuperación

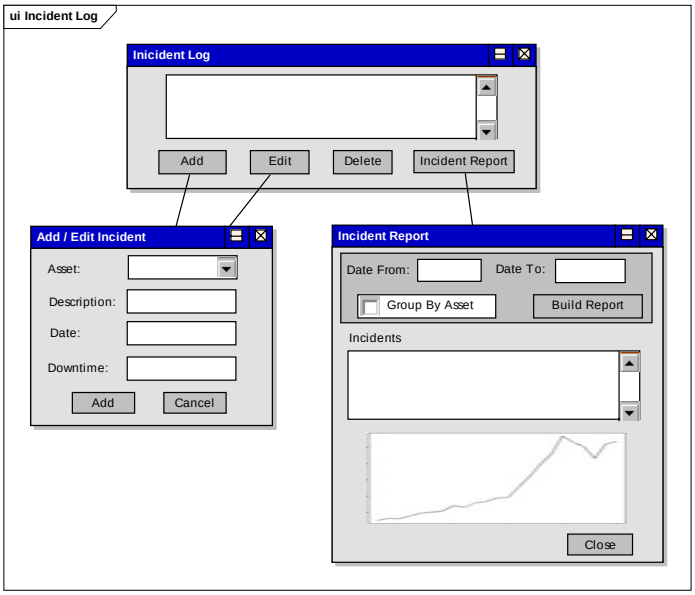
El operador podrá acceder a los informes acerca de la disponibilidad de los activos de la organización. El informe de disponibilidad permitirá listar los activos y su tiempo de recuperación deseada. El informe de dependencia de activos permitirá ver en forma gráfica la dependencia entre los activos de

la organización. El informe del plan de recuperación lista los activos, su tiempo de recuperación y todos los activos de los cuales depende.



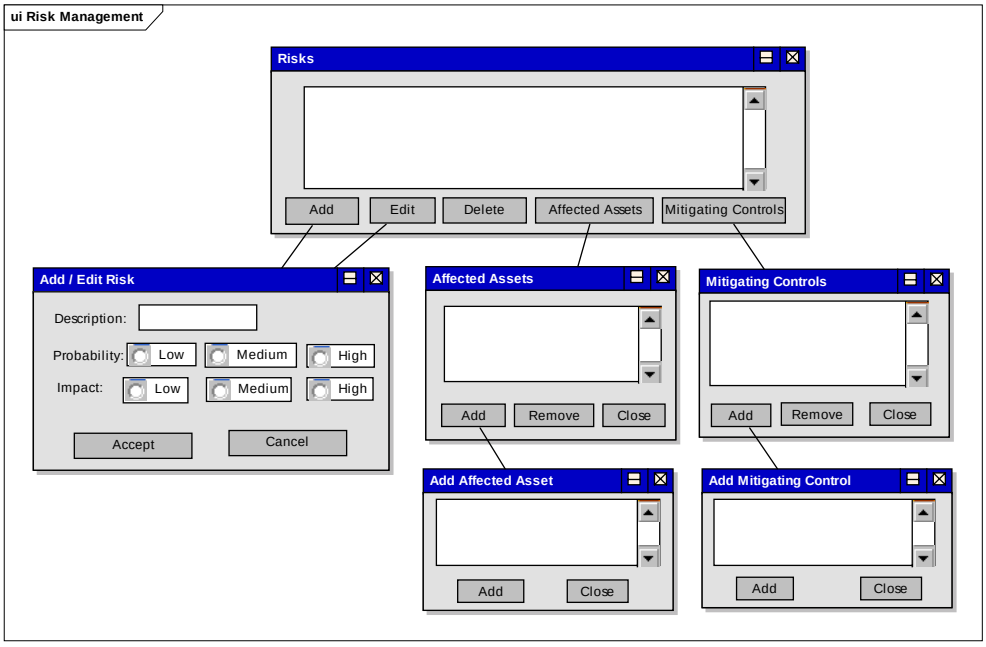
Siniestros

El operador podrá administrar los siniestros ocurridos en los activos de la organización. Se podrá realizar un reporte de los incidentes en un rango de fechas arbitrario y hasta podrá optar en agrupar los incidentes por activo.



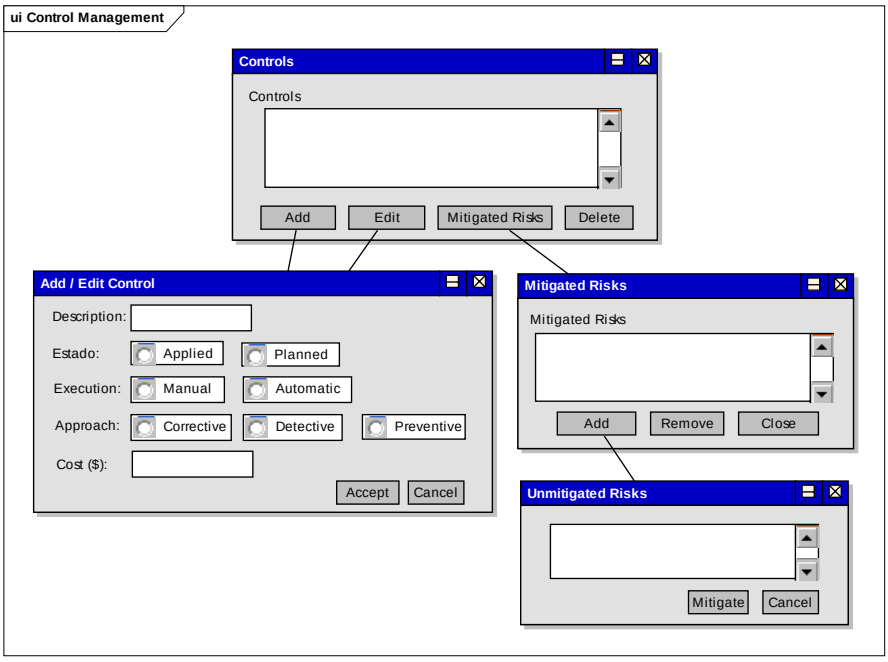
Gestión de riesgos

El operador podrá administrar los riesgos, asignar a qué activos afectará un riesgo seleccionado así como qué controles lo mitigarán.



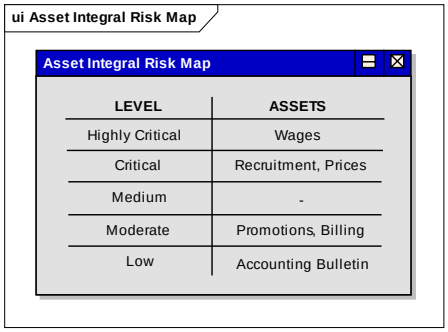
Gestión de Controles

El operador podrá administrar los controles en la organización y categorizarlas. Se podrá acceder a los riesgos mitigados por un control seleccionado y se podrán agregar riesgos a mitigar por dicho control.

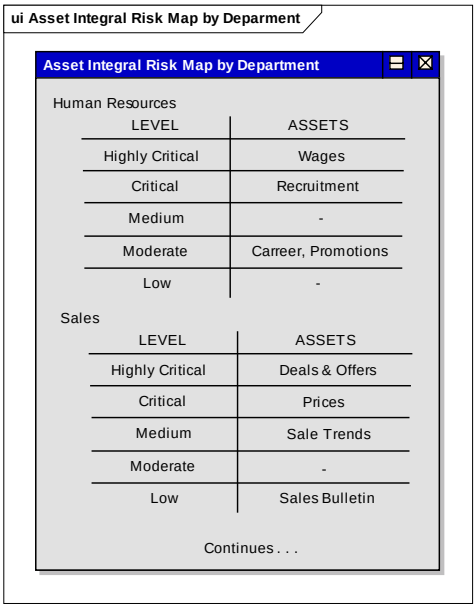


Mapa integral de riesgos

- **Consultar mapa integral de riesgos de activos**: El operador podrá acceder y ver el mapa integral de riesgos de todos los activos de la organización. De esta manera, se podrá ver el nivel de criticidad de cada activo y se podrá enfocar en invertir y planificar controles para los activos más críticos.

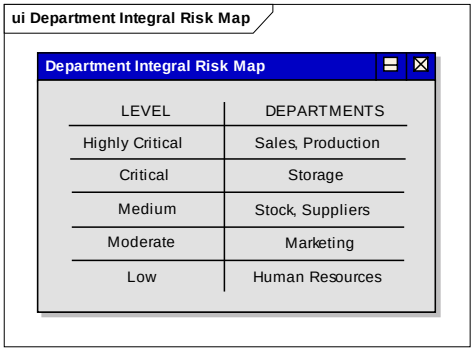


- **Consultar mapa integral de riesgos de activos agrupados por departamento**: El operador podrá acceder al mapa integral de riesgo de activos de cada departamento. De esta manera, dentro de un departamento específico se puede detectar fácilmente cuales son los activos más críticos que requieren nuevos controles. Además, se puede detectar si se están haciendo actualmente inversiones en activos que no son críticos.



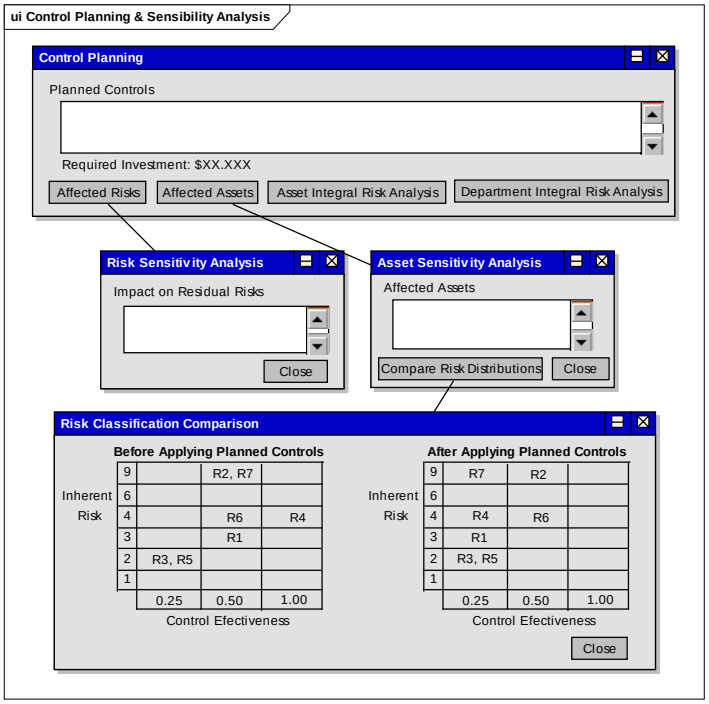
- **Consultar mapa integral de riesgos de departamentos**: El operador podrá ver la criticidad total de cada departamento en la organización al basarse en los activos que posee. Esto permitirá detectar

cuáles departamentos en la organización requieren de inversiones y en qué urgencia.

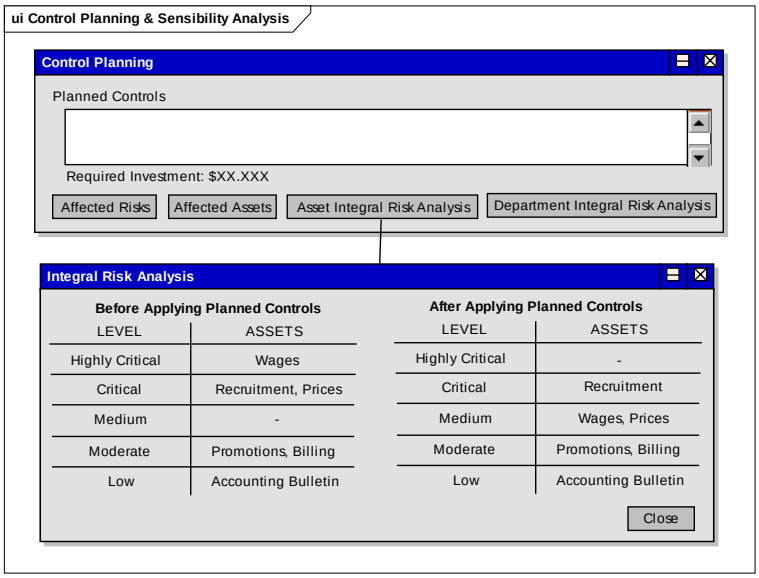


Planificación de controles

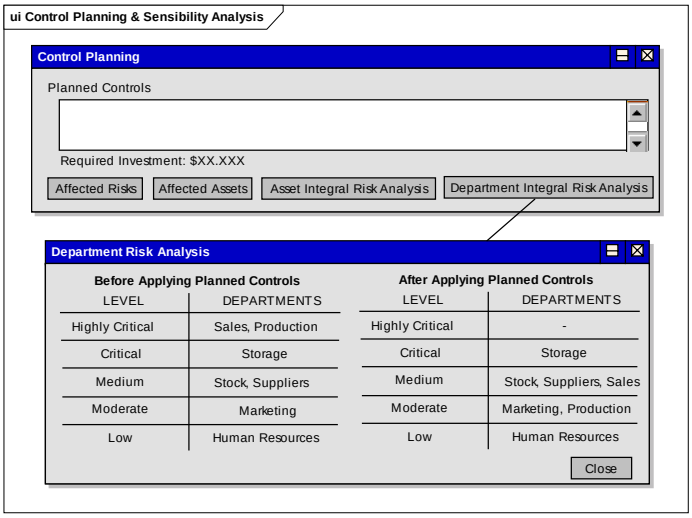
El operador podrá elegir de todos los controles planificados (no aplicados) cuáles desea analizar el impacto de su implementación. Podrá ver cuáles son los riesgos afectados por aplicar los controles planificados y ver cómo se alteran los riesgos residuales. Además, se podrán listar los activos afectados y ver la comparativa entre la clasificación de riesgos de un activo antes y luego de aplicar los controles planificados. De esta manera, se puede observar cómo la distribución de riesgos se ve alterada, desencadenando cambios en el mapa integral de riesgos.



El operador podrá ver los efectos al aplicar los controles planificados observando los cambios en el mapa integral de riesgos de los activos.



El operador podrá ver el impacto en el mapa integral de riesgos de departamentos. De esta forma, podrá analizar cómo varían los niveles de clasificación de cada departamento.



Planificación del Proyecto

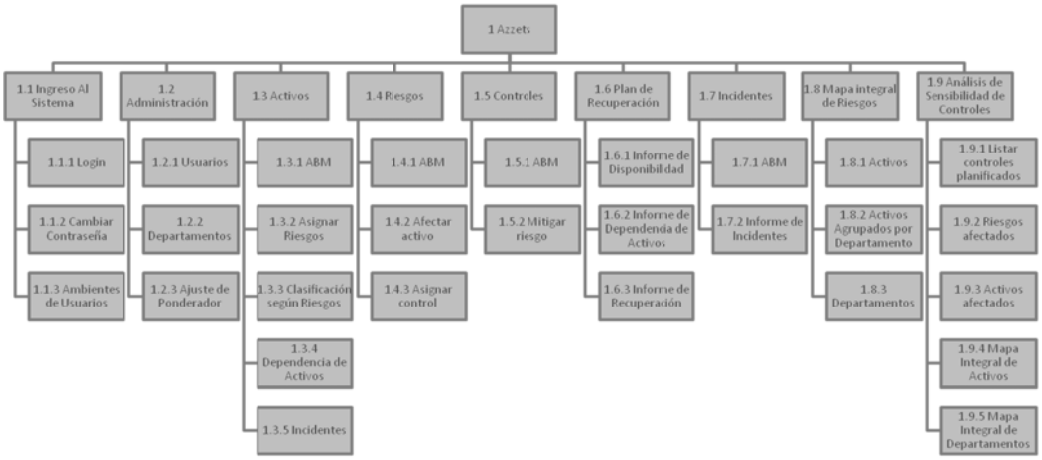
En esta sección se explayarán todos los aspectos y detalles concernientes a la planificación del proyecto. La administración de este proyecto se realizará basándose en el PMBoK, una recopilación de las mejores prácticas [5].

Plan de trabajo

El plan de trabajo de este proyecto está compuesto por tareas y productos a entregar al cliente. Para poder tener una visión global del proyecto y el valor que aporta se utiliza una estructura denominada WBS que permite subdividir el trabajo a realizar para una mejor comprensión del alcance del proyecto, mejor planificación y control del proyecto [3].

Diagrama de WBS

El WBS fue diseñado con una orientación a productos, enfocándose en el valor y entregables percibidos por el cliente. El WBS tomó toda la base de conocimiento en la etapa de diseño, en especial, en los casos de uso enumerados y en los prototipos de pantallas. A continuación se muestra el WBS generado:



Diccionario de WBS

Según la codificación de los ítems en el WBS se armó un diccionario del WBS. Además se realizaron las estimaciones para cada ítem de la WBS utilizando el método de estimación por expertos.

Código	Título	Descripción	Horas
1	Azzets	Representa al proyecto en su totalidad	**198**
1.1	Ingreso Al Sistema	Módulo que se encarga del ingreso de los usuarios al sistema, la autenticación y los ambientes para cada rol.	**17**
1.1.1	Login	Página de ingreso al sistema en el cual se debe ingresar el usuario y contraseña. Según el rol del usuario, se redirigirá al ambiente correspondiente (operador o administrador).	6
1.1.2	Cambiar Contraseña	Pantalla para que el usuario cambie su contraseña cuando lo desee.	5
1.1.3	Ambientes de Usuarios	Cada rol (operador o administrador) tendrá su ambiente, es decir, una página de inicio y un menú según la funcionalidad que pueda acceder dicho rol.	6
1.2	Administración	Módulo para la administración del sistema aportando valor para su funcionamiento correcto.	**22**
1.2.1	Usuarios	Pantalla para administrar los usuarios del sistema. Se podrán dar de alta, editar, eliminar y cambiar la contraseña.	8
1.2.2	Departamentos	Pantalla para administrar los departamentos de la organización.	8
1.2.3	Ajuste de Ponderador	Se podrá configurar los criterios para el ajuste del ponderador a la hora de clasificar los activos según el riesgo.	6
1.3	Activos	Módulo para administrar los activos de la organización.	**38**
1.3.1	ABM	Alta, Baja, Modificación.	6
1.3.2	Asignar Riesgos	Se podrán asignar riesgos que afectarán un activo seleccionado.	8
1.3.3	Clasificación según Riesgos	Para un activo seleccionado, se podrá visualizar la distribución de riesgos asociados según los riesgos inherentes y la efectividad de su mitigación.	8
1.3.4	Dependencia de Activos	Se podrán asignar de qué activos depende un activo seleccionado.	8
1.3.5	Incidentes	Se podrán registrar incidentes a un activo seleccionado.	8
1.4	Riesgos	Módulo para administrar los riesgos en activos de información.	**22**
1.4.1	ABM	Alta, Baja, Modificación.	6
1.4.2	Afectar activo	Para un riesgo seleccionado, se podrán elegir qué activos serán afectados.	8
1.4.3	Asignar control	Para un riesgo seleccionado, se podrán elegir qué controles lo mitigan.	8
1.5	Controles	Módulo para administrar los controles aplicados y planificados del sistema.	**14**
1.5.1	ABM	Alta, Baja, Modificación.	**6**
1.5.2	Mitigar riesgo	Para un control seleccionado, se podrán mitigar los riesgos deseados.	8
1.6	Plan de Recuperación	Módulo para visualizar informes sobre la dependencia de activos y los tiempos de recuperación deseables.	**17**
1.6.1	Informe de Disponibilidad	Informe sobre los activos y su tiempo de recuperación deseada.	6
1.6.2	Informe de Dependencia de	Informe de la dependencia entre activos graficada en forma de árbol.	6

Código	Título	Descripción	Horas
	Activos		
1.6.3	Informe de Recuperación	Informe sobre la disponibilidad de cada activo y de qué activos depende. Es una versión más detallada del informe de disponibilidad.	5
1.7	Incidentes	Módulo para registrar incidentes en los activos.	**14**
1.7.1	ABM	Alta, Baja, Modificación.	6
1.7.2	Informe de Incidentes	Informe de los incidentes registrados en un rango de fechas arbitrario.	8
1.8	Mapa integral de Riesgos	Módulo para la generación de mapas integrales de riesgo	**20**
1.8.1	Activos	Informe basado en el mapa integral de riesgos de activos. Cada activo será clasificado según sus riesgos.	6
1.8.2	Activos Agrupados por Departamento	Informe similar al mapa integral de activos. Para cada departamento se hará un mapa integral de los activos de la que es dueño.	8
1.8.3	Departamentos	Informe sobre el mapa integral de riesgos de departamentos basado en la totalidad de activos.	6
1.9	Análisis de Sensibilidad de Controles	Módulo para analizar la sensibilidad en los activos al aplicar nuevos controles planificados.	**34**
1.9.1	Listar controles planificados	Listado de los controles en la organización que tengan un estado no aplicado, es decir, planificado. Según los controles seleccionados en este listado se procederá a realizar el análisis de sensibilidad.	5
1.9.2	Riesgos afectados	Se listarán los riesgos afectados por los controles seleccionados y se compararán los riesgos residuales al aplicar dichos controles.	5
1.9.3	Activos afectados	Se listarán los activos afectados por dichos controles. Para cada activo se podrá comparar la distribución de riesgos antes y después de aplicar los controles planificados.	8
1.9.4	Mapa Integral de Activos	Se comparan los mapas integrales de activos antes y después de aplicar los controles planificados.	8
1.9.5	Mapa Integral de Departamentos	Se comparan los mapas integrales de departamentos antes y después de aplicar los controles planificados.	8

Planificación de Entregas

El proyecto será ejecutado siguiendo con una metodología de entregas incrementales. Las entregas incrementales se basan en entregas parciales y sucesivas al cliente aportando valor en cada una de ellas. Las ventajas de utilizar esta metodología es que el cliente tiene un retorno de la inversión mucho más corto, se familiariza con el producto rápidamente, hay mayor interacción con el cliente causando mayor *feedback*, el producto se valida en cada entrega y siempre crece en un sentido positivo.

Se diseñaron seis entregas incrementales, las cuales se detallan a continuación.

Para una visión integral del proyecto, para cada entrega incremental se incluye un diagrama WBS con los ítems a entregar.

1. Administración: Se entregará la base fundamental del sistema, incluyendo la autenticación de usuarios y la administración para su correcto funcionamiento en un futuro.

2. Activos, Riesgos y Controles: En esta entrega ya se podrán cargar las entidades críticas del sistema, es decir, los activos, riesgos y controles.

3. Plan de recuperación: En esta entrega se incluirá la lógica para establecer dependencias entre activos y generar informes sobre la disponibilidad y tiempos de recuperación.

4. Incidentes: En esta entrega se desarrollará la capacidad de registrar incidentes en los activos de información.

5. Mapas integrales de riesgos: En esta entrega se incluirá la capacidad de clasificar activos según sus riesgos y armar mapas integrales de riesgos según la configuración del ponderador.

6. Planificación de Controles: En esta última entrega se podrá realizar un análisis de sensibilidad en los activos del sistema al aplicar controles planificados.

Funcionalidad Completa

En esta sección se planificará la funcionalidad completa (FC) del proyecto. La FC busca identificar los módulos del sistema y asignarles un peso (entre cero y diez) que representa la dificultad e importancia de la funcionalidad contenida dentro de cada módulo.

Los módulos fueron agrupados por entrega incremental y se calculó un subtotal.

Entrega	Funcionalidad	Peso (0-10)	Peso Total
1	Ingreso al Sistema	5	13
	Administración	8	
2	Activos	6	20
	Riesgos	8	
	Controles	6	
3	Plan de Recuperación	9	9
4	Incidentes	8	8
5	Mapas Integrales	10	10
6	Planificación de Controles	10	10

A continuación se grafica los puntos de función acumulados para cada entrega. El gráfico permite ver una tendencia bastante pareja en las entregas, evitando picos innecesarios.

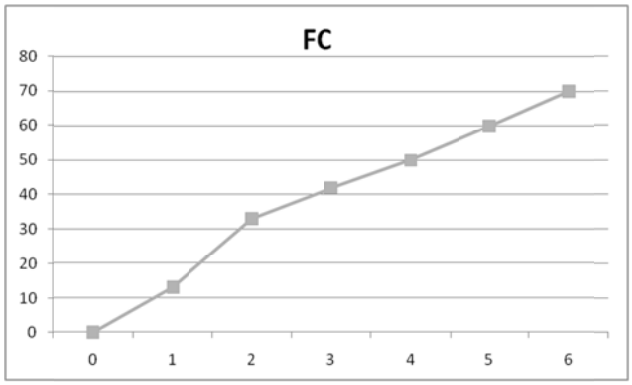
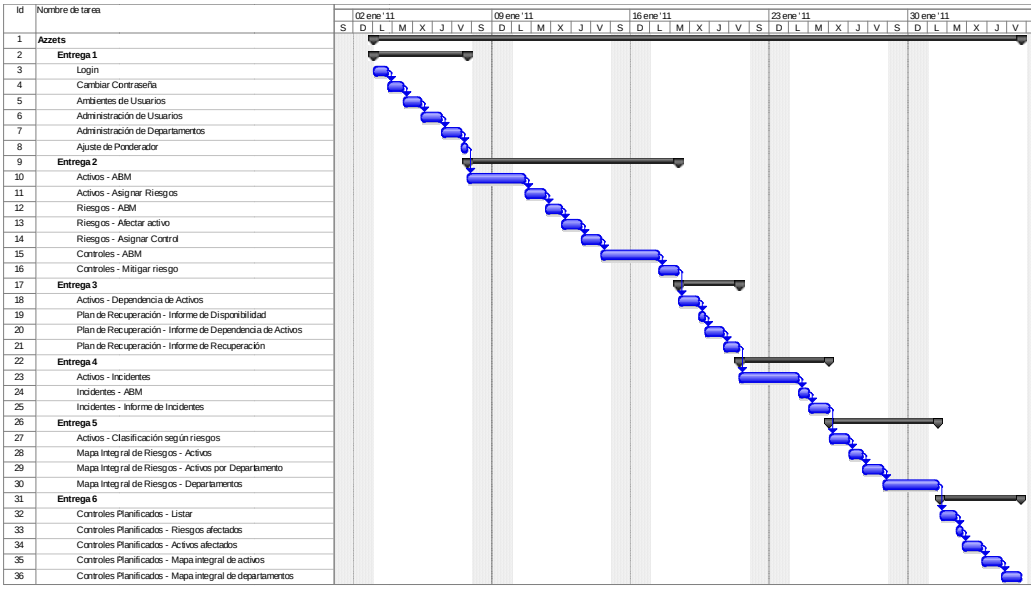


Diagrama de Gantt

A partir de las estimaciones de las tareas y las entregas planificadas, se ingresaron las tareas con sus respectivas duraciones y dependencias para el control y seguimiento del proyecto:



Earned Value

En esta sección se analizará y planificará el valor ganado en cada entrega incremental. El marco a utilizar será el de *Earned Value* [4], el cual permitirá tener métricas muy interesantes durante la ejecución del proyecto. Para ver en más detalle se recomienda leer el Anexo B.

Implementación de EV

La implementación de EV será medido en horas-hombre.

A continuación se detallan los criterios de medición:

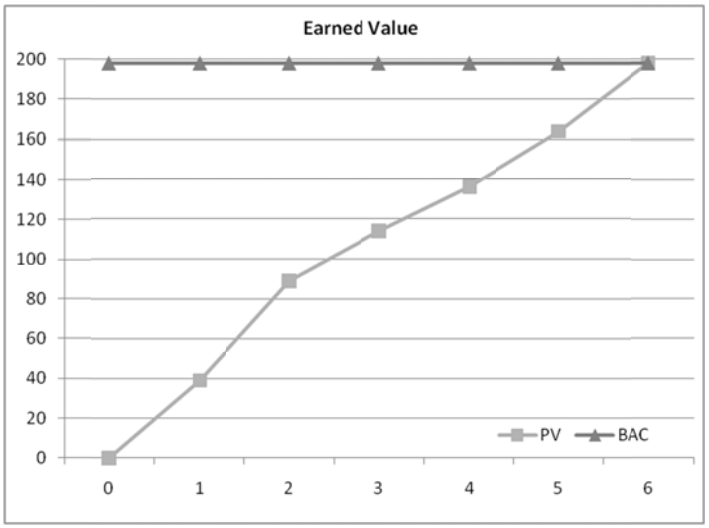
- **PV**: Su estimación está estrictamente ligada a la estimación de duración de tareas. Para poder estimar el PV para cada etapa, se basará en el WBS y las tareas a entregar en cada entrega incremental.
- **AC**: Los costos en este proyecto estarán reflejados por las horas invertidas en cada entrega incremental, es decir, estará condicionada por la duración real de las tareas planificadas.
- **EV**: El EV se medirá en función del estado de las tareas del proyecto. Las tareas pueden estar sin empezar, comenzadas y terminadas. El EV estará regida por las siguientes reglas:
  1. Si la tarea no fue comenzada, no aporta EV.
  2. Si la tarea fue comenzada, aporta el 50% del valor de la tarea.
  3. Si la tarea fue terminada, aporta el 100% del valor de la tarea.

Planificación de EV

Según las estimaciones de los ítems del WBS a entregar en cada entrega incremental, se calculó el valor aportado sumando la duración de las tareas. El PV es el valor acumulado para cada entrega y se presenta en la siguiente tabla:

Entrega	Valor Aportado	PV
1	39	39
2	50	89
3	25	114
4	22	136
5	28	164
6	34	198

El BAC, presupuesto al finalizar el proyecto, está definida como el PV de la última entrega (BAC = 198). El PV fue graficado a continuación:


Earned Value
200
180
160
140
120
100
80
60
40
20
0
0
1
2
3
4
5
6
PV
BAC

Conclusiones

La implementación de Azzets brindará una herramienta poderosa para la gestión de la seguridad informática, apoyando el cumplimiento de los objetivos estratégicos del negocio. Azzets brindará valor agregado basándose en su repositorio centralizado de activos, el almacenamiento de los incidentes ocurridos, dependencia entre activos, una vista por departamento de los activos, optimizaciones en el plan de recuperación ante siniestros, la gestión de sus riesgos y el análisis de controles a implementar.

En este trabajo se ha investigado sobre gestión de activos de información combinados con conceptos de gestión de riesgos. Es importante destacar que este trabajo permitió realizar un análisis, diseño y planificación para el desarrollo de Azzets, para luego plasmarlo en un producto operativo. Es meritorio recalcar cómo Azzets se nutre de las necesidades y las mejores prácticas para gestionar riesgos y los activos de información de una organización.

Azzets permitirá mejorar los procesos de gestión de activos y proveer evidencia sólida sobre la situación actual y futura de la seguridad informática para tomar decisiones objetivas y acertadas en cuestiones de costos, beneficios y nivel de seguridad implementada. Además, Azzets permitirá identificar cuáles son los departamentos y activos con mayor exposición y necesidad de invertir en nuevos controles. A corto y a largo plazo, Azzets permitirá ahorrar y prevenir pérdidas operacionales y monetarias a los procesos neurálgicos del negocio.

En resumen, Azzets brindará una excelente herramienta para generar y capitalizar ventajas competitivas desde la seguridad integral de la información, activos y procesos del negocio. Volviendo a los inicios de este proyecto, la pregunta precursora de Azzets era la siguiente: ¿convendría desarrollar un sistema, sin precedentes en el mercado, que permita gestionar los activos de información y mejorar la toma de decisiones y la eficiencia de los controles? Según lo expuesto en este trabajo, las ventajas provistas por Azzets son sin duda sólidas y oportunas.

Anexo A: Estudio del Mercado

Se realizó una investigación sobre los productos disponibles en el mercado que estén enfocados en la gestión de activos de información. Se ha encontrado una gran cantidad de productos y son detallados a continuación.

InvGate

Es una herramienta centralizada y automática para el control de *software* y licencias, control de cambios y control remoto de los equipos. Su enfoque es operativo, automatiza muchas tareas en la gestión de activos y reduce sus duraciones [6]. No maneja una gestión de riesgos ni controles. Hay muchísimos productos similares de todas las formas y tamaños.

IBM OpenPages

Es una solución corporativa de GRC [7], la cual permite adaptarse a cualquier metodología de gestión de riesgos. Incluye módulos para la gestión financiera de controles, gestión de riesgos operacionales, cumplimiento de regulaciones, normas y estándares, aplicación de políticas, gestión de riesgos de proveedores y evidencias para la auditoría interna. No provee gestión de activos.

FulcrumWay Integrated GRC Management

Es una plataforma para realizar una gestión de GRC integrada en toda una organización [8]. Incluye gestión de riesgos, controles, controles de acceso, regulaciones y estándares. El producto está compuesto por un servidor de gestión de contenido, centralización de documentos y flujos de trabajo. No incluye una gestión de activos de información ni su catalogación ni un inventario centralizado.

Oracle Enterprise GRC Application Suite

Es una plataforma de gestión de GRC [9]. Tiene prestaciones similares a otros gestores de GRC e incluye una variedad de tecnologías para hacer cumplir las políticas. No posee una gestión de activos.

TeamConnect GRC

Es otra plataforma de gestión de GRC [10]; provee mucha funcionalidad para la aplicación de políticas, procedimientos, investigaciones internas, prevención de pérdida de información, etc. No posee una gestión de activos.

Maclear GRC

Es una plataforma de gestión integral de GRC [11] diseñada en módulos funcionales, como implementación de políticas y su cumplimiento, gestión de riesgos, gestión de activos, gestión de proveedores y planificación para la continuidad del negocio.

PILAR

Es una herramienta GRC basada en la metodología MAGERIT para la gestión de riesgos [12]. Es una herramienta muy potente y muy completa para gestionar los activos de información. Es una de las herramientas más potentes halladas durante la investigación. Permite la gestión de activos, riesgos, costos de controles, plan de continuidad de negocio, cumplimiento con algunas normas y estándares.

Algunas desventajas halladas al implementar PILAR son:

- La herramienta es paga y cuesta 1500 euros e incluye garantía de defectos por un año y derecho a las actualizaciones de la misma versión por un año.
- Todos los años se debe renovar la licencia pagando el 15% de su valor. Esto implica un costo inicial y un costo de renovación.
- El soporte a una base de datos no está incluida y debe pagarse con 500 euros más. Esto eleva el costo de renovación anual. El soporte por base de datos se hace casi crucial para poder gestionar un repositorio centralizado de la base de conocimiento, la realización de backups y soporte para múltiples usuarios concurrentes. Una herramienta como esta quizás deba ser mantenida por más de una persona, lo cual requiere de una base de datos centralizada.

- Si se debe usar en más de una máquina se debe pagar otra licencia.
- La interfaz gráfica y el look and feel no es la mejor y por momentos no es intuitiva.
- El sistema está ligado al diseño realizado por los autores, por lo que no hay ningún tipo de customización según necesidades puntuales.

Cuadro comparativo

Se realizó un cuadro comparativo y se puede observar claramente que todos los productos abarcan necesidades complementarias.

Funcionalidad	InvGate	Open Pages	Fulcrum Way	Oracle GRC	Team Connect	Maclear	Pilar	Azzets
Control de cambios de SW	✓	×	×	×	×	×	×	×
Gestión de planes de licencias	✓	×	×	×	×	×	×	×
Regulaciones y estándares	×	✓	✓	✓	✓	✓	✓	×
Inventario de activos	✓	✓	✓	✓	✓	✓	✓	✓
Gestión de información financiera	✓	✓	✓	✓	×	✓	✓	✓
Interdependencias de activos	×	×	×	×	×	×	✓	✓
Plan de continuidad	×	×	×	×	✓	✓	✓	✓
Situaciones departamentales	×	×	×	×	×	×	×	✓
Gestión de riesgos	×	✓	✓	✓	✓	✓	✓	✓
Gestión de controles aplicados	×	✓	✓	✓	✓	✓	✓	✓
Escenarios para la incorporación de nuevos controles	×	×	×	×	×	×	✓	✓
Histórico de incidentes	×	×	×	×	×	×	×	✓
Mapa integral de riesgos	×	×	×	×	×	×	×	✓

Azzets es una herramienta especialmente diseñada para la gestión de activos, sus riesgos, controles, plan de continuidad y estudio de viabilidad de futuros controles. Si bien hay muchos sistemas en el mercado que ofrezcan módulos para la gestión de activos, riesgos, controles y cumplimiento de políticas, Azzets es uno de los pocos que está enfocado de forma central y estratégica en la gestión de activos. Varios sistemas mantienen un inventario de activos pero no gestionan sus riesgos. Otros sistemas ofrecen una plataforma muy grande incluyendo muchísima funcionalidad.

Azzets permite gestionar de forma integral los activos de forma ágil y sin requerir de un sistema de gran tamaño y envergadura. Además, permite un valor agregado con respecto a su enfoque departamental de los activos de información, su clasificación en mapas integrales de riesgo, análisis de controles en distintos escenarios y el repositorio de incidentes de cada activo.

La mejor herramienta hallada durante la investigación es PILAR sin embargo presenta algunas desventajas. A continuación se listan sus desventajas y se la compara con Azzets:

Aspecto	PILAR	Azzets
Licencia	Se debe pagar el costo inicial y una renovación anual. Tiene costos de mantenimiento anuales	Se debe invertir en el proyecto y el código fuente quedará disponible para su modificación en el futuro. No hay pagos de licencias
Uso de base de datos	Se debe pagar aparte	Ya está integrado dentro de la solución
Implantación	Se debe instalar y configurar en cada equipo. Se requiere permisos de administrador.	Se instala únicamente en un servidor. Se accede vía web con cualquier navegador.
Usuarios concurrentes	Pensado más para equipos standalone	Concurrencia manejada de forma integrada desde el servidor web y la base de datos
Necesidades específicas	Se debe amoldar a lo ofrecido por PILAR ya que es estático	Es dinámico y se pueden tomar necesidades particulares para enriquecer el sistema.
Base de conocimiento de incidentes	No tiene un registro de incidentes.	Permite registrar por cada activo los incidentes que sufrió y la duración de la demora que causó. Será una herramienta importante para buscar problemas, es decir, incidentes recurrentes causados por un problema todavía no resuelto.

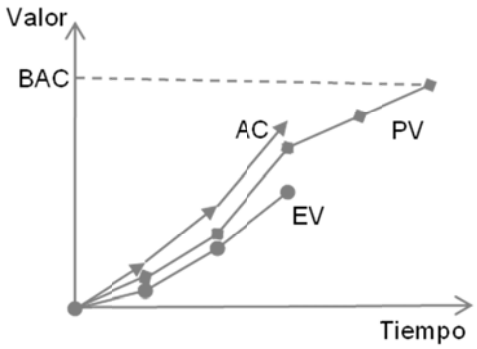
Anexo B: Earned Value

En este anexo se describirá en detalle la herramienta de EV.

Métricas de avance

A continuación se detallan algunos conceptos básicos del EV:

- **PV (*Planned Value*)**: Valor planificado. Es el valor acumulado que se espera tener en cada etapa de un proyecto.
- **AC (*Actual Cost*)**: Costos actuales. Son los costos incurridos y acumulados en una etapa específica.
- **EV (*Earned Value*)**: Valor ganado. Es el valor ganado y acumulado hasta la fecha incluyendo tareas finalizadas y ya comenzadas.
- **BAC (*Budget at Completion*)**: Presupuesto al finalizar. Es el PV al finalizar el proyecto, es decir, el valor máximo a ganar durante todo el proyecto.

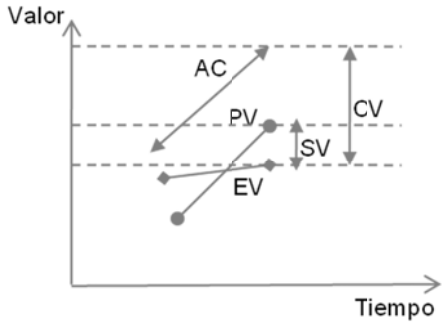


Métricas de desvío a corto plazo

El EV tiene dos tipos de varianzas según lo planificado: según el tiempo y según los costos.

- **CV (*Cost Variance*)**: Varianza de costos. Mide en una etapa específica la diferencia entre el valor ganado y los costos actuales. Se calcula como CV = EV – AC. Si CV es positiva, el desvío representa que los costos están por debajo de lo previsto. Si CV es negativa, los costos superan lo previsto.
- **SV (*Schedule Variance*)**: Varianza de calendario. Mide en una etapa específica la diferencia entre el valor ganado y el valor ganado

planificado. Se calcula como SV = EV – PV. Si SV es positiva, el desvío representa que se ha tardado menos tiempo de lo previsto. Si SV es negativa, se ha tardado más de lo previsto.



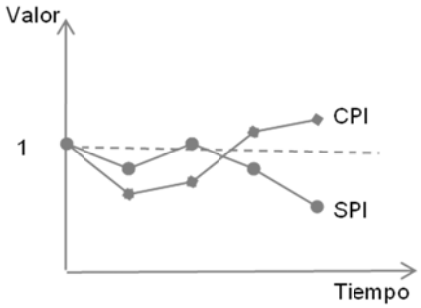
Métricas de rendimiento

Los desvíos por costos (CV) y por calendario (SV) permiten calcular unas métricas de rendimiento en ambas dimensiones:

- **CPI (*Cost Performance Index*)**: Índice de rendimiento de costos. Mide el rendimiento en la inversión de recursos en el proyecto. Se calcula como CPI = EV / AC. Si el CPI es mayor o igual a uno, la eficiencia en la utilización de recursos es buena. Si el CPI es menor a uno, la eficiencia en la utilización de recursos es mala.

- **SPI (*Schedule Performance Index*)**: Índice de rendimiento de calendario. Mide el rendimiento en la utilización del tiempo en el proyecto. Se calcula como SPI = EV / PV. Si el SPI es mayor o igual a uno, la eficiencia en la utilización del tiempo es mejor a la prevista. Si el SPI es menor a uno, la eficiencia en la utilización del tiempo es mala.

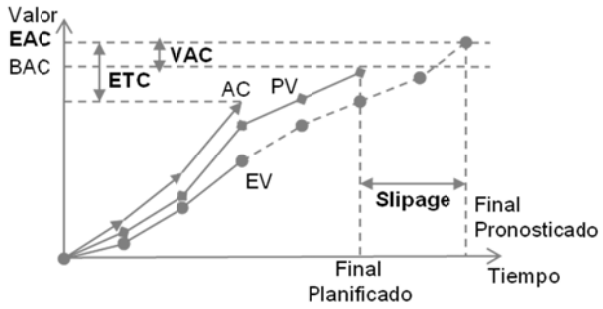
Ambos índices podrán ser graficados en un histórico para comparar la evolución en el rendimiento en el proyecto.



Métricas de desvío a largo plazo

Existen otras métricas más que permiten pronosticar el desvío total en costos y calendario al finalizar el proyecto.

- **EAC (*Estimate At Completion*)**: Estimación de costos al completar. Es el pronóstico de cuantos costos incurridos se realizarán al finalizar el proyecto. Su cálculo depende de la evolución en el BAC:
  - Si no hay variación del BAC se prevé continuar con el mismo rendimiento de costos (CPI). Se calcula como EAC = BAC / CPI.
  - Si el BAC original estaba muy desviado, se calcula como EAC = AC + ETC.
  - Si las variaciones actuales del BAC no se van a mantener en el futuro, se calcula como EAC = AC + (BAC - EV).
  - Si las variaciones actuales del BAC se van a mantener en el futuro, se calcula como EAC = AC + (BAC -EV) / CPI.
- **VAC (*Variance At Completion*)**: Varianza total de costos. Mide la diferencia entre los costos totales planificados del proyecto y los stos pronosticados al cierre del proyecto. Se calcula como VAC = BAC – EAC. Si VAC es positiva, el proyecto gastará menos de lo planificado. Si VAC es negativa, se gastará más del presupuesto asignado al proyecto.
- **ETC (*Estimate To Complete*)**: Estimación de costos que faltan incurrir para completar el proyecto. Mide la diferencia entre el costo total estimado del proyecto (EAC) y los costos acumulados hasta el momento (AC). Se calcula como ETC = EAC – AC.
- ***Slipage***: Desvío total del calendario. Mide cuánto se retrasará o adelantará la finalización del proyecto con respecto a la fecha de finalización estipulada. Se calcula como la diferencia entre la fecha pronosticada de finalización y la fecha de finalización planificada.


Valor
EAC
BAC
VAC
ETC
AC
PV
EV
Slipage
Final
Pronosticado
Final
Planificado
Tiempo

Bibliografía

[1] ISO 27002
Título: ISO 27002
Autor: ISO
Publicación: 11 de noviembre
Link: http://www.27000.org/iso-27002.htm

[2] MAGERIT
Título: MAGERIT Versión 2
Autor: Ministerio de Administraciones Públicas de España
Publicación: 11 de noviembre
Link: http://www.csi.map.es/csi/pg5m20.htm

[3] WBS
Título: WBS – Herramienta de comunicación del trabajo a realizar en un proyecto
Autor: Dora Ariza
Publicación: 3 de abril de 2011
Link: http://www.acis.org.co/geproyinfo/?p=44

[4] Earned Value
Título: Seguimiento del Proyecto mediante Earned Value
Autor: Joaquín Ibañez
Publicación: 3 de abril de 2011
Link:http://www.liderdeproyecto.com/manual/seguimiento_del_proyecto_mediante_earned_value.html

[5] PMBoK
Título: PMBoK Guide
Autor: Project Management Institute (PMI)
Publicación: 3 de marzo de 2011
Link: http://www.pmi.org/PMBOK-Guide-and-Standards.aspx

[6] InvGate
Producto cuyo website es: http://www.invgate.com

[7] IBM Open Pages
Producto cuyo website es:
http://www.openpages.com/solutions/governance_risk_compliance_management_solutions.asp

[8] Fulcrumway GRC
Producto cuyo website es: http://www.fulcrumway.com/solutions/integrated-grc-management

[9] Oracle GRC
Producto cuyo website es:
http://www.oracle.com/us/solutions/corporate-governance/grc-manager/index.html

[10] TeamConnect GRC
Producto cuyo website es: http://www.mitratech.com/teamconnect-grc

[11] Maclear GRC
Producto cuyo website es: http://maclear-grc.com/grc_solutions.html

[12] Pilar GRC
Producto cuyo website es: http://www.ar-tools.com/tools/pilar/index.html