“SEGURIDAD, ESTANDARIZACIÓN, OBJETIVOS DE CONTROL Y SU CUANTIFICACIÓN ECONÓMICA PARA EL SISTEMA TRANSACCIONAL DE GESTIÓN PRESUPUESTARIA GEPRE – UNCUYO, EN EL MARCO DE LA GESTIÓN DE CALIDAD”

Prof. Asociado a/c Carlos Masselli,
Auditoría Operativa y de Sistemas Computarizados.
Lic y Prof Daniel Cavaller JTP (Adsc).

Introducción:

El crecimiento casi exponencial de los clientes, flujos de datos, tiempos de uso y servicios para los sistemas transaccionales de gestión presupuestaria en la intranet/extranet de la Universidad hace indispensable pensar, a lo menos desde hace más de un quinquenio, se adjudiquen gran parte de los esfuerzos y dineros institucionales a tareas de clasificación, jerarquización y almacenamiento de éste. Así mismo se ha de considerar como uno de los activos con gran valor agregado a la disponibilidad del sistema transaccional para la gestión presupuestaria de la UNCuyo “GEPRE” y como consecuencia del anterior trabajo, respecto a los accesos indebidos y caídas de la seguridad en la intranet de la Facultad de Ciencias Económicas. Aunque con tal crecimiento y auge por el uso de NTIC[i] en la UNCuyo no se ha acompañado el desarrollo de un plan de contingencias ni siquiera establecida una matriz de riesgos que denote las áreas de función de informática susceptibles y por tanto no existe un plan de auditoria. En este sentido no se pretende activar una auditoria en particular sino iniciar una investigación que dispare en un marco más amplio un plan general de auditoria sustentable bajo las normas y estándares de calidad IRAM-ISO 17799 y los objetivos de control para la información y tecnología afines CoBiT. En especial contestar a la pregunta ¿cuál es el coste, para la UNCuyo, por la no estandarización y/o expresión de los objetivos de control en materia de seguridad de seguridad, caídas de servicio y de sistema, etc., en las áreas funcionales en contacto a través de la red?

El marco del trabajo:

Nos definimos en el marco de la Teoría General de Sistemas y centramos nuestros esfuerzos en gestionar con calidad dentro del modelo incremental adaptativo de calidad de Böhem, trabajando especialmente sobre CoBiT e IRAM/ISO 17799.

El objetivo:

Relevar, clasificar y analizar los riesgos de seguridad inherentes al sistema transaccional para la gestión presupuestaria y en concordancia con las áreas funcionales informatizadas en contacto en la red de la UNCuyo, que sufren o son susceptibles de riesgos, a fin de poder establecer una cuantificación económica para dichos escenarios.

Los antecedentes:

No posee en el ámbito de la UNCuyo.

La originalidad e importancia

La propuesta se desarrolla en base a los siguientes ejes:

Central: releva (históricamente, si es posible) y establece un formato y posterior modelo de evaluación económico-financiero de las afectaciones sobre seguridad en el sistema transaccional de gestión presupuestaria GEPRE para la UNCuyo.

Periféricos: capacita a alumnos avanzados de la asignatura Auditoria Operativa y de Sistemas Computarizados a través de la participación en un caso real sobre un sistema transaccional para la gestión presupuestaria. Adecuación de métodos y técnicas para efectivizar logros en este sentido. Aplicación de formatos y sistemas de medición con el fin

de revisar los impactos en un periodo de tiempo acordado para la evolución del proyecto. Desarrollo específico de métodos y técnicas aplicables a cada uno de los casos tipificados. Estructuración y automatización de éstas. Desarrollo de software. Diseño de la matriz de indicadores, relevamiento y procesamiento de los mismos. Proyección de un plan de contingencias y de un plan de auditoria coincidente con la funcionalidad del recurso de gestión para la UNCuyo. Publicación de resultados, tanto en Jornadas de Ciencias Económicas como en las de Auditoria en Informática.

Actividades y metodología:

Se tasan los riesgos del sistema: identificando, clasificando, midiendo, y estableciendo un plan de acción contra riesgos y su aceptación, al respaldar por medio de un proceso formal de trabajo con técnicas y herramientas propias de la auditoría: justificación, adecuación, formalización, desarrollo e implantación. Aplicando técnicas de: análisis, diseño, costeo, modelado de datos y procesos, documentación, entrevistas, cuestionarios, etc.

Además, se releva una historia de eventos o sucesos acaecidos desde la puesta en marcha de la intranet e internet de la UNCuyo del sistema de gestión presupuestaria GEPRE, pesquisando, analizando y adjudicando causas, efectos e impactos económicos. Desarrollo de un historial de soluciones o implementaciones. Diseño de la matriz de indicadores, modelado y análisis factorial estadístico sobre el escenario acordado.

¿Qué es GEPRE?

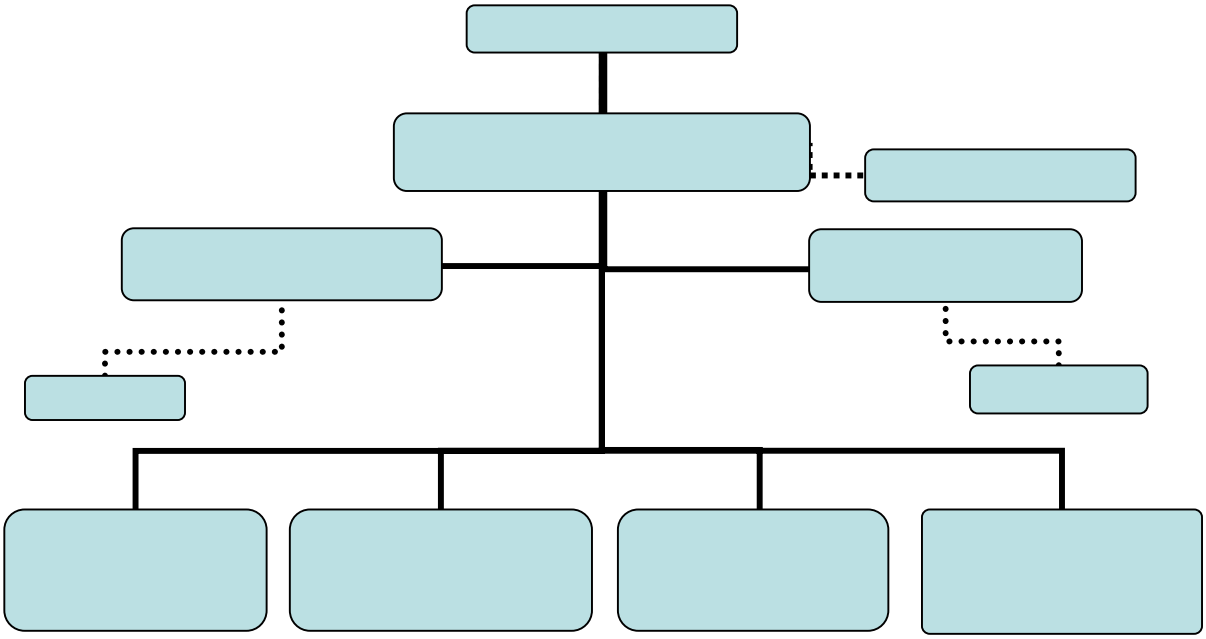
Actividad 1. Dominio – Alcance y Límites

Sus siglas corresponden a al las del sistema de gestión presupuestaria, GEPRE es un meta sistema de información de ambiente colaborativo, que cuenta con un conjunto de subsistemas a nivel de la capa transaccional de la UNCuyo, que aportan datos a la base de datos de la organización, así mismo GEPRE de vale de otro conjunto de subsistemas de información en cuyo nivel transaccional aportan a bases de datos propietarias de éstos, como ser: SIU COMENCHINGONES, SIU PAMPA, etc. En este primer nivel GEPRE consolida datos y coadyuva a la organización exponiendo los mismos bajo el modelo comunicacional a fin de que todos los actores (usuarios responsables, para el sistema), puedan presupuestar por actividad.

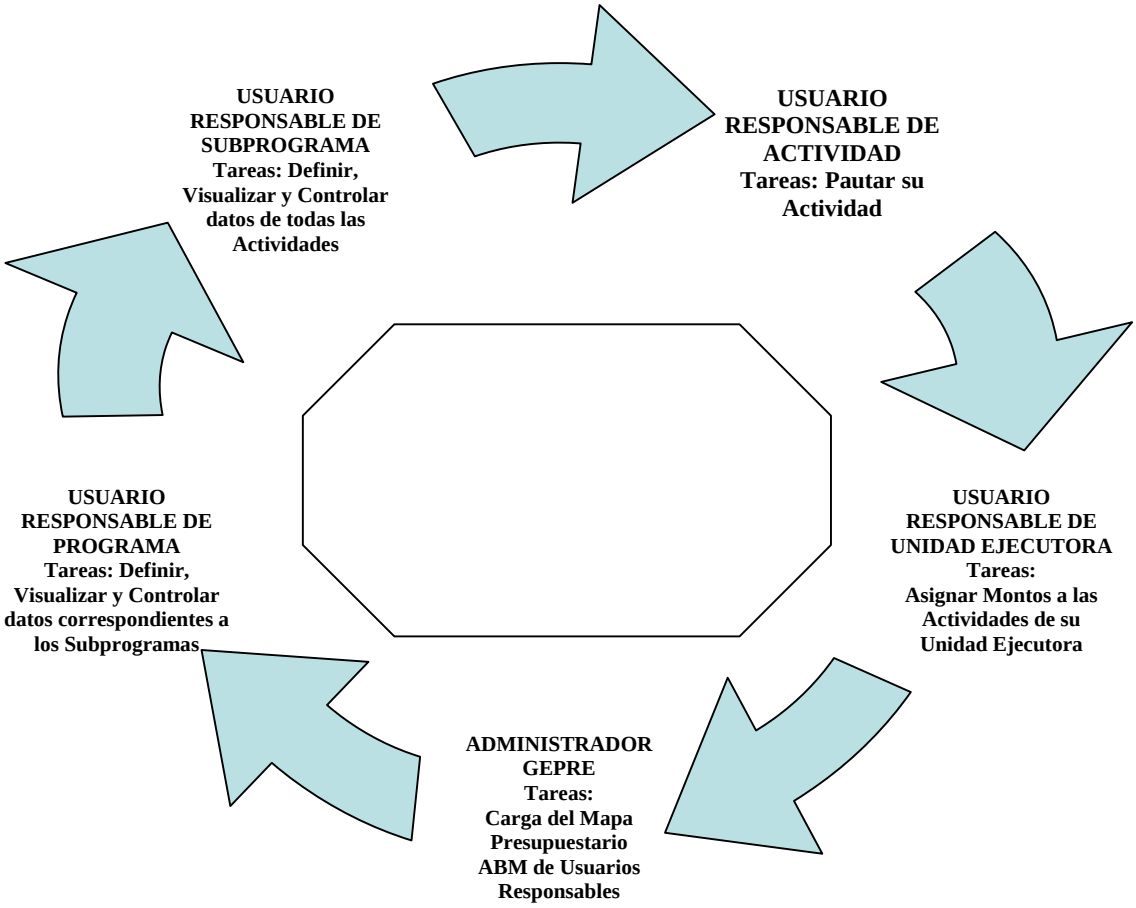
El añadido de inteligencia, ha permitido que GEPRE se posicione como un Sistema de Soporte para la toma de Decisiones, lo cual conlleva a GEPRE, el poder emitir un conjunto de reportes que dan como resultado la ordenanza de presupuesto de la UNCuyo. También se obtiene un conjunto no estrictamente definido de consultas y seguimiento de datos, valores y usuarios responsables sindicados para este propósito. La versión dos del sistema contempla la expresión de indicadores, que permitan concretar un proceso de presupuestación y posterior control y gestión mas objetivo. GEPRE cuenta con más de 500 usuarios responsables (UR); supera las 10.000 líneas de código, se soporta sobre una plataforma de producción (PP, servidor situado físicamente en el CICUNC); cuenta con un servicio de intranet e Internet para el acceso remoto de todos sus usuarios, un equipo de asesores de presupuesto, análisis, programación, diseño, mantenimiento y atención específica a usuarios (capacitadotes) por medio de pasantes.

GEPRE, como todo sistema informacional aceptado y desarrollado mediante la aplicación de NTIC, está cambiando la cultura organizacional de la UNCuyo, tornándola más flexible, dinámica, también nos gustaría decir: más democrática.

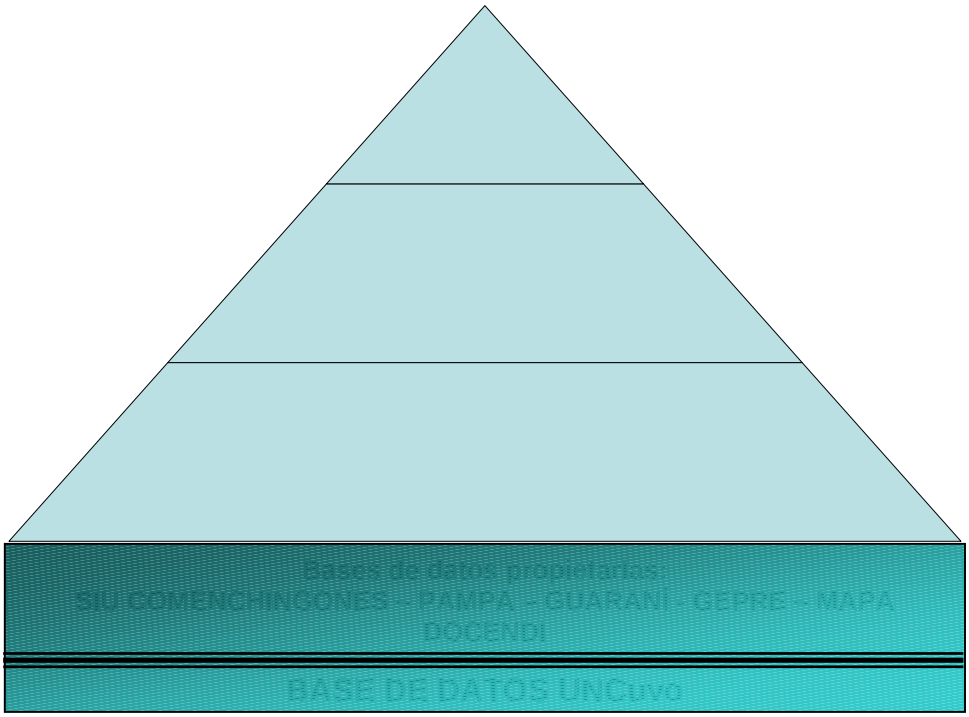
¿Cuál es su organigrama?



ESQUEMA DE FLUJO INFORMACIONAL



NIVELES INFORMACIONALES SIU - UNCuyo – GEPRE



¿Qué es COBiT?

El COBiT proporciona, en su marco referencial, un conjunto de herramientas dirigidas al propietario de procesos de la organización que le facilitan el cumplimiento de este rol.

Su fin es el de proporcionar la información que la organización necesita para alcanzar sus objetivos, los recursos de tecnología de información (TI) deben ser administraos por un conjunto de procesos de TI agrupados en forma natural[ii].

Presenta un conjunto de 34 objetivos de control de alto nivel (OC), destinados a cada uno de los procesos de TI: planeamiento, adquisición e implantación, entrega (de servicio) y seguimiento. La estructura precedente cubre todos los aspectos información y tecnológicos que se soportan en una organización.

En un orden más detallado, por cada uno de los 34 objetivos de control, de alto nivel, se favorece una guía de auditoría o aseguramiento que permite la revisión de los procesos en 302 OC, detallados, proporcionando así a la gerencia la certeza de cumplimiento y/o recomendaciones para la mejora.

Se compone de un resumen ejecutivo (RE), destinado a la alta gerencia cuya finalidad es dar luz y sensibilizar sobre los principios y conceptos fundamentales de CoBIT. La guía cuenta con dos herramientas: el Diagnóstico de Sensibilización Gerencial[iii] y el Diagnóstico de Control en TI[iv], ligados al asesoramiento y asistencia en el análisis ambiental de control de una organización.}

EL marco referencial:

En éste se da especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de la organización sobre: efectividad, eficacia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que se han de satisfacer. Aquí mismo se dan las definiciones para los requerimientos de la organización que derivaron de los objetivos de control superiores respecto a calidad y reportes fiduciarios relativos a tecnología de información. COBiT se orienta como herramienta de gobierno de TI cuyo fin es el entendimiento y la administración de riesgos asociados con la tecnología de información y

sus tecnologías adyacentes. La siguiente figura describe los procesos de IT de CoBIT, que se encuentran definidos dentro de los cuatro dominios, expresados anteriormente.

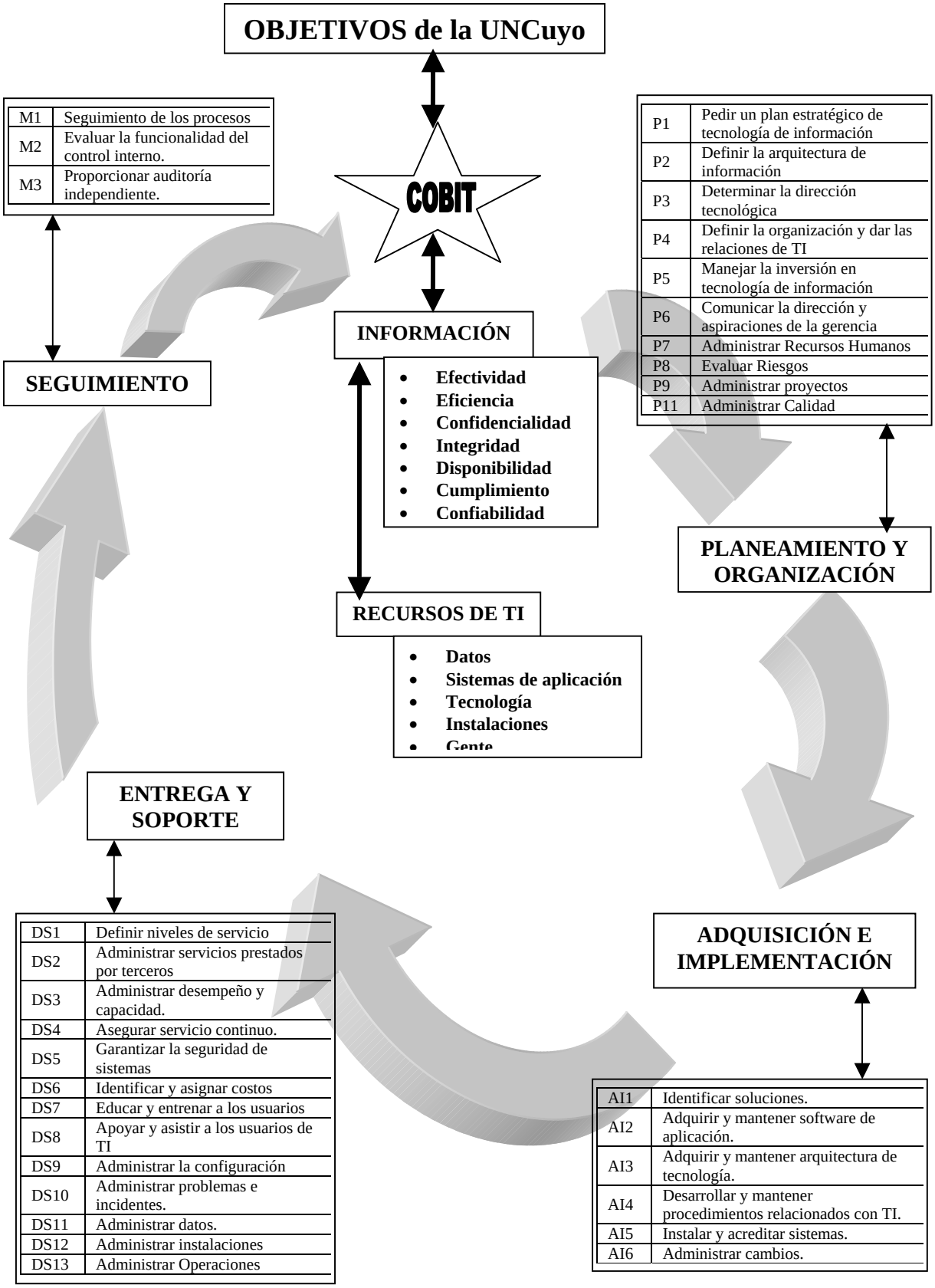


Fig. 1.- Procesos de IT en COBIT definidos dentro de los Cuadros de Dominios[v].

La necesidad del control en tecnología de información puede resumirse en los siguientes tópicos críticos:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y amplio espectro de amenazas, tales como “cyber amenazas” y la guerra de la información.
- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de la información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Muchas organizaciones reconocen hoy los beneficios potenciales que la tecnología puede producir en ellas, sin embargo también comprenden y administran los riesgos asociados con la implementación de éstas. Por tanto, la administración es quién decide la inversión razonable en seguridad y control de Ti y tiende a lograr un balance entre riesgos e inversiones en control para un ambiente de TI frecuentemente impredecible. Una creciente necesidad por parte de la comunidad de USUARIOS de TIC[vi] respecto a la seguridad en dichos servicios, mediante a acreditación y auditoría desarrollada de forma interna o mediante terceros, que aseguren adecuados controles, es confusa, al momento de ser implementada, ya que existen, actualmente, tanto ara entidades no gubernamentales como gubernamentales y empresas, diferentes métodos: ITSEC, TCSEC, ISO9000, COSO, etc.

De una serie de pesquisas, se ha determinado la posibilidad de contar con los estándares actualizados, a la IRAM/ISO 17799, ellos corresponden a: 20001/2 de mayo de 2005. Por lo que se ha preferido utilizar la metodología MAGERIT, enmarcada dentro de los nuevos estándares.

¿Qué es MAGERIT?

MAGERIT[vii]: Análisis y gestión de riesgos de los sistemas de información

El Consejo Superior de Informática de España, ha elaborado la metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT, como se muestra en la figura 2. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes, pero que también dan lugar a ciertos riesgos que deben minimizarse con medidas que garanticen la seguridad y generen confianza en la utilización de estos medios.

El ciclo de gestión de la seguridad siempre establece como primera etapa el análisis y la gestión de los riesgos del sistema que tratamos de proteger. Para una correcta definición e implantación de la seguridad, es necesario identificar y determinar los diferentes elementos significativos dentro del entorno de la seguridad de los sistemas de información.

Elementos de MAGERIT

A continuación se definen los elementos considerados significativos observados por MAGERIT para el estudio de la seguridad en sistemas de información.

- ***Activos***: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.
- ***Amenazas***: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- ***Vulnerabilidad de un activo***: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- ***Impacto en un activo***: consecuencia sobre éste de la materialización de una amenaza.
- ***Riesgo***: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

- ***Servicio de salvaguarda***: acción que reduce el riesgo.
- ***Mecanismo de salvaguarda***: procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

La figura 3 muestra los elementos y sus interrelaciones:

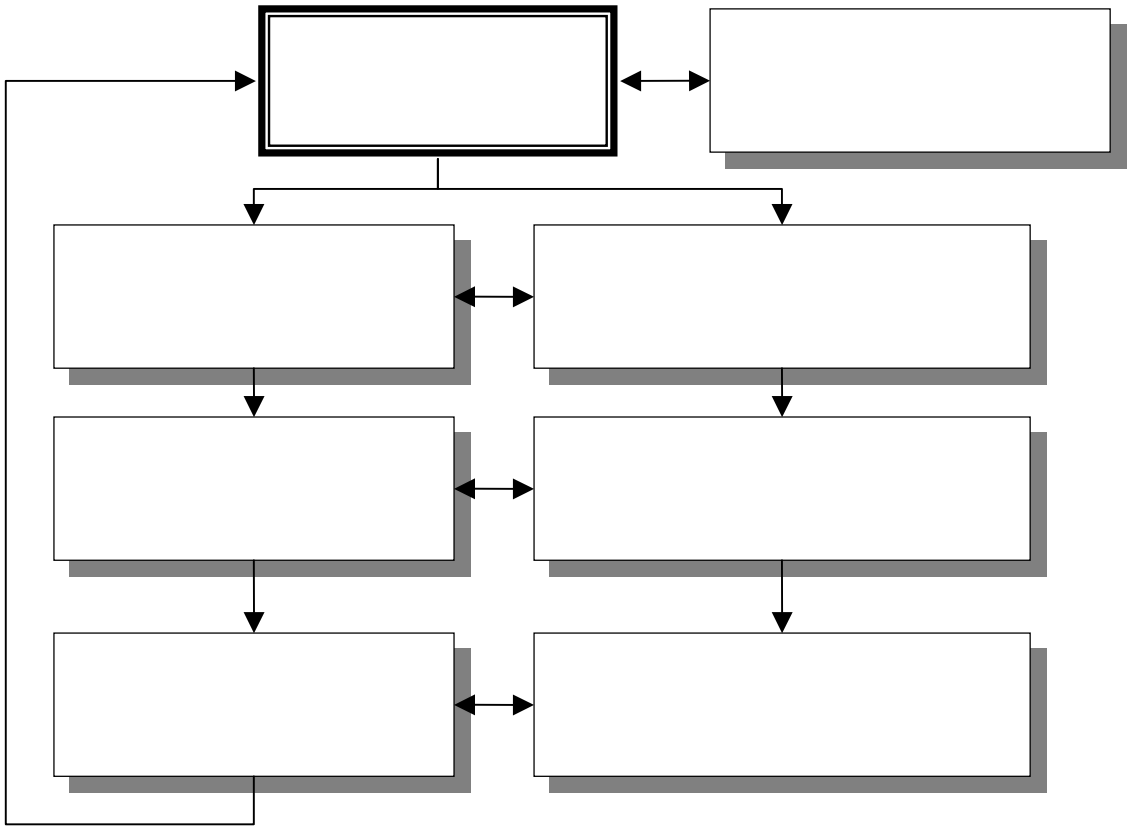


Fig. 2.- Esquema del análisis y gestión de riesgos según MAGERIT

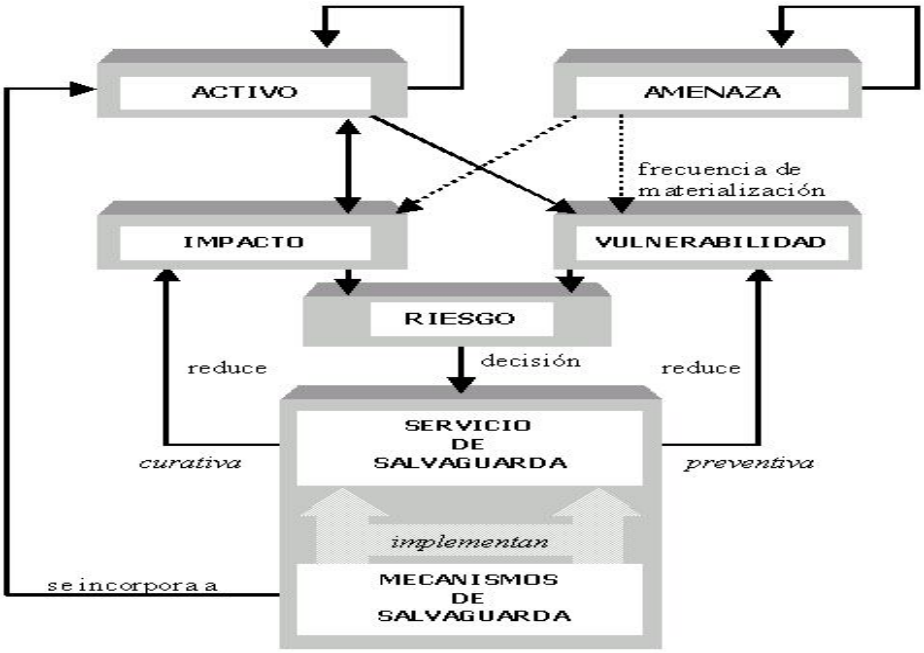


Fig. 3.- Descripción del proceso de análisis y gestión de riesgos

En el proceso de análisis y gestión de riesgos de la seguridad en los sistemas de información podemos identificar las siguientes etapas:

- **Planificación:** en esta fase, se establece el objetivo del proyecto, el dominio de estudio y las restricciones generales. Deben también definirse las métricas con las que se valorarán los diferentes elementos de seguridad, de manera que los resultados finales de medición del riesgo sean definidos en función de los parámetros adecuados para cuantificar el riesgo por la organización (por ejemplo, definir la escala de frecuencias para medir la vulnerabilidad, definir las cantidades monetarias por las que cuantificar el impacto).
- **Análisis de riesgos:** una vez definido el dominio, los analistas de riesgos procederán a realizar las entrevistas al personal de la organización para la obtención de información. En esta fase se identificarán los activos de la organización, identificando las relaciones que se establecen entre activos. De esta forma se obtiene el "árbol de activos" que representan las distintas dependencias y relaciones entre activos, es decir, todos aquellos elementos que están "encadenados entre sí" en términos de seguridad. También se identifica el conjunto de amenazas, estableciendo para cada activo, cuál es la vulnerabilidad que presenta frente a dicha amenaza. Además, se cuantifica el impacto, para el caso en el que la amenaza se materializase. Dado que los activos se encuentran jerarquizados y se encuentran establecidas las relaciones de dependencia entre los activos de las diferentes categorías, hemos conseguido de forma explicita documentar la "cadena de fallo" en caso de un incidente de seguridad. La experiencia y la sucesiva revisión de la información generada en estudios de riesgos anteriores permitirán ajustar de forma más exacta las diferentes dependencias entre activos. Con toda esta información, tendremos una estimación del costo que podría producir la materialización de una amenaza sobre un activo. Teniendo en cuenta las relaciones funcionales y de dependencias entre activos, se hallan los valores de riesgo.
- **Gestión de riesgos:** en esta fase, se procede a la interpretación del riesgo. Una vez identificados los puntos débiles, debe seleccionarse el conjunto de funciones de salvaguarda que podrían ser usados para disminuir los niveles de riesgo a los valores deseados. Para ello, deberán especificarse los mecanismos de salvaguarda que se encuentran implantados hasta ese momento y cuál es su grado de cumplimiento.

  Este proceso es ayudado por la simulación. Se van probando selecciones de diferentes mecanismos de salvaguarda y se estudia en qué medida reducen los niveles de riesgo a los márgenes deseados. Es muy importante realizar las correctas estimaciones de la efectividad de los diferentes mecanismos de salvaguarda para ajustar de forma precisa los valores de riesgo.
- **Selección de mecanismos de salvaguarda:** una vez obtenidos estos resultados, se establecen de nuevo reuniones con el equipo responsable del proyecto de la organización en estudio. De esta forma, se analizan los resultados obtenidos y se establece un plan de implantación de mecanismos.

Diferencias entre la auditoria informática y el análisis y gestión de riesgos

Podemos establecer básicamente las siguientes diferencias entre ambas tareas:

- La auditoria informática es un proceso de revisión e inventariado.
- El análisis y gestión de riesgos es un proceso de diagnóstico y detección.

Lo usual es usar la auditoria informática como información de retroalimentación, para analizar en qué medida el sistema garantiza la seguridad informática, pero no ofrece una visión general del sistema, sólo puede detectar puntos de fallo concretos sobre cada activo.

El análisis y gestión de riesgos nos aporta mucha más información sobre el sistema. Identifica las relaciones funcionales entre los distintos activos de información, analiza todas las posibles contingencias que pueden presentarse. De alguna forma, delimita y establece

en contexto de seguridad en el que se encuentra el sistema de información, pudiendo con esta información elegir de forma más precisa las herramientas de seguridad necesarias para garantizar los requisitos de seguridad deseados sobre nuestro sistema. La auditoría necesita completar un proceso de planificación y ejecución de tareas para luego emitir la opinión. En todos los casos el proceso de auditoría necesita identificar los riesgos involucrados para poder definir los distintos procedimientos a aplicar. Generalmente esta identificación de los riesgos consiste en la lectura de los diversos factores de riesgo involucrados.

Análisis preliminar

Por lo anterior se trata de ilustrar de una forma sencilla en qué consiste el proceso de análisis y gestión de riesgos descrito por la metodología MAGERIT. Por desgracia, la velocidad a la que se están produciendo los cambios en la gestión de los sistemas de información, nos llevan a tratar de solucionar los problemas de la forma más rápida posible. Además se contempla cómo, en materia de seguridad informática, este fenómeno está produciendo en algunas organizaciones el descuido en la protección de sus activos. No se llega a entender que actualmente, gran parte del valor de una organización es la información que posee, y que estos activos deben ser protegidos con el preciado valor que tienen, aunque se trate de un elemento difícil de valorar económicamente. Si bien se está realizando un gran esfuerzo, tanto por parte de los profesionales de la informática, como por parte de los directivos de las distintas organizaciones por solucionar esta situación, ello nos lleva sin ninguna duda, a justificar de una forma más contundente la necesaria formalización de las tareas relativas a la seguridad de la información.

Fig. 4.- Procesos básicos del ciclo de seguridad

La Figura 4 muestra los procesos básicos de seguridad. La actual situación, debido a la velocidad de los cambios, sólo permite a muchas organizaciones realizar las tareas de implantación y revisión de los sistemas como su ciclo de seguridad informática.

Es necesario que las organizaciones dispongan de un área dedicada exclusivamente a la seguridad de la información, y es necesario analizar y diseñar adecuadamente los sistemas de información para que garanticen los requisitos de protección de los activos que se manejan. Para ello, la concienciación de los altos directivos en la importancia que tienen estas tareas es un primer paso, y son ellos quienes deben establecer los requisitos de seguridad de los sistemas de información que manejan. Esta parte formal de la seguridad, es necesaria para realizar diseños de arquitecturas y selección de mecanismos de seguridad coherentes con la política de seguridad de la organización por parte del área técnica.

Sin duda, la fase de análisis y gestión de riesgos aporta una información muy útil, tanto a altos directivos que pueden conocer de forma más precisa cuál es el entorno de su sistema de información y por tanto tomar mejores decisiones como a las áreas técnicas, a las que proporciona medios de diagnóstico de sistemas, pudiendo seleccionar los mecanismos de salvaguarda que optimicen la inversión en seguridad informática con la que se dote a la organización en su presupuesto.

¿Cómo identificar y analizar los activos de GEPRE?

Actividad 2: Identificación y agrupación de ACTIVOS

Descripción y objetivo:

En la etapa de definición del dominio se describieron las funciones que realiza el sistema, ponderadas además según su importancia para cumplir con la misión de la organización. El objetivo de esta actividad fue el de reconocer los activos que componen los procesos, y definir las dependencias entre ambos. Así y a partir de la información recopilada en la actividad anterior, esta actividad profundiza el estudio de los activos con vistas a obtener la información necesaria para realizar las estimaciones del riesgo.

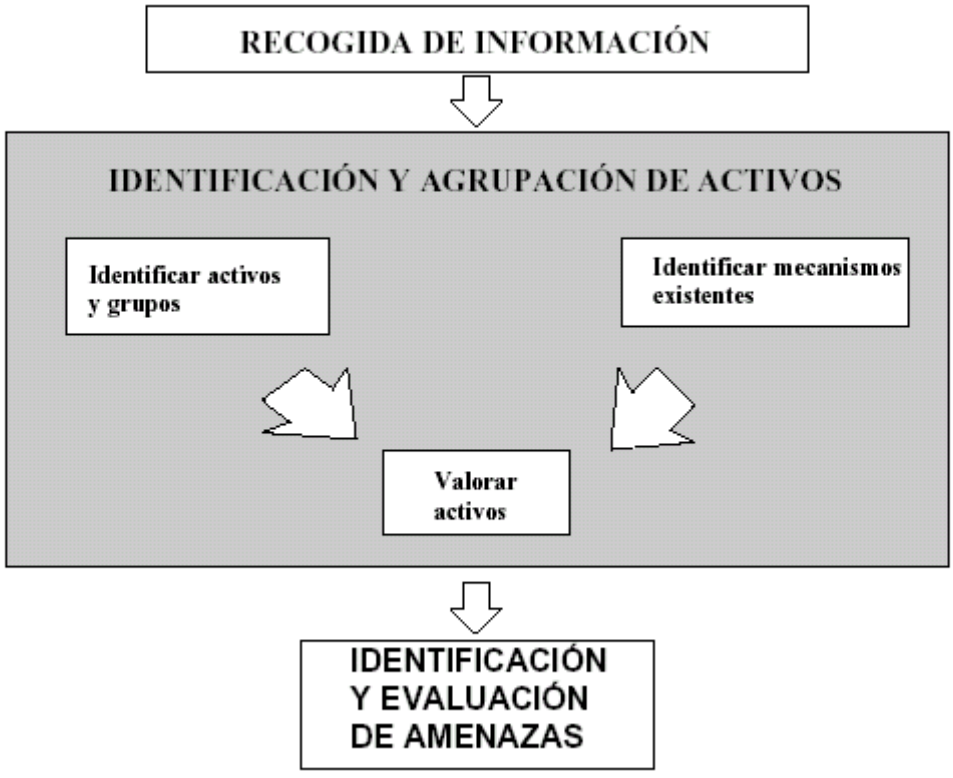


Fig. 5.- Esquema de proceso para identificar, agrupar y evaluar activos y amenazas

El objetivo de esta tarea es identificar los activos que componen el dominio, determinando sus características, atributos y clasificación en los tipos determinados en el submodelo de Elementos de MAGERIT. Una buena identificación es importante, pues de ella depende que sea más o menos fácil realizar todo el proceso posterior.

Tarea 1: Identificar activos y grupos de activos en GEPRE

Descripción y objetivo:

Para gran parte de activos materiales y algunos inmateriales (los llamados inventariables), la tarea se concretó a partir de los correspondientes ***Inventarios (disponibles)*** valorados que se desarrollan para otros fines (por de pronto para la valoración anual del Patrimonio de la UNCuyo que forma parte obligatoria de toda Contabilidad General por partida doble). Esta valoración 'oficial' de muchos activos ayuda también para comenzar con la tarea que le sigue, centrada en, valorar los activos identificados por la tarea actualmente descrita.

La tarea clasifica los activos identificados según las tipologías ofrecidas por MAGERIT y los agrupa teniendo en cuenta una consideración principal de jerarquía organizativa y otras posibles consideraciones:

- subestados de seguridad (autenticación, confidencialidad, integridad, disponibilidad, referenciados brevemente como A-C-I-D);
- amenazas que los pueden atacar;
- salvaguardas que los pueden proteger.

La tarea se completó añadiendo en el registro de cada activo otros campos pertinentes para su tratamiento posterior: descripción, ubicación, responsable encargado, número o cantidad, etc.

La tarea agrupa activos articulándolos en conjuntos definidos por el objetivo común de realizar un tipo de función determinada (que a su vez es un componente de la misión del sistema). La agrupación de activos más práctica desde el punto de vista del análisis de riesgos los articula en los 5 niveles de capas considerados en el Submodelo de Elementos de MAGERIT:

1. entorno
2. sistema de información
3. información
4. funcionalidades de la organización
5. otros activos

Una cadena 'vertical' concreta o 'árbol de activos' tomados de estas capas, agrupa los activos afectables por el desencadenamiento potencial de una amenaza determinada. Por ejemplo, la amenaza de un ladrón aprovecha la vulnerabilidad de una puerta abierta en el despacho del director financiero por el personal de limpieza fuera del horario de trabajo para robar un PC (entorno, capa 1) con sus programas (sistema de información, capa 2), lo que desencadena una carencia (de información, capa 3) crítica para el mantenimiento de la organización (funcionalidades, capa 4). Aunque la información se pueda recomponer (preguntando a los bancos de datos con los que la organización opera) es inevitable la mala imagen causada y es posible el falseamiento de datos, sin mencionar el mal uso por revelación que puede resultar del robo del contenido, si ha sido intencionado (otros activos, capa 5).

Adicionalmente se preparó otro tipo de agrupación basada en la ***naturaleza*** de los activos, a fin de facilitar el estudio de los mecanismos de salvaguarda ya implantados o a implantar en aquéllos. Por ejemplo, un computador personal PC, que normalmente utiliza cualquier usuario responsable del sistema, se encuentra formado por varios activos como monitor, teclado, CPU, periféricos, sistema operativo, aplicaciones, datos, etc. y puede ser atacado en su conjunto por determinadas amenazas. Su seguridad requiere mecanismos de

salvaguarda adaptados individualmente a cada activo y colectivamente al PC en conjunto. Este tipo de agrupación de activos abarcó grandes áreas tradicionales como éstas:

- Información y datos.
- Hardware.
- Software operativo.
- Software de aplicación.
- Comunicaciones.
- Documentos.
- Equipamiento ambiental.
- Personal interno y externo.
- Infraestructura.
- Activos organizacionales.

Productos:

- Informe de los activos componentes del dominio y de sus agrupaciones jerárquicas (Ver ANEXO III[viii]).
- Definición de las dependencias entre activos, procesos y funciones en el dominio. (Ver ANEXO III).

Técnicas (expuestas en la Guía de Técnicas):

- Diagramas de Flujos de Datos (Ver ANEXO I).
- Técnicas matriciales. (Ver ANEXO IV y aplicación de la herramienta de software RISK2; ANEXO V).

CASO GEPRE

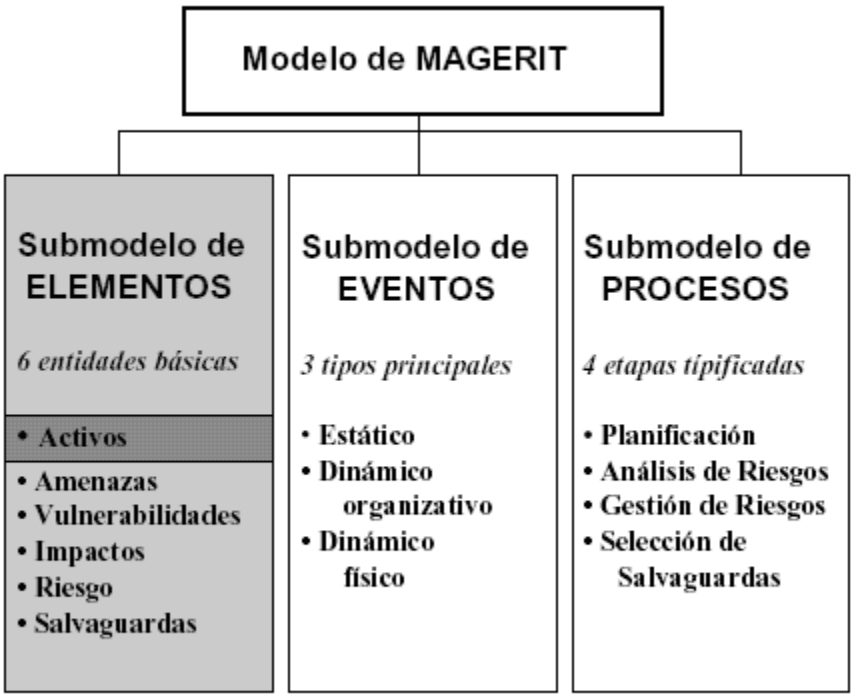


Fig. 6.- MAGERIT – aplicado a GEPRE

1.1 Definición

Los activos son los ***recursos*** *del* ***sistema de información o relacionados*** *con éste, necesarios para que la* ***organización funcione*** *correctamente y alcance los* ***objetivos*** *propuestos por su* ***dirección.***

MAGERIT no se circunscribe por tanto a la seguridad de los sistemas de información, pues no puede dejar de tenerse en cuenta que dichos sistemas afectan a la operativa correcta de los sistemas de organización (organizacionales) soportados, y que son afectados por las decisiones de la organización. Por tanto no tiene sentido hablar del sistema de información 'aislado' desde el punto de vista del riesgo.

Un proyecto de seguridad organizado con ayuda de MAGERIT tiene un 'objeto de seguridad' que se ejerce sobre un conjunto de activos que constituyen el 'objeto' en estudio o **dominio** del proyecto (un activo puede considerarse como un 'dominio unitario'). La delimitación de la frontera del conjunto de activos del dominio no impide considerar asimismo las relaciones en materia de seguridad de dichos activos con el **entorno** (todo lo situado fuera del dominio del proyecto que influye en él en términos de seguridad).

1.2 Características

Cada activo (o bien un conjunto homogéneo de activos, o bien el dominio en estudio) se caracteriza por su estado -en materia- **de seguridad;** estado que se concreta estimando los niveles de 4 ***subestados de autenticación, confidencialidad, integridad, disponibilidad (A-C-I-D),*** que MAGERIT define y valora con escalas sencillas que se definen en el apartado "1.5 Métricas", que se ve más adelante.

- **Subestado A de autenticación,** definido como la característica de dar y reconocer la autenticidad de los activos del dominio (de tipo ***información)*** y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.
- **Subestado C de confidencialidad,** definido como la característica que previene contra la divulgación no autorizada de activos del dominio. Concierne sobre todo a activos de tipo ***información,*** y a menudo se relaciona con la intimidad o 'privacidad', cuando esa información se refiere a personas físicas, que trata la LORTAD, Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal. El término divulgación debe tomarse en su sentido más estricto: el simple acceso físico o lógico al activo altera este subestado, aunque no haya modificaciones aparentes ni difusión posterior.
- **Subestado I de integridad,** definido como la característica que previene contra la modificación o destrucción no autorizadas de activos del dominio. La integridad está vinculada a la ***fiabilidad funcional*** del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél) y suele referirse (no siempre) a activos de tipo ***información.*** Por ejemplo, son típicos los problemas causados por la amenaza de un virus (llegado con un disquete externo o por la red) a la integridad de los datos almacenados en el disco duro de un PC.
- **Subestado D de disponibilidad,** definido como la característica que previene contra la denegación no autorizada de acceso a activos del dominio. La disponibilidad se asocia a la ***fiabilidad técnica*** (tasa de fallos) de los componentes del sistema de información.

1.3 Relaciones entre activos y niveles

1. Activos relacionados con el nivel del **entorno (E)**
    - Equipamientos y suministros (energía, climatización, comunicaciones)
    - Personal (de dirección, de operación, de desarrollo, otro)
    - Otros tangibles (edificaciones, mobiliario, instalación física)

2. Activos relacionados con el nivel de los **Sistemas de Información**:
    - Hardware (de proceso, de almacenamiento, de interfaz, servidores, firmware, otros)
    - Software (de base, paquetes, producción de aplicaciones, modificación de firmware)
    - Comunicaciones (redes propias, servicios, componentes de conexión, etc.)
3. Activos relacionados con el nivel de la **Información**:
    - Datos (informatizados, concurrentes al o resultantes del Sistema de Información)
    - Meta-información (estructuración, formatos, códigos, claves de cifrado)
    - Soportes (tratables informáticamente, no tratables)
4. Activos relacionados con el nivel de las **Funcionalidades de la organización**:
    - Objetivos y misión de la organización
    - Bienes y servicios producidos
    - Personal usuario y/o destinatario de los bienes o servicios producidos
5. **Otros Activos** no relacionados con los niveles anteriores
    - Credibilidad (ética, jurídica, etc.) o buena imagen de una persona jurídica o física,
    - Conocimiento acumulado,
    - Independencia de criterio o de actuación,
    - Intimidad de una persona física,
    - Integridad material de las personas, etc.

El proyecto de seguridad articula los 5 tipos o niveles como 'capas' de Activos desde el punto de vista de las cadenas potenciales de fallos 'verticales' entre dichas capas. Así, fallos en Activos del **Entorno** (1) provocarían otros fallos en el **Sistema de Información** (2); éstos inciden en fallos de la **Información** (3), que soporta las **funcionalidades de la organización** (4) y ésas condicionan los **otros activos** (5).

La calidad de la aplicación de MAGERIT depende de que esta tipificación de Activos se realice con cuidado y se adapte adecuadamente al proyecto previsto. Los problemas de seguridad se pueden manifestar en una cualquiera de las capas, pero sus consecuencias la desbordan, con problemas en todas las capas que dependen de aquélla. La explicitación de las cadenas 'verticales' no es evidente ni inmediata, pero es imprescindible realizarla para no olvidar Activos afectables.

1.4 Atributos

Cada Activo o Grupo de Activos incorpora como atributos esenciales dos indicadores sobre dos tipos de valoraciones, que ofrecen una orientación para calibrar el posible impacto que la materialización de una amenaza puede provocar en el activo:

• **la valoración intrínseca al activo** considerado tiene dos aspectos

- uno cualitativo como ***valor de uso*** del Activo; este atributo permite responder al ***para qué*** sirve el Activo y soporta la clasificación anterior en tipos por naturaleza;
- otro cuantitativo como ***valor de cambio,*** o sea ***cuánto*** vale; este atributo es válido para ciertos tipos de activo y útil tanto a efectos indirectos de la ***valoración del impacto*** causable por las amenazas, como para soportar la decisión entre la valoración del Riesgo y la de las salvaguardas para reducirlo.

• **la valoración del estado de seguridad del activo** considerado, expuesta anteriormente como característica por su importancia, se concreta en sus 4 subestados ***A-C-I-D***: autenticación, confidencialidad, integridad, disponibilidad.

1.5 Métricas

Los **Responsables del Dominio protegible** – la Secretaría Económico Financiera de la UNCuyo, como promotora del proyecto y los usuarios responsables del Dominio considerado, son quienes deben identificar, definir y valorar sus Activos.

Las valoraciones anteriores reposan sobre sendas métricas.

Las métricas de valoración intrínseca de los Activos se apoyan en los siguientes casos:

- Ciertos Activos pueden estar **inventariados**: una parte importante de los Activos de los niveles 1 (**Entorno**) y 2 (**Sistema de información**) pueden tomarse de los Inventarios preestablecidos en la Unidad Ejecutora y por tanto seguirán las clasificaciones de dichos inventarios (relacionadas a menudo con su contabilización patrimonial).
- Otros Activos pueden estar **inventariados o no**: así las Aplicaciones existentes que cubren la obtención de determinada **Información** (nivel 3) o ciertas **Funcionalidades de la Organización** (nivel 4) suelen estar inventariadas si se compran en el mercado o si se pueden valorar, por ejemplo por su coste de producción.
- Una parte de activos del sistema en estudio **no son inventariables** en el sentido contable del término, es decir como **'valor de cambio'** (apto por ejemplo para reposición en caso de deterioro). No por ello dejan de tener un **'valor de uso'** para la organización, que a menudo se suele apreciar cualitativamente por su carencia.

Sin embargo, no se recomienda la **mezcla** de valoraciones de activos inventariables y no inventariables porque dicha mezcla suele subestimar éstos últimos, los inmateriales y en particular los específicamente ligados a la administración pública, como en nuestro caso particular. Como se verá en el ANEXO VIII (Tabla ***'Valoración de Activos'***), el procedimiento recomendado para valorar activos se puede resumir en un doble esfuerzo:

- Se intentó encontrar el 'valor de cambio' del activo como valor de reposición, directa (valor de inventario) o indirectamente (coste de su regeneración tras un Impacto)
- Si esa valoración fue imposible o inconveniente (valor de 'reposición' de una persona tras un accidente causado por falta de seguridad de algún activo), se trata a este activo (con sus posibles impactos y riesgo consecuentes) como un elemento del entorno del dominio abarcado por el proyecto de seguridad; elemento que influye sobre éste a modo de una restricción parcialmente ajena al tratamiento estricto pero condicionante de su resultado (por lo que el activo o sus derivados aparecen por ejemplo en los informes intermedios y en su caso en el informe final del proceso).

Aplicación de la Etapa 2 al Caso tomado como ejemplo

Actividad 2.1: recogida de información

La tarea de preparación de información, consiste en recoger los datos recientes y bien formalizados del último plan informático (PI) y del análisis-diagnóstico (A-D).

Las entrevistas abarcaron a todos los **equipos, administradores y usuarios responsables** relacionados con los sistemas de información:

- Equipo de asesores de la gestión presupuestaria.
- Administrador del Sistema de Información GEPRE.
- Programadores
- Analistas
- Pasantes
- Usuario Responsable de Programa (todos los Decanos y algunos Secretarios de Universidad).
- Usuario Responsable de SubPrograma (todos los Secretarios de Facultad, algunos Secretarios de Universidad)

- Usuario Responsable de Actividad (todos los Directores de Carrera, algunos Secretarios de Facultad y de Universidad, Directores de Administración y Jefaturas).
- Usuario Responsable de Unidad Ejecutora (todos los Secretarios Económico-Financieros y Contadores de Facultad y de Universidad).

Para la tarea 2.1.3 de análisis de la información recogida se tomaron no sólo los resultados de las entrevistas anteriores, sino visitas de inspección a los puestos de trabajo en horas críticas (sin los ocupantes, por ejemplo) así como manejo de los documentos de procedimientos administrativos, explotación y desarrollo de sistemas empleados por el sistema.

Actividad 2.2: Identificación y agrupación de ACTIVOS

Tras el análisis de la información recogida directa e indirectamente, sobre GEPRE dependiente del Rectorado de la UNCuyo como entidad específica del sector de gobierno y de la administración pública, se abordó la tarea de Identificar activos y grupos de activos.

Ésta se centra, por la particularidad de los objetivos en este caso, en dos grandes grupos, referidos a los ***Servicios utilizadores*** y a los ***Servicios procesadores*** de los sistemas de información del GEPRE.

Ambos grupos se reparten los 5 niveles de capas considerados en el Submodelo de Elementos propuesto por MAGERIT:

1. entorno
2. sistema de información
3. información
4. funcionalidades de la organización
5. otros activos

• Los Servicios utilizadores son responsables de los Activos de los tres tipos 'dependientes' (del funcionamiento de los Activos que les dan soporte, se entiende), es decir los niveles 3 de Información, 4 de Funcionalidades de la Organización y 5 de Otros Activos.

• Los Servicios procesadores son responsables de los Activos de los dos tipos de soporte (del funcionamiento de los Activos 'dependientes', se entiende), es decir los niveles 2 de Sistemas de Información y 1 de Entorno.

Durante las entrevistas y las inspecciones se recogió también la información necesaria para cumplimentar la tarea de identificar mecanismos de salvaguarda existentes.

La tarea de valorar activos no es realmente imprescindible, para el objetivo de este proyecto (realizar el análisis y gestión de riesgos necesario para organizar un plan de contingencia racional, sin necesidad de justificar su coste por los retornos obtenidos). Sin embargo se ha emprendido el alto esfuerzo que representa valorar los activos a fin de contar en un futuro con una valoración a priori de éstos.

Actividad 2.3: Identificación y evaluación de AMENAZAS

La tarea de Identificar y agrupar amenazas se limita a reagrupar los tipos de amenazas identificados según MAGERIT para establecer un número reducido de escenarios de siniestro manejables fácilmente, que comprenden un conjunto interrelacionado Amenaza-Vulnerabilidad-Impacto (A-V-I).

Como se verá con detalle en la Actividad 2.6, los Escenarios cubren los siguientes grupos de Amenazas:

1. *accidente natural o industrial*
2. *ataque físico sin provecho directo*
3. *interrupción de servicio*
4. *errores o insuficiencias de diseño*
5. *sustracción lógica*
6. *ataque lógico*

Tarea que permite establecer los árboles de fallos generados por amenazas se incluye en la agrupación anterior de Amenazas en escenarios.

Actividad 2.4: Identificación y estimación de VULNERABILIDADES

La tarea de Identificar vulnerabilidades para cada activo amenazable de los ***Servicios utilizadores*** o de los ***Servicios procesadores*** se realiza por el especialista a la vez que la tarea de Estimar vulnerabilidades, y dentro de la aplicación de un Escenario de Amenaza-Vulnerabilidad-Impacto a cada activo.

Actividad 2.5: Identificación y valoración de IMPACTOS

La Tarea de Identificar impactos para cada Activo vulnerable de los ***Servicios utilizadores*** o de los ***Servicios procesadores*** se realiza por el especialista a la vez que la tarea de Tipificar impactos y la tarea de Valorar impactos, dentro de la aplicación de un Escenario de Amenaza – Vulnerabilidad - Impacto a cada activo.

Actividad 2.6: Evaluación del RIESGO

Las tres Tareas de esta Actividad se realizaron de forma reducida y simultánea. Así, la tarea de evaluar el riesgo intrínseco se soslaya para pasar directamente a la tarea de evaluar el riesgo efectivo, tras ejecutar la tarea de analizar las funciones de salvaguarda existentes. El objetivo del proyecto no requiere la separación de las salvaguardas existentes y el aislamiento del riesgo intrínseco. Bastó con que el especialista fue aplicando a lo largo de la descripción de cada activo considerado, el escenario adecuado entre los que siguen, se ha descrito en forma de fichas explicativas:

FICHA DE ESCENARIO de SINIESTRO ES1

- **TIPO DE AMENAZA:** ***ACCIDENTE NATURAL O INDUSTRIAL***

  Cubre los tipos de Accidentes A1 y A3 de MAGERIT:

  - ***A1: Accidente físico de origen industrial:*** incendio, explosión, inundación por rotura de cañerías, contaminación por fuga polo petroquímico
  - ***A3: Accidente físico de origen natural:*** terremoto, inundación, rayo, deslave, derrumbe, granizada.
- **ACTIVO alcanzable:** sistema físico y entorno del Nodo de la UNCuyo (Centro de Proceso).
- **VULNERABILIDAD:** mientras que A3 puede considerarse excepcional, A1 presenta una posibilidad de ocurrencia mucho más alta: aún contando con la reducción actual de vulnerabilidad lograda por las medidas de protección contra incendios tomadas por ejemplo en el Centro de Proceso del Sistema Corporativo (Nodo), se encuentra situado en una zona considerada como de alto riesgo sísmico (estructura que antiguamente pertenecía a un tanque aprovisionador de agua, encontrándose en los últimos pisos de la torre el conjunto de servidores, antenas y cableado, los archivos altamente inflamables), sin posibilidades de cambio de ubicación global a corto plazo. El 'AGRESOR' es aquí la naturaleza o entorno industrial que actúa evidentemente sin MOTIVACIÓN, de forma aleatoria (lo que no excluye la posibilidad de cierta predictibilidad y por tanto de reducción de ***Exposición*** a sus efectos) y con gran ***Fuerza***.
- **TIPO DE IMPACTO:** Grandes ***pérdidas:***
  - ***N1. económicas:*** gasto de tasar, sustituir, reparar o limpiar lo dañado.
  - ***N2. inmateriales:*** gastos de tasación y restauración de elementos no materiales del sistema: datos, programas, documentación, procedimientos.

ESCENARIO de SINIESTRO ES2

- **TIPO DE AMENAZA:** ***ATAQUE FÍSICO SIN PROVECHO DIRECTO***

  Cubre el tipo de amenaza malintencionada:

- **ACTIVO alcanzable:** sistema físico y entorno de la UNCuyo (Plataforma de Producción y de Desarrollo, Oficinas diversas Unidades Ejecutoras).
- **VULNERABILIDAD:** está en relación directa con la facilidad de acceso físico al Activo (los controles son claramente disuasorios). Este tipo de ataque puede ser devastador si alcanza un centro neurálgico del sistema de la UNCuyo, por ejemplo: El AGRESOR será una persona con conocimientos técnicos someros que actúa con MOTIVACIÓN ideológica o psicológica, pero no económica. La exposición está directamente unida a la falta de controles de acceso físicos, puesto que el riesgo para el agresor es bajo (su motivación no económica no se frenará por un riesgo de localización bajo, pese a unas consecuencias penales altas). Al agresor le basta una fuerza baja, pues no requiere capacidad técnica ni medios sofisticados.
- **TIPO DE IMPACTO:** Grandes ***pérdidas:***
    - ***N1. económicas:*** gasto de tasar, sustituir, reparar o limpiar lo dañado.
    - ***N2. inmateriales:*** gastos de tasación y restauración de elementos no materiales del sistema: datos, programas, documentación, procedimientos

ESCENARIO de SINIESTRO ES3

- **TIPO DE AMENAZA:** ***INTERRUPCIÓN DE SERVICIO,*** debido a:
    - ***A2: Avería de origen físico o lógico.***
    - ***A4: Interrupción de servicios o de suministros esenciales:*** energía, agua, telecomunicación, gas, fluidos y suministros diversos.
    - ***A5: Accidentes mecánicos o electromagnéticos:*** choque, caída, cuerpo extraño.
    - ***P5: Indisponibilidad de recursos humanos*** *o* ***técnicos*** (desvío de uso, bloqueo).
- **VULNERABILIDAD:** Aunque con frecuencia decreciente, estos 3 tipos de accidente siguen siendo posibles, sobre todo en los puestos periféricos, tanto por fallos de energía debidos a la falta de sistemas de alimentación ininterrumpida o por problemas de líneas de comunicación, como por falta de mantenimiento preventivo o de terminales de repuesto, como por una instalación deficiente. Los 'AGRESORES' son las insuficiencias de servicios e instalaciones internos o las deficiencias del mantenimiento preventivo y evidentemente carecen de MOTIVACIÓN. La exposición natural es media y depende de situaciones concretas (sobrecargas a la red eléctrica) o aleatorias; y la Fuerza para que se produzca la agresión es baja (no se requiere capacidad técnica ni medios especiales).
- **ACTIVO alcanzable:** en general sólo la ejecución de aplicaciones determinadas. En los PC no protegidos de los usuarios responsables de las diversas unidades ejecutoras del presupuesto donde pueden perderse datos introducidos desde la última salvaguarda.
- **TIPO DE IMPACTO:** Perdidas ligeras por:
    - ***SD. Indisponibilidad:*** reducción de recursos por falta de resultados; o bien gastos suplementarios para mantener la funcionalidad precedente a la amenaza.

ESCENARIO de SINIESTRO ES4

- **TIPO DE AMENAZA:** ***ERRORES O INSUFICIENCIAS DE DISEÑO***

  Cubre todo el Grupo E de Errores:
    - ***E1: Errores de utilización*** en la recogida y transmisión de datos o en su explotación.
    - ***E2: Errores de diseño*** existentes desde los procedimientos de desarrollo del software.

- ***E3: Mala ruta/mala secuencia*** de entregas de un Mensaje o Correo Electrónico.
- ***E4: Monitorización/Trazabilidad/Registro*** inadecuados del Tráfico, tanto en la Intranet de la UNCuyo, como en la Internet.

- **VULNERABILIDAD:** Pese a su origen aparentemente distinto, se trata de errores debidos al diseño en sentido amplio. Así el tipo de error E1 es más fácilmente detectable que el E2 (puede darse por falta de rutinas de verificación interna y de cuadre con otra información externa), mientras que los errores E3 y E4 dependen del software de comunicación. En todos los casos y para equipos de desarrollo y explotación competentes y bien equipados, la posibilidad de todos ellos será baja (mayor para E1 que para los demás). En cuanto a AGRESOR, los técnicos de desarrollo no tienen motivación en este tipo de errores. En aplicaciones complejas la Exposición natural es media, pero el 'agresor' sólo necesita una Fuerza baja pues carece de responsabilidad aunque su trabajo es rastreable y además la oportunidad de error crece con la disminución de competencias técnicas).
- **ACTIVO alcanzable:** la aplicación con errores y el servicio que dependa de ella.
- **TIPO DE IMPACTO:** pérdidas ligeras por:
  - ***SD. Indisponibilidad:*** menores recursos o gastos excesivos para mantener la funcionalidad.
    - ***L2. Incumplimiento de obligaciones legales.***[ix]
    - ***L3. Perturbación o situación embarazosa político-administrativa*** (por ejemplo credibilidad, prestigio...).

ESCENARIO de SINIESTRO ES5

- **TIPO DE AMENAZA: *SUSTRACCIÓN LÓGICA***, que cubre:
  - ***P3 y T1: Acceso lógico con sustracción (presencial o teleactuado):*** uso del sistema, reduciendo su confidencialidad para obtener bienes o servicios aprovechables (programas, datos, tablas.).
- **VULNERABILIDAD:** En general este tipo de amenaza depende del valor intrínseco de lo sustraíble, por lo que la posibilidad depende de la aplicación. Para el AGRESOR el valor de la información sustraíble constituye la motivación principal. El agresor debe contar con una accesibilidad alta; y necesita una fuerza alta si se tiene en cuenta la competencia técnica necesaria y cuenta con la rastreabilidad de la agresión. La combinación de lo anterior da como resultado del perfil probable un agresor interno.
- **ACTIVO alcanzable:** Información sustraída.
- **TIPO DE IMPACTO:** Pérdidas medias de:
  - ***SC. Confidencialidad***[x]***:***
    - ***L2. Incumplimiento de obligaciones legales.***
    - ***L3. Perturbación o situación embarazosa político-administrativa.***

ESCENARIO de SINIESTRO ES5

- **TIPO DE AMENAZA: *SUSTRACCIÓN LÓGICA***, que cubre
  - ***P3 y T1: Acceso lógico con sustracción (presencial o teleactuado):*** uso del sistema, reduciendo su confidencialidad para obtener bienes o servicios aprovechables (programas, datos ...)
- **VULNERABILIDAD:** En general este tipo de amenaza depende del valor intrínseco de lo sustraíble, por lo que la posibilidad depende de la aplicación. Para el AGRESOR el valor de la información sustraíble constituye la motivación principal. El agresor debe contar con una accesibilidad alta; y necesita una fuerza alta si se tiene en cuenta la competencia técnica necesaria y cuenta con la rastreabilidad de la

agresión. La combinación de lo anterior da como resultado del perfil probable un agresor interno.

- **ACTIVO alcanzable:** Información sustraída.
- **TIPO DE IMPACTO:** Pérdidas medias de
    - ***SC. Confidencialidad:***
        - ***L2. Incumplimiento de obligaciones legales***
        - ***L3. Perturbación o situación embarazosa político-administrativa***

ESCENARIO de SINIESTRO ES6

- **TIPO DE AMENAZA:** ***ATAQUE LÓGICO***, que cubre
    - ***P4 y T2: Acceso lógico con destrucción (presencial o teleactuado):*** uso del sistema para reducir su integridad y/o disponibilidad sin provecho directo (sabotaje inmaterial, infección vírica...)
- **VULNERABILIDAD:** directamente y a los programas del sistema central es baja, pues requiere una gran capacidad técnica para transgredir las defensas de acceso; pero puede ser alta respecto a los datos del sistema central o a los programas de los PCs (bien por incompetencia o por falta de precauciones en la desinfección de entradas). La falta de motivación económica, unida a una accesibilidad natural alta fuera de los programas del sistema central y a la baja fuerza necesaria (dada la impunidad relativa por ser de rastreabilidad difícil, combinada con una tecnicidad requerida baja) componen un perfil agresor de usuario desmotivado o desinformado.
- **ACTIVO alcanzable.** Más amplio que el activo agredido, abarca los programas que alcanza la infección o los datos descohesionados por la agresión o el descuido.
- **TIPO DE IMPACTO:** pérdidas altas ligeras por
    - ***N1. económicas:*** gasto de tasar, sustituir, reparar o limpiar lo dañado.
    - ***N2. inmateriales:*** gastos de tasación y restauración de elementos no materiales el sistema: datos, programas, documentación, procedimientos
    - ***L2. Incumplimiento de obligaciones legales***
    - ***L3. Perturbación o situación embarazosa político-administrativa*** (por ejemplo credibilidad, prestigio, competencia política ...)
    - ***SD. Indisponibilidad:*** reducción de margen por falta de resultados; o bien gastos suplementarios para mantener la funcionalidad precedente a la amenaza.

CASO DE ACTIVO DE UN SERVICIO "Carga del MAPA PRESUPUESTARIO"

La aplicación de los escenarios anteriores para el análisis de riesgos de un activo de tipo sistemas de información en un servicio por parte de utilizadores típico, como el registro y el seguimiento de la gestión presupuestaria. El analista de riesgos (en este caso, como consultor externo) ha recogido en un primer informe descriptivo las respuestas al correspondiente cuestionario realizado con los usuarios responsables del sistema para obtener la información básica sobre el servicio.

La tarea consiste en ir 'incrustando' uno de los escenarios, tomado de los 6 anteriores, en cada lugar que se considere adecuado del informe. Simultánea o sucesivamente, el Analista deduce los niveles de **criticidad del riesgo** en cada 'incrustación', con lo que el informe inicial se ha convertido en un 'informe de los riesgos efectivos' ya evaluados.

Tomando el activo reseñado, se recogió en el informe[xi] que la **Secretaría Económico Financiera de la UNCuyo** a cargo del Sistema **GEPRE**[xii] provee sobre el seguimiento y control de la situación de éstos en la organización, tanto por la obligación legal (Presupuesto Nacional 2006 - Ley Nro 26.078 **y** Decreto Nro. 8 de Promulgación de la Ley Nro 26.078) de informar a la

comunidad universitaria afectada del estado del trámite que refiere, así como por el interés de la propia administración de la UNCuyo en conocer el estado de su producción.

• En caso de incumplimiento de esta misión, la repercusión es la paralización de los trámites reseñados en los expedientes si éstos no son consultables y actualizables, lo que tiene perjuicios para la comunidad usuaria, con un Impacto ***L2 de incumplimiento de obligaciones legales*** y causa sobre todo una inseguridad jurídica general, con un Impacto ***L3 de perturbación o situación embarazosa político-administrativa.***

Entrando en un nivel mayor de detalle que permita **evaluar riesgos** y aunque no se tienen aún estadísticas, la organización mueve mucho más de 3.000 expedientes por año. La aplicación tiene un centenar de usuarios responsables (incluidos unos 15 secretarios Económico Financieros) con su correspondiente dotación de terminales o los PC con placa de conexión.

• Al estar unidos a la plataforma (nodo) donde reside la aplicación, si se da en éste un posible ESCENARIO DE SINIESTRO ***ES1 de accidente natural o industrial*** o bien un ESCENARIO ***ES2 de ataque físico*** pueden generar un incumplimiento de la misión del servicio de ***impacto muy alto***, con las ***vulnerabilidades*** de cada caso y por tanto con un RIESGO respectivamente BAJO y ALTO.

La presupuestación por ACTIVIDAD se inicia por impulso de la propia organización o por peticiones que llegan a la oficina de GEPRE (por el que entran también otros documentos que se incorporan a un expediente ya iniciado). Los impulsos internos o los documentos registrados se introducen en el sistema para 'disponerlos' a las unidades ejecutoras correspondientes. Ésta los tramita con ayuda informatizada y cuando considera realizado su trámite, cierra el MAPA PRESUPUESTARIO en el sistema central y lo 'envía' a la Unidad Ejecutora, según su criterio, a la que pide acuse de recibo: si pasan 10 días sin recibirlo, se dispara una 'alarma' de recuerdo en el sistema.

Este encadenamiento 'abierto' de los trámites a su paso por las unidades ejecutoras es más simple que un encadenamiento ‘predeterminado’, pero como contrapartida, todo el proceso se para con que una unidad lo interrumpa (el sistema permite al menos saber quien es la unidad paralizadora).

• Un posible ESCENARIO DE SINIESTRO ***ES1 de accidente natural o industrial*** o bien otro ***ES2 de ataque físico,*** pueden generar un incumplimiento de ***impacto muy grave*** de la misión del servicio, con las ***vulnerabilidades*** de cada caso y por tanto con RIESGOS respectivamente MEDIO y ALTO.

• Un posible ESCENARIO DE SINIESTRO ***ES1 de accidente natural o industrial*** o bien otro ***ES2 de ataque físico,*** pueden generar un incumplimiento de ***impacto gravísimo*** de la misión del servicio, con las vulnerabilidades de cada caso y por tanto con RIESGOS respectivamente ALTO y MUY ALTO. Por su parte, la **misión principal** de la unidad de **REGISTRO GENERAL,** utilizadora de una parte del sistema de información GEPRE (módulos de registro de entrada y salida) consiste en registrar todos los objetivo y metas físicas para luego poder asignar montos a los incisos correspondientes y finalmente obtener la ordenanza de Consejo Superior “PRESUPUESTO”.

• La repercusión, en caso de incumplimiento de esta misión, es un grave perjuicio ocasionado tanto a la corporación como al ciudadano, debido al posible incumplimiento de plazos que marca la Ley, con un ***impacto L2 de incumplimiento de obligaciones legales,*** así como la paralización de la actividad del resto de las unidades administrativas (con ***Impactos SD de disponibilidad*** y posiblemente ***SI de integridad***) y pérdida de imagen de la organización (***con impacto L3 de perturbación o situación embarazosa político-administrativa***).

Entrando en un nivel mayor de detalle que permita **evaluar riesgos,** actualmente el registro de entrada, como media, recibe más de 1.000 instancias diarias (con picos de 2.000) de las que el 10% se considera urgente de ‘determinar’. Aunque el plazo para registrar, los documentos deben de tramitarse y enviarse al circuito de GEPRE, debe ser lo antes posible, porque hasta que no se tramiten por el registro, el MAPA PRESUPUESTARIO no se puede

abrir la carga de objetivos y metas; con lo que toda materialización de amenazas en el registro y por tanto la CRITICIDAD de los RIESGOS evaluada por la aplicación de los escenarios de siniestro en el registro se **transmite** al circuito de carga del MAPA PRESUPUESTARIO (objetivos y metas físicas, no iniciado) y a la criticidad de los riesgos citados en los párrafos anteriores.

En cada una de las **14 facultades más los institutos, de registro de entrada** (la sede central de GEPRE en FCE y la secretaría económico financiera en rectorado, se consideran aparte) se graba la información que consta en la instancia que presentan los usuarios responsables, sea cual sea su destino, y se introducen en el sistema (se manejan más datos que con el tratamiento manual, que ha quedado en desuso y sin vuelta atrás). Los documentos se agrupan por gran tipo de destino (las unidades ejecutoras o los usuarios responsables de sedes e institutos – Balseiro -) en paquetes encabezados con carátulas o relaciones de envío generadas por el ordenador central para las diferentes Unidades tramitadoras (unas 50) de los servicios, a los que se remiten junto a los documentos (relaciones por duplicado para que el receptor firme en una el recibí y lo devuelva al registro).

Los más de 2000 posibles terminales actuales de registro están vinculados por intranet y/o internet al nodo de la UNCuyo central donde reside el paquete informático.

• Si sucede en este sistema central un posible ESCENARIO DE SINIESTRO ***ES1 de accidente natural o industrial*** o bien un ESCENARIO ***ES2 de ataque físico***, se pueden generar un incumplimiento de ***impacto muy grave*** de la misión del servicio, con las ***vulnerabilidades*** de cada caso y por tanto con RIESGOS respectivamente MEDIO y ALTO.

El proceso de **registro de salida** se genera de forma automática con la informatización global del circuito de carga del MAPA PRESUPUESTARIO (aunque la unidad ejecutora tramitadora no asigne la salida) y no implica tanto problema de plazos ni por tanto de RIESGO sensible.

• Por otra parte, la falta de aprovechamiento de información ya existente en el sistema (la aplicación permitiría introducir textos repetidos precodificados) puede reflejar un ESCENARIO DE SINIESTRO ***ES4 de errores o insuficiencias de diseño,*** con un ***impacto bajo*** y una ***vulnerabilidad alta***, es decir con un RIESGO BAJO.

• La falta de experiencia en el USO DE CLAVES DE USUARIO (aún se usa sólo el número de funcionario) no deja de implicar un conjunto de ESCENARIOS DE SINIESTRO ***ES5 de sustracción lógica y ES6 de ataque lógico*** que en conjunto suponen una amenaza de probabilidad baja y nivel leve con ***impactos*** de tipo ***SC de pérdida de confidencialidad y L3 de perturbación o situación embarazosa político-administrativa***: en los dos casos se tiene un RIESGO BAJO.

• Asimismo la posibilidad o el deseo de cambiar fechas de entrada en registro implican un ESCENARIO DE SINIESTRO ***ES5 de sustracción lógica*** con un nivel de ***impacto medio*** y un nivel de ***vulnerabilidad bajo,*** con un RIESGO BAJO.

• El ACCESO DE PERSONAS EXTERNAS al recinto de los terminales tanto por la mañana (al cerrar, las personas externas que están dentro salen por el interior de la Unidad), como por la tarde, con las dependencias abiertas sin vigilancia, implica un posible ESCENARIO DE SINIESTRO ***ES2 de ataque físico*** de ***impacto medio*** y ***vulnerabilidad alta***, es decir con un RIESGO BAJO.

CASO DE ACTIVO DE UN SERVICIO UTILIZADOR “Asignar montos a incisos: MAPA”

El análisis de riesgos de activos de los ***servicios procesadores*** se efectúa en las áreas tradicionales:

- Entorno organizativo
- Entorno físico
- Hardware y software de base

- Comunicaciones
- Explotación
- Desarrollo de aplicaciones

Aquí se transcriben sólo los 'Activos' cuya seguridad tiene relevancia para el plan de contingencia como objetivo del proyecto.

Por ejemplo, la ubicación del hardware principal (CPU, discos, impresoras, concentradores,...) en la planta sótano implica un posible escenario de siniestro ES1, de accidente natural/industrial, con un impacto crítico y con potencialidad insignificante, de lo que resulta en un RIESGO **ALTO**; y un posible escenario de siniestro ES2, de Ataque físico, con un impacto muy grave y con potencialidad baja, de lo que resulta un RIESGO **ALTO**.

En cuanto a la **redundancia de materiales informáticos,** en la unidad central de proceso no existe redundancia, aunque el presente estudio tiene como uno de sus objetivos prever dicha redundancia a través de un centro externo. Existen varios concentradores de comunicaciones, como ya se destacó, aunque en la actualidad todos están ubicados en el sótano, junto al ordenador. Las impresoras centrales también son redundantes aunque igualmente se encuentran las dos en el 1er. piso.

La concentración de los anteriores elementos en la sala de ordenadores (en el sótano) anula la seguridad de estas redundancias e implica que un posible escenario de siniestro ***ES1***, ***accidente natural/industrial***, o ***ES2***, ***ataque físico,*** pueden tener un impacto muy grave, ya que implicaría la disrupción de las actividades, y con potencialidad insignificante o baja respectivamente, de lo que resulta un RIESGO BAJO a **ALTO,** respectivamente.

En cuanto a la **ubicación de los elementos de comunicaciones** de cabecera, es decir, los concentradores conectados a canal del ordenador, el procesador de comunicaciones, los multiplexores, etc., están ubicados, como se reflejó anteriormente, en la sala de ordenador. Esto implica un posible escenario de siniestro ***ES1***, ***accidente natural/industrial***, con un impacto crítico y con potencialidad insignificante, lo que resulta un RIESGO **ALTO**; y un posible escenario de siniestro ***ES2***, ***ataque físico***, con un impacto crítico y con potencialidad baja, de lo que resulta un RIESGO **MUY ALTO**.

Archivo de soportes. El área de archivo está ubicada en la sala del ordenador, lo cual implica un posible escenario de siniestro ***ES1***, ***accidente natural/industrial***, con un impacto muy grave con potencialidad insignificante, de lo que resulta un RIESGO **BAJO**; y un posible escenario de siniestro ***ES2***, ***ataque físico***, con un impacto muy grave con potencialidad baja, de lo que resulta en un RIESGO **ALTO**.

Copias de seguridad. Se realizan copias de seguridad de los datos, software y todo el entorno de desarrollo con una periodicidad determinada, guardando un número de generaciones y en ciertos lugares de almacenamiento. Estos aspectos serán detallados en el ANEXO IV. No obstante resaltar, que las copias de seguridad almacenadas en el edificio del nodo (Área de Sistemas) comprenden información con periodicidad semanal, lo cual implica un posible escenario de siniestro ***ES1***, ***accidente natural/industrial***, con un impacto crítico pero con potencialidad insignificante, de lo que resulta en un RIESGO **ALTO**; y un posible escenario de siniestro ***ES2***, ***ataque físico***, con un impacto crítico y con potencialidad baja, de lo que resulta en un RIESGO **MUY ALTO**.

Documentación de explotación. La documentación de explotación, tanto el manual de operaciones de explotación como los manuales de explotación de las diversas aplicaciones, no están actualizados, lo cual implica un posible escenario de siniestro ***ES4***, ***errores de diseño***, con un impacto medio con potencialidad alta, de lo que resulta en un RIESGO **BAJO**. En algunos casos la documentación de aplicaciones o de modificaciones a aplicaciones al pasar a producción se considera escasa, lo cual implicaría un posible escenario de siniestro ***ES4***, ***errores de diseño***, con un impacto medio y con potencialidad alta, de lo que resulta un RIESGO **BAJO**.

Seguimiento de la explotación. Existe un plan de explotación, de tal forma que los trabajos se ejecutan de acuerdo a dicho plan. Los operadores cumplimentan un informe de actividad

diario con los trabajos ejecutados, sus resultados e incidencias. Esta implantado un procedimiento de control visual y archivo de los mencionados informes de actividad de los trabajos ejecutados, incidentes, etc. En el caso de las incidencias, se anotan en libreta (manual), reflejando su naturaleza y las acciones tomadas. La petición de trabajos batch, por parte de los usuarios, se realiza de forma automática, ya que incluye parámetros en procesos online, que originan al lanzamiento del batch las extracciones necesarias y ejecutan la petición. No obstante, en aplicaciones antiguas o en casos especiales se encuentra establecido su cumplimento por medio de un impreso normalizado para realizar las peticiones. Periódicamente se confeccionan resúmenes sobre el uso del ordenador (tiempos de CPU, número de transacciones por terminal, desviaciones respecto a la media,...). El paso de programas de desarrollo a producción (explotación) se realiza a través de un paso intermedio llamado de Integración, donde se recompilan los fuentes para cambiar los apuntadores a ficheros. Hay una o dos personas autorizadas por aplicación para el paso de desarrollo a integración. A Producción solo pasan ejecutables. Esto conlleva un posible escenario de siniestro ***ES6***, ***ataque lógico***, con un impacto medio y con potencialidad insignificante, de lo que resulta un RIESGO **MUY BAJO**.

Mantenimiento de material. El mantenimiento del material informático está contratado a empresas externas, que se encargan del mantenimiento preventivo y correctivo, no habiéndose detectado problemas en sus actuaciones. Pero no se recogen dichas actuaciones en un diario. Esto está ligado a un posible escenario de siniestro ***ES3***, ***servicio interrumpido***, con un impacto medio y con potencialidad insignificante, de lo que resulta un RIESGO **MUY BAJO**. La instalación de material informático (terminales, impresoras, concentradores,...) habitualmente se realiza por personal del área de Sistemas. El software de base es mantenido y provisto en el modelo Open-Source (Software abierto y gratuito), disponiendo en general de versiones bien actualizadas. Las averías, anomalías, etc., se registran, así como las medidas tomadas para su resolución, en una aplicación en PC; obteniendo diversos tipos de listados por servicios. Esto está ligado, en caso de no explotar la información obtenida, a un posible escenario de siniestro ***ES3***, servicio interrumpido, con un impacto medio y con potencialidad insignificante, de lo que resulta un RIESGO **MUY BAJO**.

Gestión de configuración. No se realiza en la actualidad un control detallado sobre cambios, es decir, una gestión de cambios que permita controlar las modificaciones en las aplicaciones. No se realiza en la actualidad un control detallado sobre configuraciones, que permita controlar la versión actual de cada aplicación y las anteriores. Lo anterior implica un posible escenario de siniestro ***ES4***, ***errores de explotación***, con un impacto muy grave y con potencialidad media, de lo que resulta un RIESGO **ALTO**.

Documentación en Desarrollo. Se realizan manuales de usuario en las nuevas aplicaciones, aunque no se mantienen actualizados directamente con las posteriores modificaciones, lo cual implica un posible escenario de siniestro ***ES4***, ***errores de diseño***, con un impacto muy grave y con potencialidad media, de lo que resulta un RIESGO **ALTO**. La documentación de las aplicaciones no es completa (se utiliza en parte Design/4), no siendo siempre actualizada con las diversas modificaciones, lo cual es perjudicial para el sostenimiento de los manuales de diseño y programación aplicados a mejoras, aunque los primeros se encuentran bastante actualizados.

El Análisis de Riesgo y los Requerimientos de la ISO 27001:2005[xiii]

La ISO 270001:2005 requiere que la organización que esta planeando implantar un SGSI, primero defina el alcance del estándar de la organización, y luego, con base en dicho estándar, identifique los todos los activos de información involucrados. Dichos activos deben ser tasados con el fin de identificar el impacto en la organización. Posteriormente se requiere de un análisis de riesgos para determinar que activos se encuentran susceptibles de esto. Requiriéndose por parte de la dirección una planificación estratégica que monitoree los mismos a intervalos regulares, asegurando adecuación y eficacia en los controles. La misión de la dirección respecto a los SGSI, corresponde en controlar los niveles de riesgo aceptados y el estado de riesgo residual[xiv]. La ISO 27001:2005 es un sistema dinámico que

obliga a la dirección de una organización a proceder de manera constante en la revisión y definición de controles, sus amenazas, vulnerabilidades e iniciar las acciones correctivas y preventivas cuando sean necesarias.

El Proceso de Evaluación de Riesgos

Dicho proceso permite a la organización estar en conformidad con los requerimientos del estándar que se muestran en la siguiente figura. El proceso, configurado en seis fases, da un marco de ayuda a cualquier tipo de organización que desee establecer un SGSI. Aquí se muestra una breve descripción de las fases del proceso de evaluación de riesgo cuyo fin es el implantar el estándar para la organización.

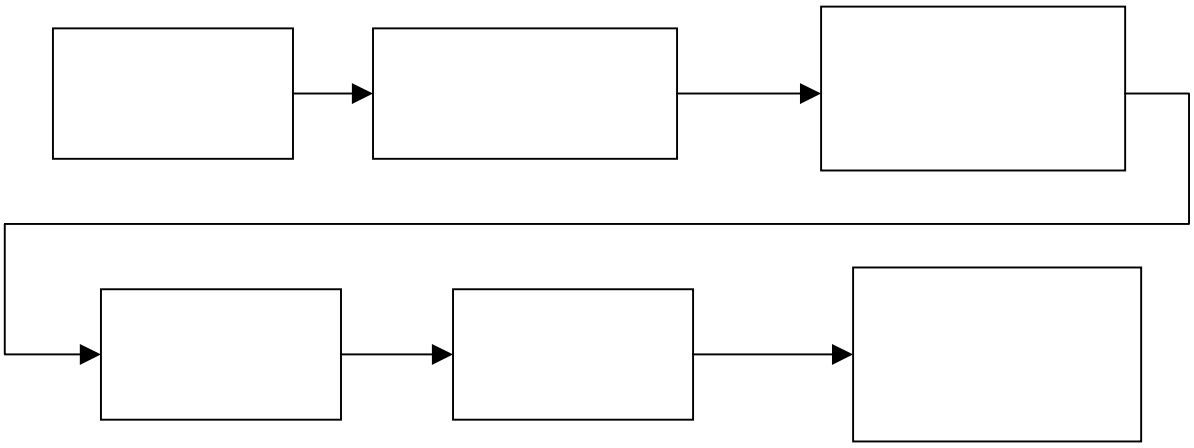


Fig. 7.- Esquema de procesos para la evaluación de riesgos.

CONCLUSIONES

Para la identificación y tasación de los activos, se dijo que un activo es algo que posee valor o utilidad para la organización, sus operaciones y su continuidad. Los activos necesitan ser protegidos a fin de asegurar las correctas operaciones del negocio y la continuidad de la organización.

Cada activo debe estar claramente identificado y rápidamente valorado, adjudicando su propiedad y clasificación de seguridad acordada por la organización. La ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera:

1. **Activos de información:** bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad.
2. **Documentos impresos:** documentos impresos, contratos, lineamientos, documentos de la organización, documentos que contienen resultados importantes para el negocio.
3. **Activos de Software:** Software de aplicación, Software de sistemas, Herramientas de desarrollo.
4. **Activos físicos:** Equipos de comunicación y Computación, Medios magnéticos, Otros Equipos técnicos.
5. **Personas:** Personal, Usuarios Responsables, Suscriptores del SIC[xv],
6. **Imagen y reputación de la organización:**
7. **Servicios:** Servicios de computación y comunicación, otros Servicios técnicos.

De ésta manera se lograron identificar 26 activos en 5 grupos; la valoración de los mismos se realizó de forma directa, indirecta y por su impacto; los costes asociados a dichos activos se aplican cuali-cuantitativamente según las técnicas desarrolladas; la metodología empleada por MAGERIT, y en particular se detectaron 19 posibles amenazas, describiéndose 20 salvaguardas.

Se diseñó un libro de cálculos en Excel, cuyas fórmulas y funciones de encabezado permitieron integrar los conceptos en el nivel más bajo de la desagregación de los datos relevados, así pues se obtuvieron 19 hojas relacionadas:

1. Parámetros
2. Valoración de activos
3. Amenazas
4. Descripción de salvaguardas
5. Salvaguardas por amenaza
6. Salvaguardas agregadas por amenaza
7. Riesgo intrínseco Grupo 1
8. Riesgo efectivo Grupo 1
9. Riesgo intrínseco Grupo 2
10. Riesgo efectivo Grupo 2
11. Riesgo intrínseco Grupo 3
12. Riesgo efectivo Grupo 3
13. Riesgo intrínseco Grupo 4
14. Riesgo efectivo Grupo 4
15. Riesgo intrínseco Grupo 5
16. Riesgo efectivo Grupo 5
17. Riesgos por Grupo y amenaza
18. RI y RE por amenaza
19. Valor activos, RI y RE por amenaza Parámetros

En una etapa posterior, se obtuvieron los software: RISK2 y PILAR, con sus respectivas licencias, herramientas que vinculan por medio de grafos (nodos y caminos) a los Activos, Amenazas y Salvaguardas, con sus respectivos costes. Sobre ellas se comprobaron los resultados obtenidos en las veinte Tablas (hojas de Excel) que corresponden al ANEXO VIII.

Los resultados obtenidos, denotan la precariedad en cuanto a la seguridad en sistemas de información que posee la UNCuyo.

PROYECCIONES

Esta representa una primera aproximación, y establece una fuerte vinculación con los diversos de perfiles que debe poseer el equipo de Auditores. Aquí se ha observado cómo la tarea de identificación y clasificación de los activos es “propietaria” de quienes los poseen o usufructúan, con el asesoramiento del profesional en ciencias económicas; además se observa cómo para calcular y producir datos con mayor inteligencia se han de combinar éste perfil con el del informático a fin de lograr la coherencia y consistencia necesaria del equipo Auditor.

AGRADECIMIENTOS:

A todos los alumnos y pasantes, sin los cuales no se podría haber logrado el relevamiento de Activos, discutido las Amenazas y sus posibles Salvaguardas.

BIBLIOGRAFÍA CONSULTADA

- *Auditoría Informática, Un enfoque Práctico, M. Pattini y E. del Peso Navarro, (2da. Edición). RA-MA, 2001.*
- *Information System Audit and Control Foundation, 1998, R. Weber, Prentice Hall, 1999.*
- *MAGERIT: Guía de Procedimientos. MAP y BOE y otras, Ministerio de Administraciones Públicas, España, 2001/02/04/05, http://www.map.es/csi/pg5m21.htm*
- *ISACA. Normas Generales del Estándar de la ISACA. ISACA, 2002.*
- *COBiT 4.0, Control Objectives for Information and related Technology, Governance Institute® (ITGI) (COBIT®), 2005.*
- *Norma de Calidad: IRAM/ISO 17799 y 20001.*
- *Objetivos de Control para la Información y Tecnología Relacionada, COBIT-ISACF, 1998.*

Disponibles en la Web:

[CERT]: Center of Internet security expertise, located at the Software Engineering Institute, Carnegie Mellon University, 2006, http://www.cert.org/

[ISACA]: http://www.isaca.org/; Serving IT Governace Professionals

[COSO]: The Committee of Sponsoring Organizations of the Treadway Commission, 1985-2005, http://www.coso.org

[SIGEN]: Sindicatura General de la Nación, PEN, Argentina, http://www.sigen.gov.ar

[i] NTIC, nuevas tecnologías de la información y de la comunicación.

[ii] Information System Audit and Control Foundation, pág. 6, 1998.-

[iii] MAD: Management Awareness Diagnostic, Diagnóstico de Sensibilidad Gerencial.
[iv] ITCD: IT Control Diagnostic, Diagnóstico de Control en TI
[v] Reproducción de pág. 7, Information System audit and Control Foundation, 1998.-
[vi] TIC: Tecnología de Información y Comunicación.
[vii] **MAGERIT,** Consejo Superior de Informática, Ministerio de Administraciones Públicas de España; http://www.csi.map.es/csi/pg5m20.htm
[viii] RIS2K es un producto de software que consta de tres Guías y de una herramienta de apoyo sobre plataforma PC, presentados todos ellos en un CD-ROM, publicado por el Ministerio de Administraciones Públicas, España, ISBN: 84-87366-61-9.
[ix] Ley 24176 Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y las Normas de Control Interno para Tecnologías de la Información – ANEXO I, Res. N° 48/05 SIGEN.
[x] **Decreto 2.628/2002,** implementa "FIRMA DIGITAL", con los siguientes lineamientos: Reglamentación de la Ley N° 25.506. Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional.
[xi] Corresponde a los documentos que forman parte del ANEXO correspondiente a la Ordenanza de Consejo Superior de la UNCuyo, sobre: PESUPUESTO 2006.
[xii] **Ley 25.506, "**LEY DE FIRMA DIGITAL", promulgada el 11/12/2001 y cuyo contenido se refiere a: Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones complementarias.
[xiii] **ISO 27001:** the ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for an ISMS, and Information Security Management System. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world. ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification.
[xiv] Entiéndase Riesgo Residual, como el riesgo que queda después del tratamiento del mismo riesgo.
[xv] SIC; Sistema de Información y Comunicación