ESCUELA POLITECNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

ANÁLISIS Y GESTIÓN DE RIESGOS PARA LA ELABORACIÓN DE PLANES DE CONTINGENCIA EN LOS SISTEMAS DE INFORMACIÓN DE LA ESPEL.

PROYECTO PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS E INFORMATICA

WELLINGTON BLADIMIR MONTES TACO.

EDUARDO GABRIEL BALAREZO VARGAS

Latacunga, Octubre del 2003

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por Eduardo Gabriel Balarezo Vargas y Wellington Bladimir Montes Taco, bajo nuestra supervisión .

Ing. Edison Espinoza

DIRECTOR DE PROYECTO

Ing. Fabián Montaluiza

CODIRECTOR DE PROYECTO

DEDICATORIA

El presente trabajo va dedicado a mis padres quienes con su apoyo tanto moral como economico supieron apoyarme en la culminacion de mis estudio; a mis hermanas quienes supieron incentivarme a seguir adelante para alcanzar mis metas.

Eduardo Balarezo V.

AGRADECIMIENTO

Agradezco de un manera especial a dios por haberme dado la dicha de tener uno excelentes padres quienes fueron una verdadera guía y ejemplo para llegar a cumplir con mis objetivos.

Al personal docente de la facultad quienes con sus conocimientos y experiencias fueron la guía para la culminación de esta carrera

Eduardo Balarezo V.

DEDICATORIA

De una manera especial a mi Madre que siempre me dio su apoyo incondincional, impartiendome sus consejos y comprensión para darme lo mejor de ella; a mi Padre y Hermanos que me apoyaron en mi vida estudiantil, la cual hicieron lo posible, que con entero sacrificio y abnegación supieron entregar todo de si para la culminación de mis estudios.

Wellington Montes T.

AGRADECIMIENTO

Agradezco a Dios que por medio de su voluntad me dio la vida, para culminar uno mas de mis objetivos, como el de llegar ha ser un profesional y poder prestar mis servicios a la sociedad.

A mis Padres, Hermanos y Esposa por el apoyo brindado durante mi carrera estudiantil, a mis profesores por su labor de educación brindada y a la ESPEL que me acogido durante mis estudios, brindándome los conocimientos necesarios.

A todas las personas que por sus sabios consejos me supieron apoyar en esta vida estudiantil

Wellington Montes T.

INDICE

CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

LISTADO DE ANEXOS

RESUMEN

Para que una organización funcione correctamente y alcance los objetivos propuestos por la Dirección son necesarios unos activos o recursos; estos recursos pueden ser humanos, materiales (edificios, instalaciones, hardware, etc.) e inmateriales (software, conocimiento acumulado, credibilidad o buena imagen, etc.).

Todos estos recursos se encuentran en un entorno de incertidumbre, que en ocasiones puede mostrase agresivo y provocar interrupciones inesperadas del funcionamiento normal de la actividad del Departamento Administrativo en la ESPEL.

La mayor parte de estas interrupciones suelen ser temporales y las condiciones vuelven a ser normales en un período que no ocasiona situaciones críticas para la actividad normal de la empresa. Sin embargo, puede haber circunstancias que generen interrupciones prolongadas, que lleguen a influir en la capacidad de funcionamiento de los servicios o impidan el desarrollo normal de los mismos en los locales habituales.

Para prever las consecuencias de estas situaciones y definir las estrategias que aseguren la continuidad de la actividad en el menor tiempo y con el menor trastorno posible, se hace preciso la elaboración de planes de contingencia o de reanudación para las distintas actividades del Departamento Administrativo con el fin de:

- Asegurar que todos los recursos conocidos y disponibles se utilizan para recuperar las funciones de la actividad tras una emergencia o desastre que haya afectado al edificio actual.

- Proporcionar un conjunto de procedimientos que serán ejecutados para restablecer los procesos prioritarios lo antes posible y con el menor impacto sobre la actividad, empleados y estudiantes de la ESPEL.

Como se ha indicado anteriormente, para que una organización funcione correctamente y alcance los objetivos propuestos por la Dirección son necesarios unos activos o recursos, que pueden ser humanos, materiales (edificios, instalaciones, hardware, etc.) e inmateriales (software, conocimiento acumulado, credibilidad o buena imagen, etc.)

El Riesgo es la probabilidad de que se produzca un impacto determinado en un activo, en una parte de la organización o en toda ella.

Fruto de una decisión y con el objeto de reducir el riesgo surge un conjunto de acciones que constituyen la Función de Salvaguarda, que se materializa en el correspondiente Mecanismo de Salvaguarda o conjunto de procedimientos o dispositivos que reducen el riesgo y que opera de dos formas posibles, que son, en general, alternativas:

- Neutralizando otra acción: la amenaza
- Modificando el estado de seguridad del activo agredido con reducción posterior al evento productor de dicho impacto.

Resulta imposible garantizar que no ocurran hechos imprevistos que provoquen desastres, por lo que una de las finalidades de estos planes consiste en minimizar la ocurrencia de éstos, así como tener definida y poner en marcha la organización necesaria para poder aplicar las acciones, procedimientos y recursos para la vuelta a la normalidad en el menor tiempo posible.

PRESENTACIÓN

La presente Tesis pretende describir, analizar y evaluar los principales aspectos relativos al análisis y gestión de riesgos de los Sistemas de Información, con el objetivo de elaborar un plan de contingencia como mecanismo de salvaguarda en las amenazas con mayor riesgo.

El alcance de esta tesis contempla los mecanismos de salvaguarda en el Departamento Administrativo ya sea en el Entorno, Sistemas de Información, Funciones e Información.

Los servicios contemplados en esta tesis son de dos tipos:

- Realización del análisis y gestión de riesgos en los Sistemas de Información.
- Selección de los mecanismos de salvaguarda como Plan de Contingencia.
- Aplicación del estudio a la herramienta RIS2K

Ponemos a disposición de ustedes “ANALISIS Y GESTION DE RIESGOS PARA LA ELABORACION DE PLANES DE CONTINGENCIA EN LOS SISTEMAS DE INFORMACIÓN DE LA ESPEL”

I.- GENERALIDADES

1.1.- GESTIÓN GLOBAL DE SEGURIDAD

La Gestión global de Seguridad de un Sistema de Información determinado es una acción permanente, cíclica y recurrente (es decir, se ha de reemprender continuamente debido a los cambios del sistema y de su entorno) que se descompone en Fases sucesivas.

1.2.- ESTRATEGIA / POLÍTICA DE SEGURIDAD

El establecimiento de una Estrategia de seguridad en los niveles directivos máximos de una Organización y de la consecuente Política de Seguridad puede verse como parte de las salvaguardas.

Los recursos a emplear en salvaguardas de seguridad para sistemas de información deben compararse con los costes derivados de los riesgos que implican impactos en los activos.

Los riesgos y salvaguardas de la Organización se deben revisar cuando sea adecuado y sistemáticamente como una parte más de la gestión de los cambios de la Organización.

La valoración de riesgos considera, tanto la vulnerabilidad y probabilidad real de que la amenaza prevalezca frente a las salvaguardas implantadas y se materialice, como el impacto en los activos de la Organización que resulte de dicha vulnerabilidad.

El resultado de esta valoración global orienta al responsable de seguridad de la información y determina la dirección adecuada de sus acciones y de sus prioridades para implantar las salvaguardas necesarias.

Las siguientes condiciones suelen ser importantes para tener una buena implantación de seguridad de los sistemas de información dentro de una Organización:

- Los objetivos y las acciones en materia de Seguridad deben basarse en los objetivos y necesidades de la Organización.
- Deberá existir un apoyo visible y el compromiso de la alta dirección con la seguridad, así como una dirección de ésta con suficiente nivel orgánico.
- Deberá haber una buena comprensión en la Organización de los niveles y riesgos en materia de seguridad dentro de la organización.
- Debe 'venderse' la seguridad eficazmente a todos los directivos y empleados.
- Debe distribuirse a todos los directivos y empleados una norma adecuada sobre la política y los estándares de seguridad existentes en la Organización.

1.3.- ORGANIZACIÓN DE LA SEGURIDAD

La Seguridad es una responsabilidad de la Organización que ha de compartirse por todos los miembros de su Equipo Directivo. El establecimiento de un Comité superior de Seguridad de sus Sistemas de Información permite asegurar la persistencia de una orientación clara y de un apoyo visible del Equipo Directivo a las iniciativas de Seguridad.

Las cuestiones a tratar por el Comité superior de Seguridad deberán referirse a los siguientes:

- Revisar y aprobar las normas de seguridad de los Sistemas de Información en la organización, así como las responsabilidades derivadas de aquéllas.
- Evaluar de forma periódica el grado de exposición a riesgos que afecten a los activos esenciales para la organización.
- Aprobar los proyectos y soluciones de alto coste o repercusión propuestos para mejorar la seguridad de la Información en la organización.

1.4.- ACCESO A LOS SISTEMAS DE INFORMACIÓN

Con el objetivo de prevenir accesos no autorizados a los sistemas de información, se debe empezar por insistir que el control de acceso a los activos, servicios o datos de los sistemas de información ha de responder a los requerimientos del funcionamiento de la organización establecidos en su política de seguridad, teniendo en cuenta las normativas de protección y distribución de la información en todos los niveles corporativo y departamentales, así como los requisitos contractuales o legales para proteger dicho acceso.

Para lograr una protección efectiva, se necesita la cooperación de los usuarios autorizados. Éstos deben saber su responsabilidad en el mantenimiento de la eficacia de los controles de acceso (sus contraseñas, claves secretas de acceso o passwords) y en la seguridad del material que se pone a su disposición (expedientes, ordenadores personales, listados, etc.)

Para proteger la información frente a accesos no autorizados, pérdida, robo u otros daños, la Organización adoptará una política de conservación de la información (documentos, disquetes, etc.) dentro y fuera del horario normal de trabajo. Sobre todo la información que queda encima de las mesas puede perderse o incluso destruirse. Para evitarlo se deben aplicar las siguientes medidas o mecanismos de salvaguarda:

- Los documentos y disquetes deben guardarse en armarios cuando no se usen y especialmente fuera del horario normal de trabajo.
- La información crítica o sensible debe encerrarse bajo llave cuando no se requiera especialmente o la oficina esté vacía (lo mejor es almacenarla en un armario ignífugo).
- Los computadores personales y los terminales deben estar protegidos por llave, contraseñas u otras salvaguardas cuando no se usen.

- Se debe proteger la entrada y salida de correo, así como los puntos de fax desatendidos.

1.5.- SALVAGUARDAS LIGADAS AL PERSONAL

La seguridad debe contemplarse desde las etapas de selección de las personas e incluirse en los contratos y definiciones de puestos de trabajo para poder cumplir el Objetivo de reducir los riesgos derivados de actuaciones humanas (errores, robos, fraudes o mal uso de las aplicaciones por ejemplo).

Los procesos de selección de recursos humanos para puestos que impliquen acceso a información considerada como sensible por la Organización deben contar con suficientes garantías. La Organización debe al menos:

- Examinar cuidadosamente el Curriculum Vitae del candidato.
- Contrastar los datos personales y de identificación: C.I, Pasaporte.
- Verificar la información sobre su trabajo en Organizaciones anteriores.
- Acreditar las certificaciones académicas.
- Analizar las garantías para puestos especialmente sensibles (control de finanzas, etc.)

Los nuevos empleados que vayan a ser usuarios de los sistemas de información de la Organización deben firmar con la Organización cláusulas de seguridad (al menos de confidencialidad) como parte de sus condiciones iniciales de trabajo.

Con objeto de garantizar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de los sistemas de información y que están preparados para asegurar la Política de seguridad de la Organización en el curso

normal de su trabajo, deberán recibir formación sobre seguridad y uso correcto de los sistemas de información y de sus facilidades.

Todos los empleados de la Organización y sus contratados externos deben conocer los procedimientos para realizar y remitir informes sobre los diferentes tipos de incidentes e infracciones en materia de seguridad; las amenazas, vulnerabilidades o simplemente el mal funcionamiento que puedan tener impacto en la seguridad de los activos de la Organización.

La Organización debe establecer y mantener un procedimiento formal de informes sobre incidentes de seguridad dirigido a centros de responsabilidad definidos, así como el procedimiento de la respuesta a la recepción del informe sobre dichos incidentes, que permita ajustar la acción a tomar.

1.6.- SEGURIDAD FÍSICA

Los requerimientos sobre seguridad física varían considerablemente según las Organizaciones y dependen de la escala y la organización de los sistemas de información, así como de la sensibilidad de la Organización y de la criticidad de su funcionamiento. Así, una gran Organización con tendencia a la centralización informática requerirá normalmente mucho más nivel de seguridad física que una pequeña Organización que use microinformática.

Pero son aplicables universalmente los conceptos de asegurar áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de seguridad.

1.7.- NORMAS DE PROTECCIÓN E INTERCAMBIO

La Protección de Información, tomada en sentido estricto, consiste en la especificación de un nivel elevado de los Subestados de Autenticación y Confidencialidad de los Activos de tipo Información sobre todo. Para conseguir estos niveles, la Organización debe implantar mecanismos de salvaguarda de

carácter organizativo, técnico y documental; mecanismos que se han de atener incluso a normas legislativas en ciertos casos (por ejemplo, por razón de la naturaleza de la información o de las organizaciones que los manejan).

1.8.- SEGURIDAD EN NODOS Y REDES

Debe tenerse en cuenta de entrada que los niveles de detalle y de formalización de los procedimientos requeridos para manejar y operar las instalaciones de servidores centrales y de redes variarán considerablemente según el tipo de equipos, el tamaño de la Organización, la naturaleza de su funcionamiento y la criticidad de las aplicaciones.

II.- DESCRIPCION DE LA METODOLOGIA MAGERIT

2.1.- INTRODUCCIÓN

2.1.1.- INTRODUCCIÓN A MAGERIT

El Consejo Superior de Informática de España ha elaborado la Metodología de Análisis y GEstión de Riesgos de los sistemas de Información de las administraciones Públicas, MAGERIT, cuya utilización promueve, como respuesta a la dependencia creciente de éstas (y en general de toda la sociedad) de las tecnologías de la información.

La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generen confianza cuando se utilicen tales medios.

2.1.2.- OBJETIVOS DE MAGERIT

El método MAGERIT tiene un objetivo inmediato doble**:**

• Estudiar los riesgos que soporta un determinado sistema de información (SI) y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la acepción habitual del término.

• Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

2.1.3.- ELEMENTOS DE MAGERIT

Para conseguir estos objetivos, MAGERIT tiene una estructura con dos tipos de elementos:

- Un conjunto de Guías.

- Un panel de herramientas de apoyo.

Esta estructura de MAGERIT permite realizar:

- El análisis de los riesgos para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el Sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

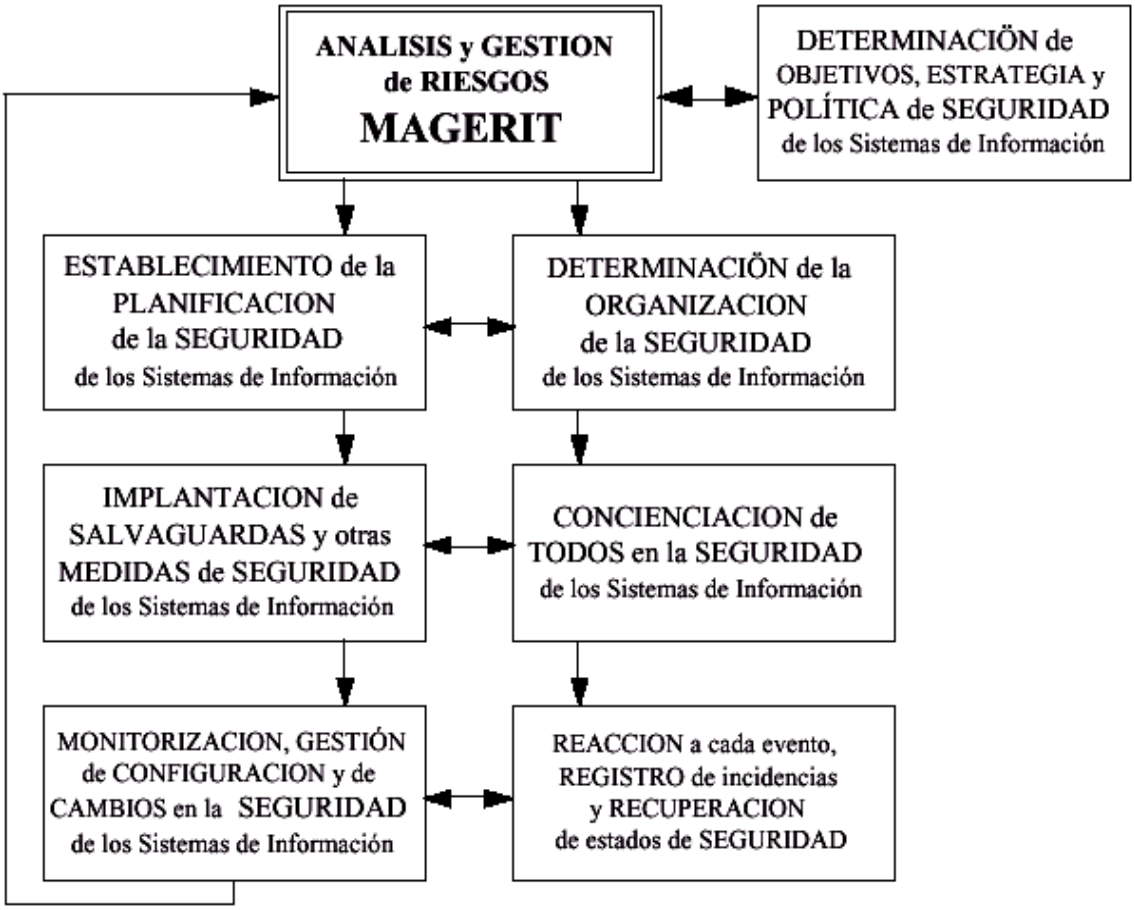
- La gestión de los riesgos, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

2.2.- EL MODELO MAGERIT

2.2.1.- ENCUADRE DE MAGERIT EN LA GESTION DE LA SEGURIDAD DE LOS SI

MAGERIT, como método de Análisis y Gestión de Riesgos, cubre sólo una Fase de la GESTIÓN global de la Seguridad de un Sistema de Información determinado. La Gestión global de Seguridad (representada en la figura siguiente) es una acción permanente, cíclica y recurrente (es decir, se ha de reemprender continuamente debido a los cambios del sistema y de su entorno).

Figura 2.1 Magerit en la gestión de la seguridad



El ANÁLISIS Y GESTIÓN DE RIESGOS, Fase nuclear de 'medición' y cálculo en el ciclo de gestión de la seguridad, es punto de arranque del ciclo de Gestión de Seguridad y además requiere técnicas de proceso especiales (propias del ámbito de la seguridad).

• La Fase de Determinación de OBJETIVOS, ESTRATEGIA y POLÍTICA de Seguridad de los Sistemas de Información se nutre de y nutre a su vez la Fase de Análisis y Gestión de Riesgos.

• La Fase de Establecimiento de la PLANIFICACION de la Seguridad de los Sistemas de Información deriva de la Fase de Análisis y Gestión de Riesgos como su consecuencia funcional más inmediata.

• La Fase de Determinación de la ORGANIZACION de la Seguridad de los Sistemas de Información deriva de la Fase de Análisis y Gestión de Riesgos como su consecuencia orgánica más inmediata.

• La Fase de IMPLANTACION de SALVAGUARDAS y otras medidas de Seguridad para los Sistemas de Información deriva de las Fases de Planificación y Organización.

• La Fase de CONCIENCIACIÓN de TODOS en la SEGURIDAD de los Sistemas de Información deriva de las Fases de Planificación y Organización. Tiene en cuenta el papel fundamental del recurso humano interno en todo proyecto de seguridad.

• La Fase de REACCIÓN a cada evento, de MANEJO y REGISTRO de las incidencias y de RECUPERACIÓN de Estados aceptables de Seguridad tiene un carácter básicamente operacional.

• La Fase de MONITORIZACIÓN, GESTIÓN de CONFIGURACIÓN y de CAMBIOS en la Seguridad de los Sistemas de Información tiene un carácter básicamente de mantenimiento.

2.2.2.- MAGERIT EN PROYECTOS DE COMPLEJIDAD MEDIA Y ALTA

Los proyectos de complejidad media o alta en materia de seguridad requieren la realización de más de un ciclo de Gestión global de seguridad (figura siguiente). La primera aplicación del ciclo de Gestión abarca todo el sistema en estudio: arranca de la fase de Análisis y Gestión de Riesgos, enfocada a grandes rasgos para conseguir una primera dicotomía o clasificación en dos grandes bloques de los componentes del sistema:

• Los componentes que implican riesgos menores, a los que bastará aplicar globalmente medidas básicas de seguridad ‘práctica’.

- Los componentes que implican riesgos mayores, a cada uno de los cuales será necesario aplicar un nuevo Análisis y Gestión de Riesgos más detallado.

Esta primera aplicación ofrece así una primera visión sintética de la seguridad con ayuda de las otras fases del ciclo de Gestión de Seguridad, es decir:

Una Determinación global de Objetivos, Estrategia y Política de Seguridad.

- Una Planificación inicial de la Seguridad.

- Una primera determinación de la Organización necesaria para la Seguridad.

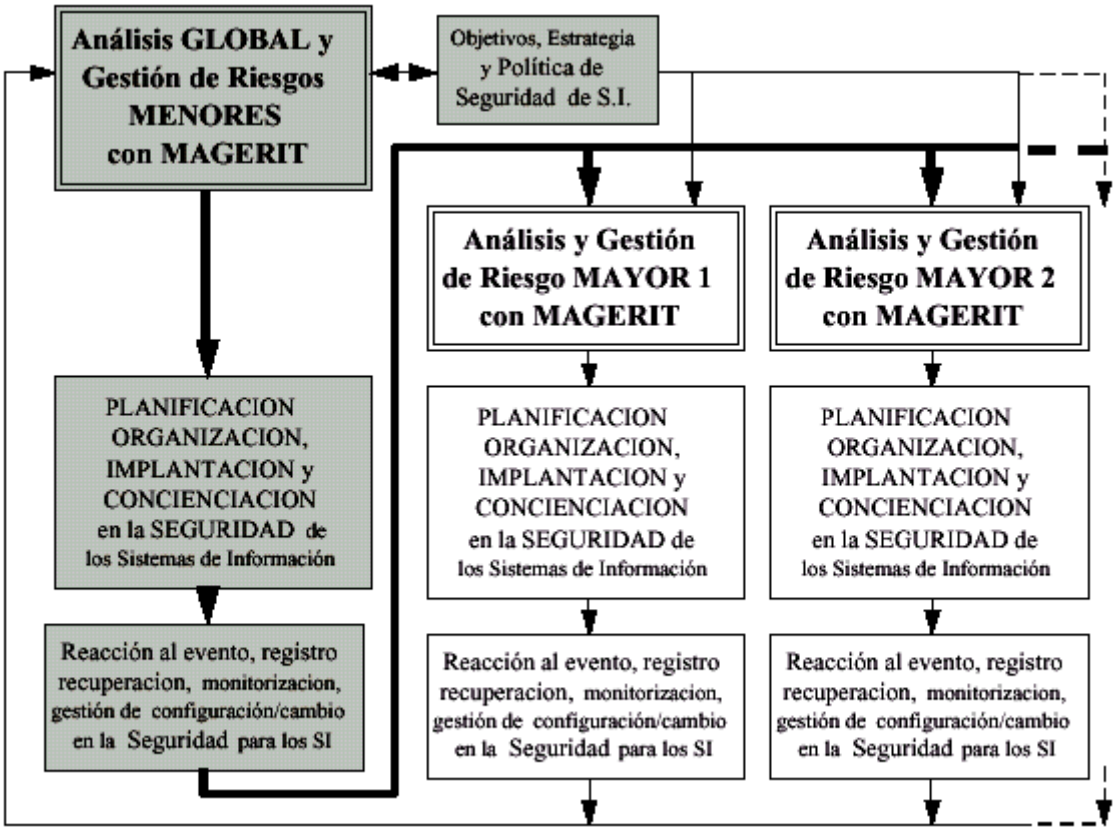
- La Implantación de las Salvaguardas generales en los componentes de riesgos bajos.

- La concienciación.

- El Entrenamiento a la participación en la Seguridad de componentes de riesgos bajos.

- La preparación a la Reacción ante cada evento, el manejo y registro de las incidencias y la recuperación de Estados aceptables de Seguridad ligados a los componentes de riesgo bajo.

Figura 2.2 Magerit en proyectos de complejidad media y alta



Las aplicaciones siguientes del ciclo de gestión de seguridad a los componentes retenidos por sus riesgos mayores arrancan de la Fase de Análisis y Gestión de Riesgos, enfocada con un detalle proporcionado al riesgo detectado, relacionando el beneficio esperado con el coste de la aplicación de todas las fases del ciclo la gestión de seguridad.

2.2.3.- ESTRUCTURA DE LA FASE DE ANÁLISIS Y GESTIÓN DE RIESGOS

El método MAGERIT se empieza por definir aquí en su nivel más genérico (para que pueda adaptarse a cada situación concreta como se verá en todas las ocasiones necesarias). MAGERIT maneja así una visión estratégica global sobre la Seguridad de los Sistemas de Información, visión que arranca de un Modelo de Análisis y Gestión de Riesgos que comprende 3 Submodelos:

- Submodelo de Elementos

- Submodelo de Eventos

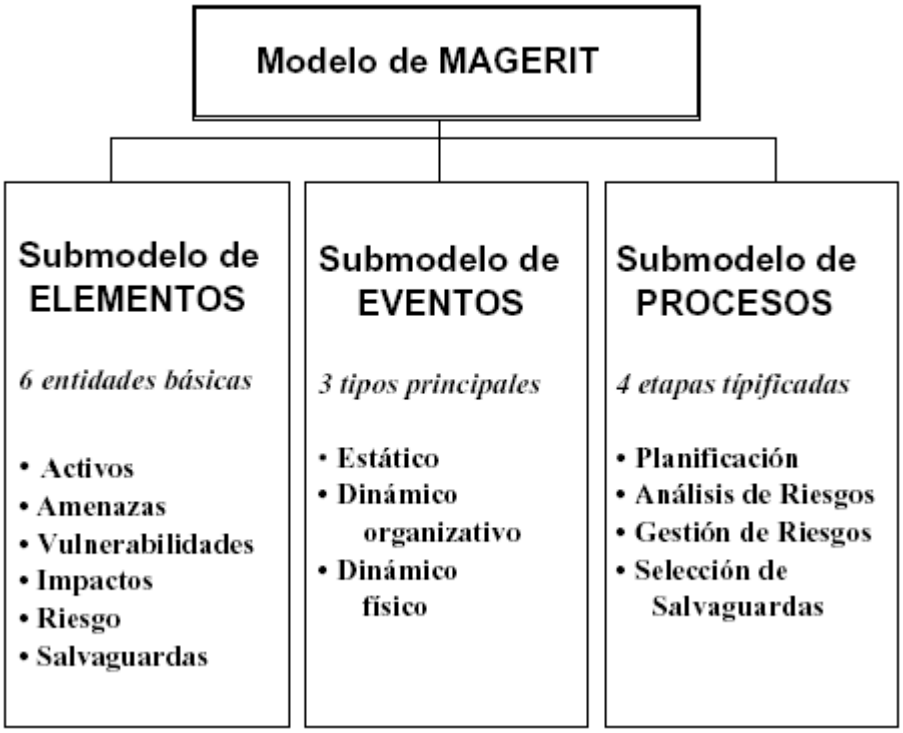
- Submodelo de Procesos.

El Submodelo de Elementos proporciona los ‘componentes’ que el Submodelo de Eventos relacionará entre sí y con el tiempo, mientras que el Submodelo de Procesos es la descripción funcional (el ‘esquema explicativo’) del proyecto de seguridad a construir.

Para construir un proyecto de seguridad específico, el ‘esquema’, es decir el Submodelo de Procesos, ayuda por una parte a seguir el procedimiento general y por otra a adaptarlo al problema concreto, teniendo siempre en cuenta la Política de seguridad que haya marcado la Dirección de la Entidad afectada.

El Procedimiento particularizado para el proyecto concreto de seguridad determina las Funciones y Servicios de Salvaguarda adecuados a los problemas detectados al aplicar el método e indica tipos de Mecanismos de Salvaguarda para resolverlos. Aunque no forman parte de MAGERIT, éste prepara la Planificación, la Organización y las otras fases posteriores necesarias para implementar y explotar adecuadamente dichos Mecanismos.

Figura 2.3 Modelo de Magerit



2.3.- SUBMODELO DE ELEMENTOS

El Submodelo de Elementos de MAGERIT comprende las seis Entidades básicas siguientes, así como sus procesos de adquisición y actualización:

- Activos
- Amenazas
- Vulnerabilidades
- Impactos
- Riesgos
- Salvaguardas (Funciones, Servicios y Mecanismos)

2.3.1.- ACTIVOS

Los Activos del Dominio, "recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione

correctamente y alcance los objetivos propuestos por su dirección" se pueden así estructurar en 5 categorías:

1.- El entorno del Sistema de Información necesario para su funcionamiento: instalación física, infraestructura de comunicaciones y otras, suministros, personal operacional o desarrollador de aplicaciones.

2.- El sistema de información (hardware, redes propias, software básico, aplicaciones)

3.- La propia información

4.- Las funcionalidades de la organización que justifican y dan finalidad a la existencia de los Sistemas de Información, incluido el personal usuario o los objetivos propuestos por la dirección.

5.- Otros Activos (por ejemplo la credibilidad de una persona jurídica o física, su intimidad, la imagen ...).

A su vez, cada activo (o bien 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.

El fallo de un Activo de una categoría o nivel' pueden generar 'cadenas' de fallos en otros niveles. 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).

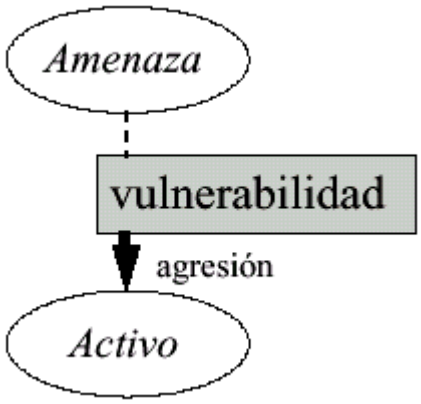
2.3.2.- AMENAZAS

Se definen como "los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos". Las Amenazas se pueden materializar y transformarse en agresiones. MAGERIT ve las Amenazas bajo un enfoque dinámico, o sea como acciones capaces de modificar el 'Estado de seguridad' del Activo amenazable; acciones de tipo 'evento', pues hay otras de tipo 'decisión' humana.

2.3.3 VULNERABILIDADES

Definida como la "ocurrencia real de materialización de una Amenaza sobre un Activo", la Vulnerabilidad es una propiedad de la relación entre un Activo y una Amenaza. Ejerce entre ambos una función de 'mediación' en el cambio del 'estado de seguridad' del Activo; siendo también el mecanismo de paso desde la Amenaza a la Agresión materializada. La Vulnerabilidad tiene así dos aspectos: el estático, ligado a la función (forma parte del 'estado de seguridad' del Activo); y el dinámico, ligado al mecanismo (convierte la Amenaza en agresión).

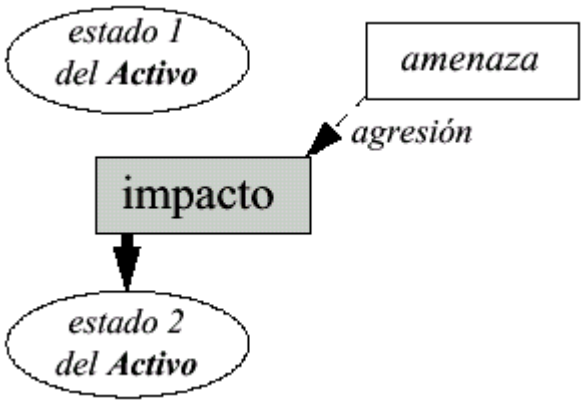
Figura 2.4 Vulnerabilidad



2.3.4.- IMPACTOS

Se define como "daño producido a la organización por un posible incidente" y es el resultado de la Agresión sobre el Activo, o visto de manera más dinámica, "la diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento". MAGERIT clasifica los Impactos sobre los Activos a partir de sus consecuencias: o Pérdidas bien Cualitativas; por reducción de subestados de seguridad. El Impacto puede ser cuantitativo (sí representa Pérdidas cuantitativas monetarizables directas o indirectas); cuantitativo con pérdidas orgánicas (por ejemplo, de fondo de comercio, daño de personas); y cualitativo con pérdidas funcionales (o de los subestados de seguridad).

Figura 2.5 Impacto

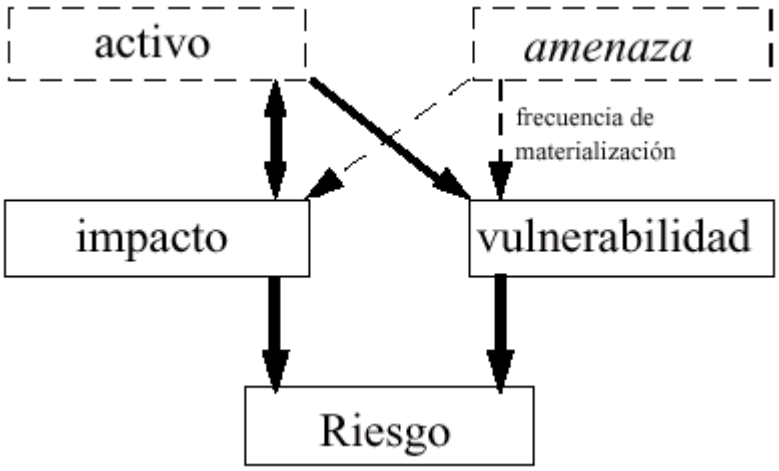


2.3.5.- RIESGO

Se ha definido como la "Posibilidad de que se produzca un impacto dado en la organización". Su importancia como resultado de todo el Análisis organizado sobre los Elementos anteriores (activos, amenazas, vulnerabilidades e impactos) queda velada por su apariencia como Indicador resultante de la combinación de la Vulnerabilidad y el Impacto que procede de La amenaza del activo.

Este riesgo calculado permite tomar decisiones racionales para cumplir el objetivo de seguridad de la organización. Para dar soporte a dichas decisiones, el riesgo calculado se compara con el umbral de riesgo, un nivel determinado con ayuda de la política de seguridad de la Organización. Un riesgo calculado superior al umbral implica una decisión de reducción de riesgo. Un riesgo calculado inferior al umbral queda como un riesgo residual que se considera asumible.

Figura 2.6 Riesgo



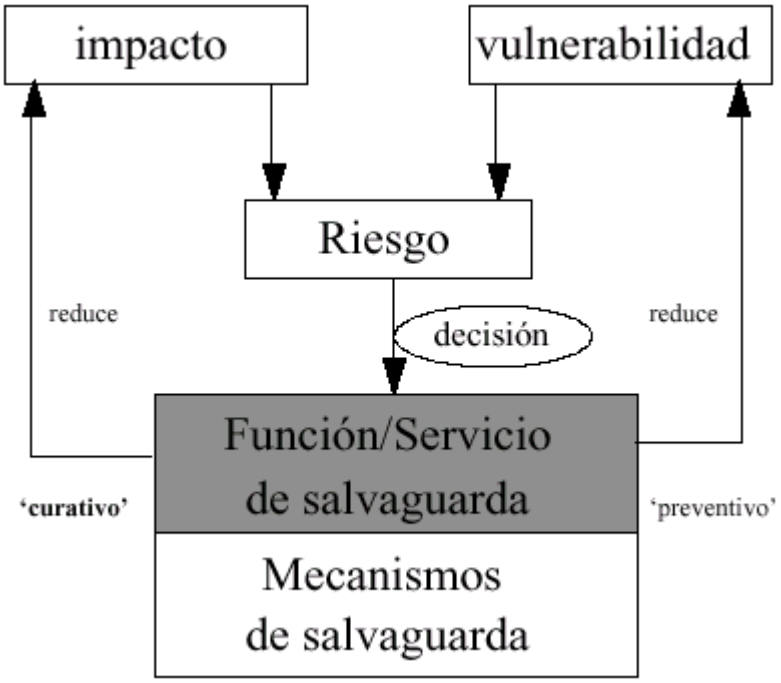
2.3.6.- FUNCIONES, SERVICIOS Y MECANISMOS DE SALVAGUARDA

Para reducir el riesgo se necesita la implantación de salvaguardas existentes o la incorporación de otras nuevas. MAGERIT distingue entre la organización abstracta llamada función o servicio de salvaguarda y la organización concreta llamada mecanismo de salvaguarda. Se define la función o servicio de salvaguarda como "reducción del riesgo"; y el mecanismo de salvaguarda como "dispositivo, físico o lógico, capaz de reducir el riesgo". una función o servicio de salvaguarda es así una acción para reducir un riesgo de tipo actuación u omisión (es una acción fruto de una decisión, no de tipo evento). esa actuación se concreta en un mecanismo de salvaguarda que opera de dos formas:

- La salvaguarda preventiva ejerce como acción sobre la vulnerabilidad, 'neutralizando' otra acción, la materialización de la amenaza, antes de que actúe ésta (lo que es válido en general para amenazas de origen humano, sea por error o intencional).

- La salvaguarda curativa actúa sobre el impacto, modificando el estado de seguridad del activo agredido y reduciendo el resultado de la agresión; o sea después de ésta (lo que es válido en general para amenazas de tipo accidente).

Figura 2.7 Mecanismos de Salvaguarda



2.4.- SUBMODELO DE EVENTOS

2.4.1.- INTRODUCCIÓN AL SUBMODELO

Recordando de nuevo que el método MAGERIT se construye en torno a un Modelo de Análisis y Gestión de Riesgos que comprende 3 Submodelos:

- Submodelo de Elementos

- Submodelo de Eventos
- Submodelo de Procesos

Se ha venido presentando intuitivamente este submodelo en forma de 'ciudad amurallada': los Activos están dentro y las Amenazas son el enemigo exterior. Las salvaguardas existentes son las murallas y sus 'brechas' son las vulnerabilidades. El ataque de las amenazas aprovecha las brechas y causa impactos en los Activos. El reforzamiento de estas salvaguardas repara los Impactos y reduce las brechas-vulnerabilidades.

Este submodelo estático de eventos de seguridad cada vez está más superado, debido a los nuevos tipos de amenaza (sobre todo las intencionales, sean presenciales o teleactuadas). Los actuales Sistemas de Información se parecen a 'ciudades abiertas' casi 'sin fronteras' más que a 'ciudades amuralladas' cerradas y requieren salvaguardas más dinámicas y flexibles: en cada 'urbanización' de Activos hay que 'incrustar' mecanismos de salvaguarda dinámicos (que crezcan con la urbanización, la 'patrullen' y cambien de aspecto para burlar a unos agresores cada vez más inteligentes).

2.4.2.- VISTA ESTÁTICA RELACIONAL DEL SUBMODELO DE EVENTOS

Refleja las relaciones generales entre las 6 Entidades reseñadas en el Submodelo de Elementos. Se necesita para establecer el Modelo lógico de Datos que requieren las herramientas de apoyo a MAGERIT.

La vista estática relacional del Submodelo de Eventos recoge el esquema de las relaciones generales entre las entidades reseñadas en el Submodelo de Elementos preanalizado.

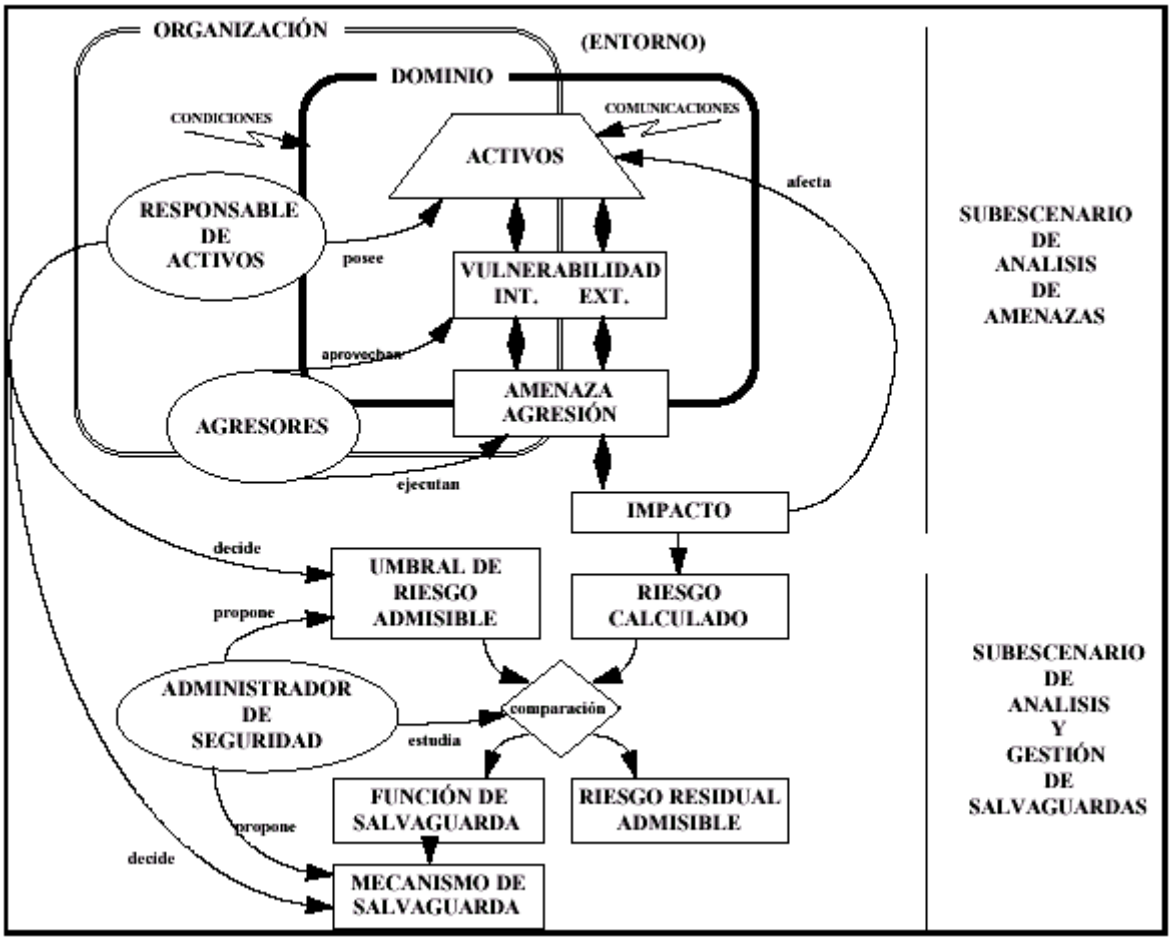
2.4.3.- VISTA DINÁMICA ORGANIZATIVA DEL SUBMODELO DE EVENTOS

Recoge el detalle de los 'escenarios' donde actúan los Elementos de MAGERIT. Esta vista se necesita para articular las técnicas de cálculo de riesgos y selección de salvaguardas, para dar soporte al Submodelo lógico de Procesos de MAGERIT, para estructurar sus Manuales de Procedimientos para los usuarios, así como para construir las herramientas de apoyo a la aplicación de MAGERIT.

El evento Amenaza desencadena, con cierta potencialidad propia o vulnerabilidad intrínseca (poco precisa y en general reducida), una o más posibles disfunciones y que se materializan como Impactos sobre los activos, según su vulnerabilidad a cada tipo de amenaza. El submodelo funciona dinámicamente como escenario de 'aseguramiento' (acción para obtener seguridad) con dos subescenarios.

Así y para cada Activo, el subescenario de 'ataque' empieza con una Amenaza como evento virtual o potencial. La vulnerabilidad específica asociada al 'Activo' para dicha Amenaza permite concretarla o no en una agresión. Esta desencadena distintos tipos de profundidad de Impacto: un deterioro del Activo, que puede concretarse en un daño y finalmente en una pérdida, valorables económicamente o no según sea el Activo.

Figura 2.8 Vista Dinámica del Submodelo de Eventos



2.4.4.- VISTA DINÁMICA 'FÍSICA' DEL SUBMODELO DE EVENTOS

La vista dinámica física recoge otra forma de articular los escenarios de funcionamiento de los Elementos de MAGERIT, asimilando el Submodelo de sus Elementos de Seguridad concretos a las Entidades y Relaciones más abstractas que se emplean en otros modelos físicos, cuyo funcionamiento está ampliamente experimentado y que ya están dotados de numerosas técnicas de análisis y de simulación así como de herramientas para su gestión. Esta vista se puede necesitar para dar soporte tanto a ciertas técnicas y herramientas sofisticadas de cálculo de riesgos y de selección de salvaguardas.

2.5.- SUBMODELO DE PROCESOS

2.5.1.- INTRODUCCIÓN AL SUBMODELO

El método MAGERIT se construye en torno a un Modelo de Análisis y Gestión de Riesgos que comprende 3 Submodelos:

- Submodelo de Elementos
- Submodelo de Eventos
- Submodelo de Procesos

2.5.2.- ESTRUCTURA DEL SUBMODELO

Para poder construir proyectos específicos de seguridad, MAGERIT posee interfaces básicas de enlace con Métrica versión 2.1. Como método de seguridad de tercera generación (es decir adaptado a unas amenazas crecientemente intencionales que usan cada vez más recursos lógicos), MAGERIT permite añadir durante el desarrollo del Sistema la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento. Estas interfaces tienen ventajas inmediatas: analizar la seguridad del Sistema antes de su desarrollo, incorporar defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema. MAGERIT enlaza con las Fases de Planificación, Análisis, Diseño, Construcción e Implantación de Métrica v.2.1.

2.5.3.- ETAPAS DE MAGERIT

El Submodelo de Procesos de MAGERIT comprende 4 Etapas:

1.- Planificación del Proyecto de Riesgos. Como consideraciones iniciales para arrancar el proyecto de análisis y gestión de riesgos, se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.

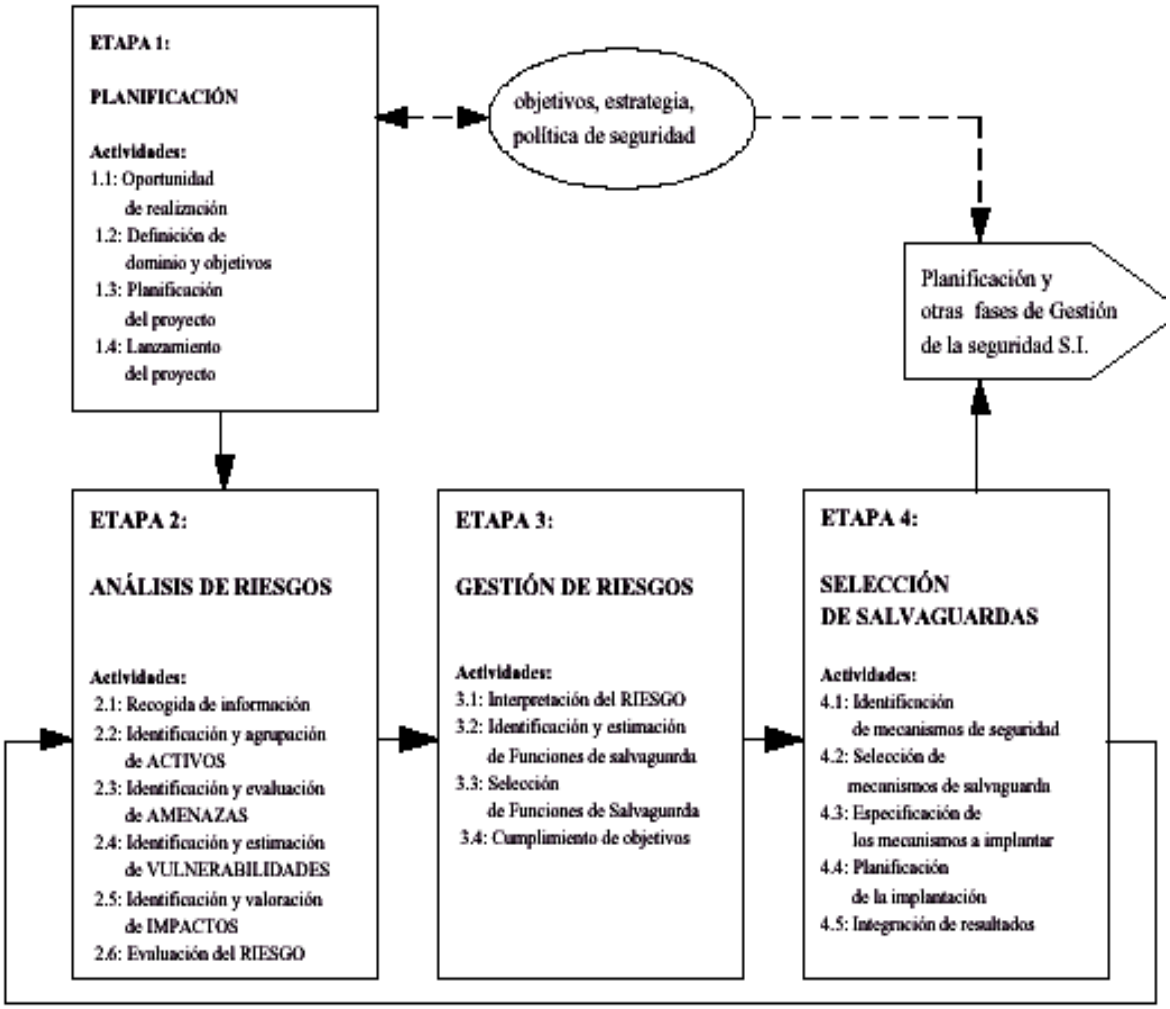
2.- Análisis de riesgos. Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.

3.- Gestión de riesgos. Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

4.- Selección de salvaguardas. Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del AGR, para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

2.5.4.- VISIÓN GLOBAL DE LAS ETAPAS DEL PROCESO MAGERIT

Figura 2.9 Visión global de Magerit

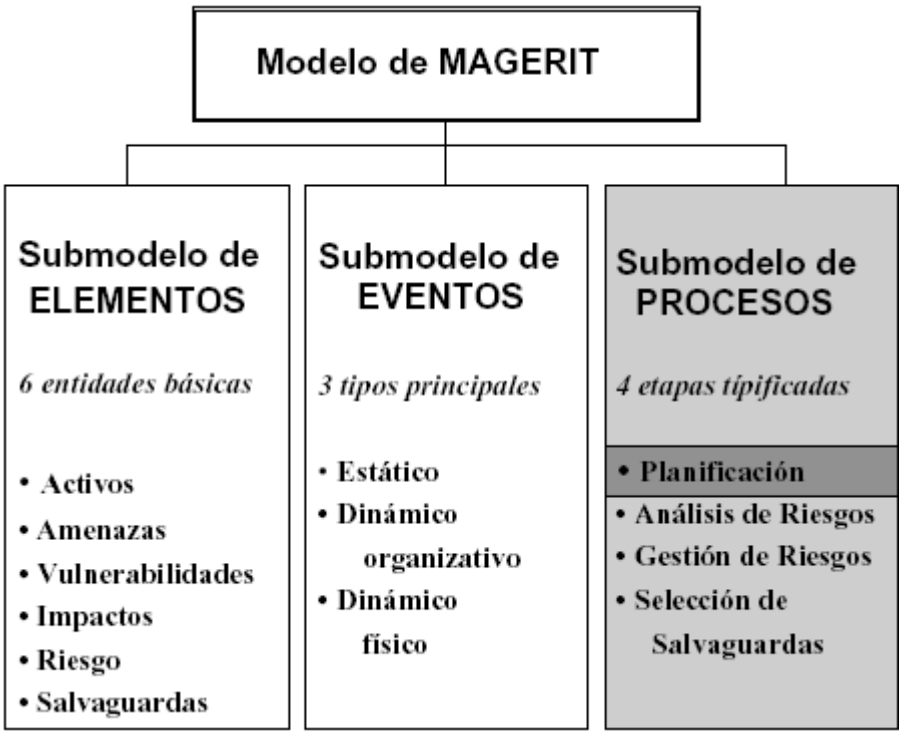


La figura representa el ciclo de etapas (iterativo) del proceso cubierto por MAGERIT que constituye la fase de análisis y gestión de riesgos dentro de la gestión de la seguridad de los sistemas de información. Asimismo se anotan los enlaces de este ciclo MAGERIT con la fase de 'Objetivos, Estrategia y Política de Seguridad' y con la fase de 'Planificación de los Mecanismos de Salvaguarda' (que inicia el resto de la Gestión de la Seguridad).

III.- PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS EN LA ESPEL

3.1.- UBICACIÓN DE LA ETAPA 1 EN EL MODELO DE MAGERIT

Figura 3.1 Ubicación de la Etapa1



3.2.- ESTRUCTURA DE LA ETAPA 1

PLANIFICACION

Actividades:

1.- Oportunidad de realización
2.- Definición de dominio y objetivos
3.- Planificación del proyecto
4.- Lanzamiento del proyecto

3.3.- VISIÓN GLOBAL DE LA ETAPA 1

El objetivo principal de esta etapa de planificación es establecer y definir el marco general de referencia para todo proyecto de realización de análisis y gestión de riesgos.

Esta etapa de planificación de análisis y gestión de riesgos se enmarca, como ocurre con cualquier otra planificación concreta, en la planificación estratégica de la organización, como una concreción a corto y medio plazo de ésta. No sólo será lógico, sino conveniente, que muchos de los conceptos de esta etapa de magerit retomen y readapten elementos de la fase 0 de planificación de sistemas de información de métrica v.2.1.

Para facilitar la lectura de este capítulo, se aclara el contenido diferenciado de tres términos usados: finalidad, meta y objetivo. La Organización tiene metas, así como sus subdivisiones (Unidades, departamentos, dominios, etc.); las funciones tienen finalidades (motivaciones intrínsecas); los proyectos y sus componentes (etapas, actividades, etc.) tienen objetivos (que no pueden ser contradictorios con las metas más amplias de la Organización o sus subdivisiones ni con las finalidades lógicas de sus funciones, pero que no se confunden con ambas).

3.4.- ACTIVIDAD 1: OPORTUNIDAD DE REALIZACIÓN

Esta actividad tiene por objetivo suscitar el interés de la Dirección de la Organización en la realización de un proyecto de Análisis y Gestión de Riesgos.
En la ESCUELA SUPERIOR POLITECNICA DEL EJERCITO – LATACUNGA la Dirección de la Organización suele ser consciente de las ventajas que aportan las técnicas electrónicas, informáticas y telemáticas a su funcionamiento, pero no de los nuevos problemas de seguridad que estas técnicas implican.

Tarea única: Clarificar la oportunidad de realización

Se ha elaborado un cuestionario-marco (documento poco sistematizable, luego externo al núcleo de productos de MAGERIT) para provocar la reflexión sobre aspectos de la seguridad de los Sistemas de Información por parte de los responsables de las Unidades. El cuestionario permite proceder a un examen superficial de la situación en cuanto a la seguridad de sus sistemas de información.

Cuestionario para los encargados de los sistemas de Información

CUESTIONARIO

OBJETIVO :

Conocer aspectos de la seguridad de los Sistemas de Información(Hardware, Software, Comunicación), para proponer la elaboración de un Plan de Contingencia en el Departamento Administrativo de la ESPEL.

Marcar con una X la respuesta seleccionada.

1.- Existen seguridades en los sistemas de información.

Si( ) No( )

2.- Existen incidentes relacionados con la seguridad en los Sistemas de Información.

Si( ) No( )

3.- La ausencia de seguridad en los Sistemas de Información afecta el cumplimiento correcto de la misión y funciones del Departamento Administrativo.

Si( ) No( )

4.- Hay reestructuraciones en los servicios proporcionados.

Si( ) No( )

5.- Hay cambios en la tecnología utilizada.
Si( ) No( )

6.- Se desarrollan nuevos Sistemas de Información en el Departamento Administrativo.
Si( ) No( )

7.- Esta de acuerdo con la Elaboración de un Plan de Contingencia para los Sistemas de Información en el Departamento Administrativo de la ESPEL.
Si( ) No( )

Informe entregado al jefe del departamento administrativo.

Clarificar la Oportunidad de realización

En la Escuela Superior Politécnica del Ejercito sede Latacunga, en la actualidad no se cuenta con mecanismos de seguridad en caso de que ocurra un daño o perjuicio en la seguridad de los sistemas de información, por lo que no estamos preparados para un evento de tal magnitud, ya que en el Departamento Administrativo de la ESPEL se cuenta con recursos de información muy importante.

Luego de revisar los cuestionarios efectuados a los técnicos encargados del manejo de los sistemas de información(Hardware, Software, Comunicaciones), y de las entrevistas con los mismos en el Departamento Administrativo, se ha encontrado dos puntos referentes a Seguridad:

- Existe escasez de seguridad en los Sistemas de Información.
- La inexistencia de un plan de Contingencia.

Para dar una solución se requiere un estudio de cierta profundidad.

El departamento Administrativo esta organizado por las siguientes unidades:

- Unidad de Administración de Personal
- Unidad de Finanzas
- Unidad Logística
- Unidad de Seguridad.

En cuanto al recurso Humano el Departamento Administrativo cuenta con 10 personas aproximadamente, además esta conformado por los siguientes recursos:

4 profesionales informáticos que manejan los sistemas de información, en el Departamento Administrativo actualmente cuenta con 7 ordenadores de marca distinta, un servidor en el Departamento de Organización y Sistemas como departamento de apoyo, además estos ordenadores están conectados a una red local interna de la ESPE-L .

Como misión importante del departamento esta administrar eficaz y permanentemente los recursos humanos, físicos, financieros y logísticos, por medio de una aplicación adecuada del proceso administrativo (planificación, organización, dirección, ejecución y control), a fin de impulsar el desarrollo de los departamentos de la Espe-ltga mediante la satisfacción de sus necesidades administrativas.

Se pretende Generar un plan de contingencia para los sistemas de información, haciendo esfuerzos especiales para garantizar la seguridad de la información, para este fin se ha conformado un equipo de trabajo de dos personas.

3.5.- ACTIVIDAD 2: DEFINICIÓN DE DOMINIO Y OBJETIVOS

Una vez que se ha constatado la oportunidad de realizar el proyecto de Análisis y Gestión de Riesgos y el apoyo por la Dirección, esta Actividad procede a identificar los objetivos que debe cumplir el proyecto y a definir su dominio y límites.

Tarea 2.1: Especificar los objetivos del proyecto

En el Departamento Administrativo de la ESPEL el objetivo básico es determinar el conjunto de acciones que debería realizar en caso de desastre (incendio, inundación, ...) para asegurar el servicio informático a sus usuarios hasta la vuelta a las circunstancias normales.

El proyecto tiene por tanto tres grandes objetivos, sistematizables en tres grandes fases:

- Planificación global de la seguridad
- Análisis de la situación actual y especificación de necesidades funcionales de seguridad.
- Diseño detallado de los Mecanismos de Salvaguarda como Plan de Contingencia.

Tarea 2.2: Definir el dominio y los límites del proyecto

El dominio del proyecto se centra en el Departamento Administrativo que esta conformada por las siguientes unidades:

- Administración de Personal Responsable: Mayor Bravo
- Finanzas Responsable: Alicia Navas
- Logística Responsable: Mayor Bravo

- Seguridad Responsable: Tnt Edison Hidalgo

El Departamento Administrativo depende directamente de la Dirección y del Departamento de Organización y Sistemas como apoyo.

Visto como es lógico desde el punto de vista de la Seguridad de sus Sistemas de Información tomados en el sentido más amplio posibles, es decir con todas las repercusiones sobre las funcionalidades del Departamento y sobre Activos abstractos que atañen a su misión.

Tarea 2.3: Identificar el entorno y las restricciones generales

DEPARTAMENTO ADMINISTRATIVO
MISION:

Constituirnos en departamento modelo, organizados en unidades administrativas funcionales, eficientes y guiados bajo un sólido plan estratégico, que contenga principios de calidad total.

FUNCIONES:

1.- Efectuar el seguimiento en los procesos de captación de recursos.

2.- Formular, ejecutar y evaluar estrategias para el cumplimiento de objetivos y Políticas relacionadas con el manejo de los recursos.

3.- Emitir informes y recomendaciones en el área de su compendia.

4.- Propender al autofinanciamiento.

5.- Optimizar el manejo financiero de la Sede.

6.- Diseñar un plan operativo priorizando las obras que serán ejecutadas.

7.- Elaborar y ejecutar el plan de construcciones e infraestructura.

8.- Realizar el mantenimiento de instalaciones y proporcionar servicios para la Institución.

9.- Planificar, coordinar, organizar y ejecutar las actividades de seguridad en la Institución.

10.- Reportar a la dirección.

Figura 3.2 Organigrama del Departamento Administrativo

UNIDAD DE ADMINISTRACIÓN DE PERSONAL

MISION:

Administrar los procesos de selección capacitación y evaluación, así como recomendar a la dirección de Recursos Humanos de la ESPE la reclasificación, ascensos y promoción del personal administrativo, civil, militar y docente del instituto.

FUNCIONES:

1.- Administrar la información sobre los recursos humanos

2. Determinar necesidades de personal.

3.- Realizar contratación y empleo.

4.- Administrar los procesos de selección, capacitación, evaluación del personal.

5.- Dar cumplimiento y mantener actualizado el manual de clasificación y valoración de puestos.

6.- Elaborar y actualizar permanentemente el proceso de evaluación del desempeño del personal

7.- Velar por el bienestar de la comunidad politécnica.

8.- Colaborar en la elaboración y actualización de manuales de procedimientos.

9.- Coordinar con los encargados de los servicios que presta la ESPE.

10.- Realizar el procesamiento de datos para la reclasificación, ascensos y promoción del personal.

11.- Custodiar la documentación reservada y confidencial del personal militar.

12.- Reportar al departamento Administrativo.

UNIDAD DE LOGISTICA:

MISION:

Lograr un adecuado control de los abastecimientos y servicios asignados al instituto de manera rápida y oportuna, así como su adquisición, almacenamiento y distribución.

FUNCIONES:

1.- Determinar las necesidades, realizar la obtención, registro, almacenamiento y distribución de abastecimiento e insumo, que aporten al desempeño profesional, docente y administrativo.

2.- Realizar una adecuada planificación y ejecución en el uso del transporte, de los lubricantes y combustibles, así como del mantenimiento de vehículos de la sede hasta el cuarto escalón.

3.- Satisfacer las necesidades de alimentación al personal docente, militar, administrativo y estudiantes.

4.- Planificar, dirigir, coordinar, supervisar y ejecutar labores de apoyo logístico a las diferentes dependencias de la Sede.

5.- Administrar el servicio de talleres (zapatería, sastrería, carpintería, etc).

6.- Administrar y garantizar la provisión de material bélico e Intendencia.

7.- Controlar los diferentes servicios (sauna, panadería, micromercado, etc).

8.- Brindar servicios médicos, odontológicos, de planificación familiar, de laboratorio clínico y farmacia al personal del instituto, registrando información de los pacientes.

9.- Administrar los servicios de comunicaciones del instituto.

10.- Reportar al Departamento Administrativo.

UNIDAD DE FINANZAS:

MISIÓN:

Dirigir , coordinar y controlar todos los procesos financieros de la Sede.

FUNCIONES:

1.- Planificar, organizar, dirigir, coordinar y controlar todas las actividades contables.

2.- Aplicar control interno sobre compromisos, gastos y desembolsos.

3.- Administra los almacenes y bodegas.

4.- Realizar el control de contabilidad de costos de producción.

5.- Realizar análisis de costos.

6.- Efectuar periódicamente el control de bienes.

7.- Elaborar estados financieros e informes.

8.- Realizar todas las demás actividades que la ley lo establece.

9.- Determinar stocks máximos y mínimos.

10.- Mantener un estado actualizado de los bienes de la institución.

11.- Establecer un sistema apropiado de control, mantenimiento, conservación y seguridad de bienes.

El alcance del Estudio previo, no se lo realiza a la unidad de seguridad por no existir sistemas de información en el mismo.

Tarea 2.4: Estimar dimensión, coste y retornos del proyecto

Los recursos a emplearse se detallan:

RECURSO FISICO Y LOGICO	COSTO
Computadora Personal.	$ 950.00
Windows 95/98(Laboratorios, Personal)	$ 48.00
Microsoft Office (Laboratorios, Personal)	$ 36.00
Herramientas MAGERIT, RIS2K (Dominio Público)	$ 0.00
TOTAL	$1034.00

RECURSO HUMANO	COSTO/MES
2 Ingenieros Sistemas	$400
2 Asesores	$500

Tiempo estimado 6 meses

Total de Recurso Humano = $4500

Total del Proyecto = 5534

En la Escuela Politécnica del Ejercito ESPE – Latacunga, esta dotada con el hardware y software necesarios, y se hallan disponibles para su uso, además contamos con la buena colaboración de las personas encargadas en manejar la información para la toma de información; cubriendo así todos los requerimientos por lo cual aprovecharemos de estos recursos para realizar esta investigación, efectuando un pedido formal a las autoridades pertinentes, así como también de información a través de Internet y el existente en nuestras máquinas personales.

Por lo anteriormente anotado podemos definir que el proyecto tiene viabilidad Técnica, Operativa y Económica.

3.6.- ACTIVIDAD 3: PLANIFICACIÓN DEL PROYECTO

Esta actividad estima los elementos de Planificación del proyecto, es decir sus cargas de trabajo, el grupo de usuarios, los participantes y su modo de actuación y el plan de trabajo para la realización del proyecto.

Tarea 3.1: Evaluar cargas y planificar entrevistas

En la ESPEL para la realización de la entrevista se solicitara una cita al entrevistado en un plazo que no deba ser mayor a 5 días laborables, con el fin de no retrazar el proyecto.

Para evaluar cargas el proyecto consta de 5 fases:

Fase 1. Planificación del análisis y gestión de riesgos en la ESPEL.
Fase 2 Análisis del Riesgo.
Fase 3 Gestión del Riesgo.
Fase 4 Plan de Contingencia, Selección de Mecanismos de Salvaguarda.
Fase 5. Aplicación del estudio realizado a la herramienta RIS2K.

Tarea 3.2: Organizar a los participantes

El proyecto para el Departamento Administrativo de la ESPEL esta constituida por los siguientes órganos:

Equipo de Estudio: Está constituido en este caso por un Director del Proyecto; y dos egresados en sistemas.
Grupo de usuarios: Está formado por los utilizadores, actuales, del Sistema de Información. En principio está formado por 4 responsables de las Áreas y Servicios del Departamento Administrativo de la ESPEL, descendiendo al nivel adecuado según las necesidades de información que se detecten durante el desarrollo del Estudio.

3.7.- ACTIVIDAD 4: LANZAMIENTO DEL PROYECTO

Esta actividad completa las tareas preparatorias del lanzamiento del proyecto de Análisis y Gestión de Riesgos: empezando por seleccionar y adaptar los cuestionarios que se utilizarán en la recogida de datos, así como especificar los

criterios y las técnicas concretas a emplear en el análisis y gestión de riesgos; y terminando por asignar los recursos necesarios para la realización del proyecto y por realizar la campaña informativa de sensibilización a los implicados en el proyecto.

Tarea 4.1: Adaptar los cuestionarios

Se ha realizado una adaptación de cuestionarios, debido a la especificidad de este proyecto y la recogida directa de información a los directivos y en los lugares potencialmente vulnerables. Los cuestionarios de la encuesta realizada deben verse por tanto más un recordatorio para el análisis que un documento a autorellenar directamente por los responsables del Dominio protegible.

La entrevista realizada a los responsables de sistemas informatizados se divide en dos grandes bloques, uno específico sobre las vulnerabilidades inherentes a las funciones propias del sistema en el servicio (y por tanto de respuestas poco estructuradas); y el otro genérico, a partir de una batería de preguntas que permite situar a cada servicio dentro de un cuadro homogéneo.
Este bloque genérico, único sintetizable a partir de las propias respuestas, se resume a continuación.

VULNERABILIDADES ORGANIZATIVAS

• ACCESO AL SISTEMA POR PERSONAS EXTERNAS
• DISPONIBILIDAD DE ACCESO AL SISTEMA (CAÍDAS, LENTITUD,...)
• OBTENCIÓN DE PRODUCTOS DEL SISTEMA
• ACCESO DE PERSONAS EXTERNAS AL RECINTO DE TERMINALES

VULNERABILIDADES TÉCNICAS

• AVERÍAS EN TERMINALES/IMPRESORAS: FRECUENCIA/SOLUCIÓN
• CORTES DE FLUIDO ELÉCTRICO
• CONTROL DEL SOPORTE PAPEL. ALMACENAMIENTO DE ÉSTE

VULNERABILIDADES 'HUMANAS'

• POSIBILIDAD FÍSICA DE ROBO/INUTILIZACIÓN DE RECURSOS
• ERRORES EN LA INTRODUCCIÓN DE DATOS
• INASISTENCIAS DE PERSONAL SIGNIFICATIVAS
• OBTENCIÓN DE INFORMACIÓN POR PERSONAS AJENAS
• CONOCIMIENTO DE LAS APLICACIONES
• USO INDEBIDO DE CLAVES DE USUARIO. BORRE DE ANTIGUAS
• INTERVENCIÓN DE INFORMÁTICOS EN CAMBIAR DATOS REALES

Tarea 4.2: Seleccionar criterios de evaluación y técnicas para el proyecto

La situación de la seguridad de los sistemas de información del Departamento Administrativo de la ESPEL es producto de la incorporación de las salvaguardas tomadas para prevenir o reducir unos riesgos hasta ahora no analizados de forma sistemática. Hasta ahora, no ha tenido fallos operacionales informáticos de envergadura que hayan forzado a tomar precauciones drásticas (también hubieran sido difíciles por su cuantía económica).

Sin embargo, la falta de análisis sobre riesgos no ha permitido priorizar hasta ahora estas numerosas medidas adquiridas, que en no pocos casos se están subempleando por falta de criterios de coste-beneficio sobre su uso. Dicho análisis permitirá racionalizar las medidas actuales y completarlas con algunas otras. El Estudio Previo encargado se basa parcialmente en esta situación paradójica de abundancia y a la vez carencia de medidas de seguridad. Lo que exige un Análisis global de riesgos para el que faltan actualmente ciertos elementos importantes (por ejemplo, un registro histórico de las contingencias anteriores).

Tarea 4.3: Asignar los recursos necesarios

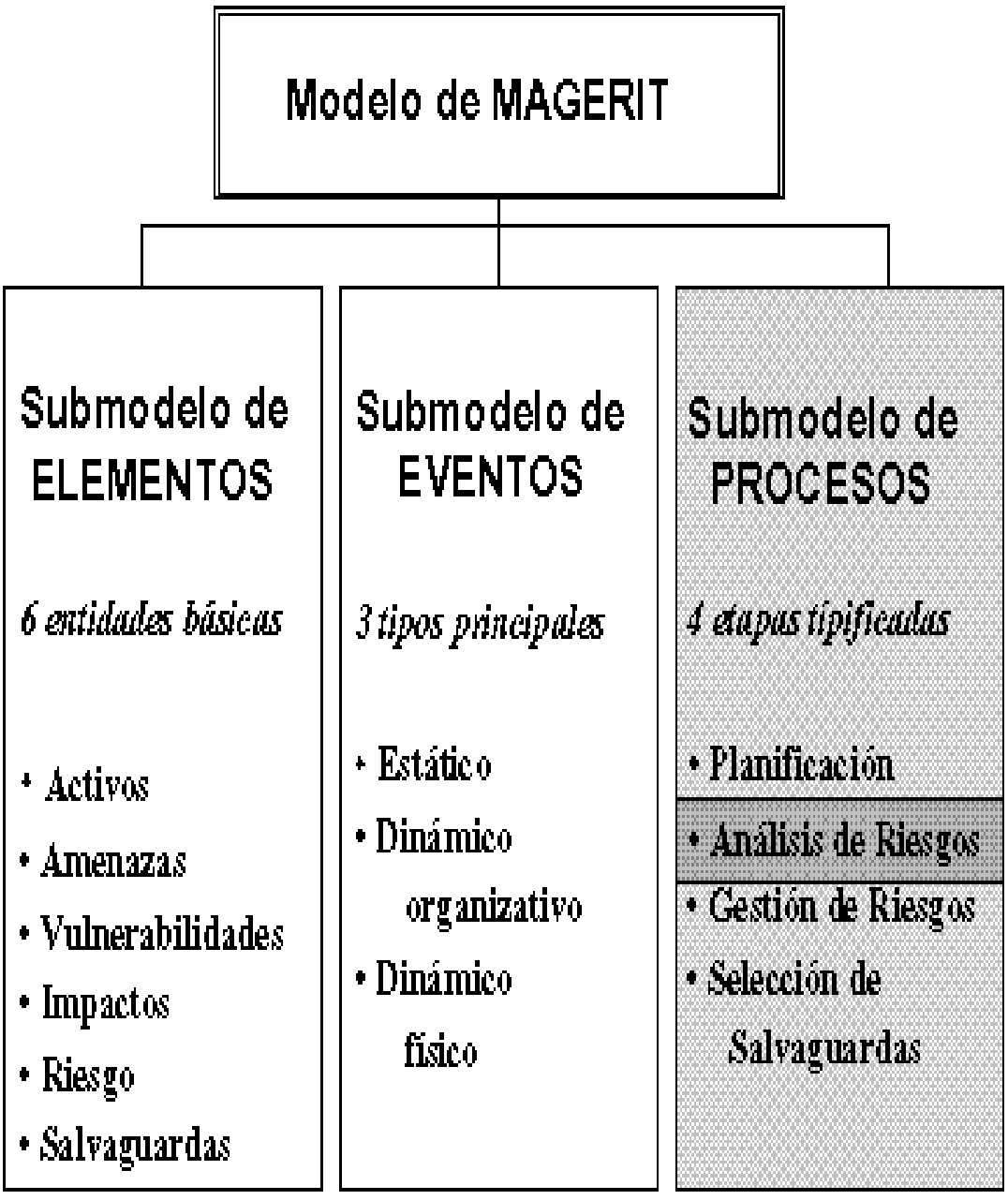
La ESPEL cuenta con todo lo que implica , disponibilidad de equipos y herramientas, traslado de documentos y manuales, etc.

Tarea 4: Sensibilizar (campaña informativa)

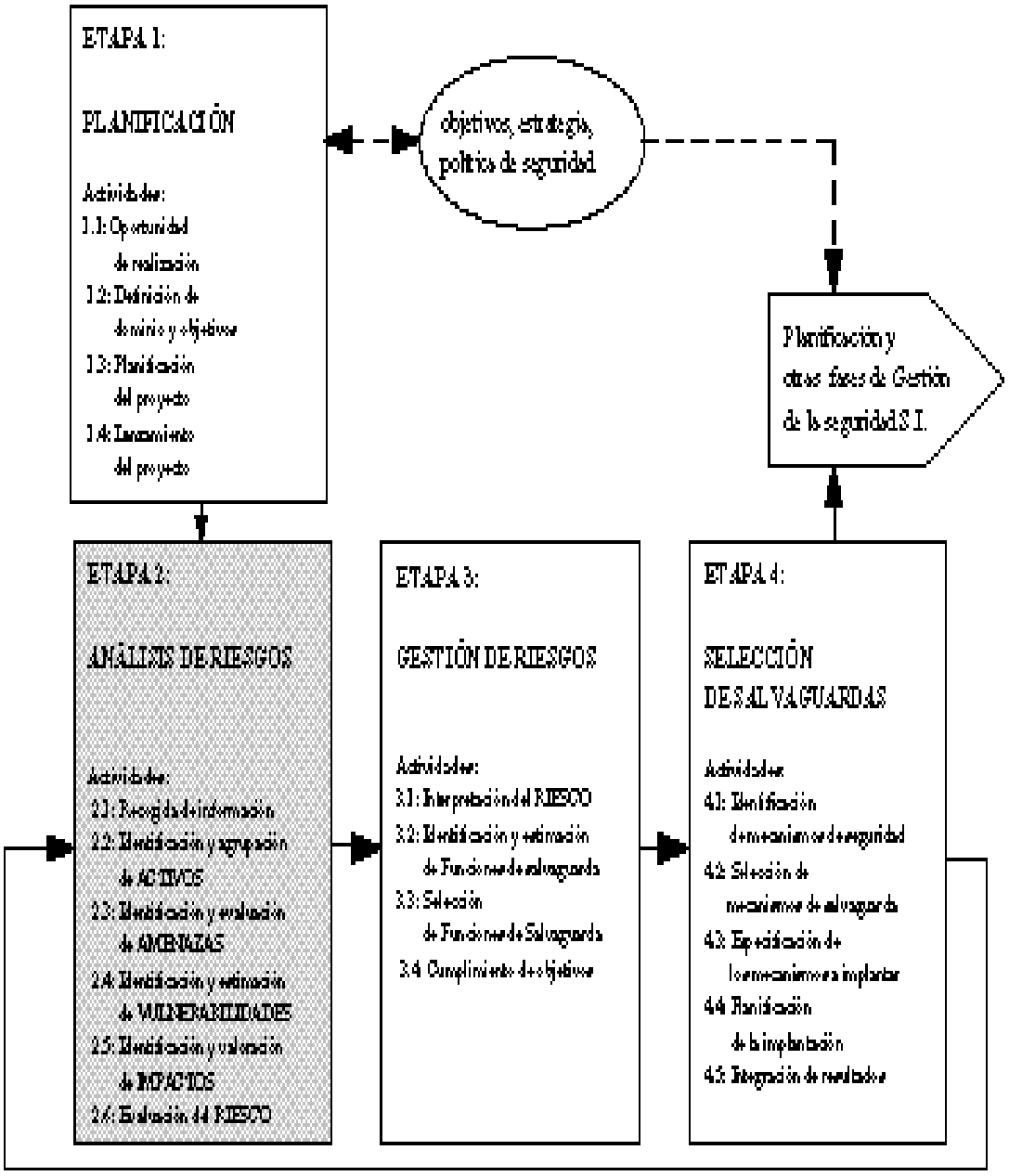
Después de presentar nuestro informe sobre la realización del proyecto de Análisis y Gestión de Riesgos la directiva de la institución autorizó la realización del mismo.

IV.- ETAPA 2: ANÁLISIS DE RIESGOS

4.1.- UBICACIÓN DE LA ETAPA 2 EN EL MODELO DE MAGERIT



4.2.- ESTRUCTURA DE LA ETAPA 2



4.3.- VISIÓN GLOBAL DE LA ETAPA

Objetivos de la Etapa

Esta etapa tiene los siguientes objetivos:

• Evaluar el riesgo del sistema en estudio, tanto el riesgo intrínseco (sin salvaguardas), como el riesgo efectivo (incluyendo el efecto de las salvaguardas implementadas sí se trata de un sistema actual, no de un sistema previsto).

Esta Etapa es el núcleo central de MAGERIT y su correcta aplicación condiciona la validez y utilidad de todo el procedimiento. La identificación y estimación de los Activos y de las posibles Amenazas que les acechan representa una tarea compleja, aunque relativamente rutinaria. La estimación de los Impactos y Vulnerabilidades no sólo es compleja, sino que es mucho más incierta y por tanto requiere cierta decisión creativa, que debe ser dirigida por expertos debido a la influencia determinante de ambos elementos, Impacto y Vulnerabilidad, en la determinación del Riesgo.

Contenido de la Etapa

1. Recogida de información

Obtención de la información sobre el sistema, de sus componentes, y de los factores que pueden influir en la seguridad.

2. Identificación y agrupación de ACTIVOS

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de los Activos en cuanto a su contribución a la evaluación del riesgo.

3. Identificación y evaluación de AMENAZAS

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de las Amenazas en cuanto a su contribución a la evaluación del riesgo.

4. Identificación y estimación de VULNERABILIDADES

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de las Vulnerabilidades en cuanto a su contribución a la evaluación del riesgo.

5. Identificación y valoración de IMPACTOS

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de los Impactos en cuanto a su contribución a la evaluación del riesgo.

6. Evaluación del RIESGO

Valoración del riesgo intrínseco y del riesgo efectivo, a partir de los resultados de las Actividades anteriores.

4.4.- ACTIVIDAD 1: RECOGIDA DE INFORMACIÓN

Esta actividad tiene por objeto recoger la información sobre el sistema y de los factores que pueden influir en la seguridad.

Esta actividad tiene una importancia crucial por dos motivos: la información a recoger condiciona el conocimiento del equipo del proyecto (ajeno en parte al funcionamiento del Dominio o sea dependiente de los conocedores de su comportamiento cotidiano); y la recogida en sí es una operación delicada que exige una confianza mutua profunda (la transmisión de información es siempre delicada y más sí concierne a la seguridad).

Tarea 1: Preparar la información

Se recogió los datos recientes y bien formalizados, así como la documentación de la información existente.

Tarea 2: Realizar las entrevistas

Se abarcó a todos los **Jefes de Servicio o de Área** De la ESPEL relacionados con sistemas de información :

UNIDAD LOGISTICA

RESPONSABLE: SRGTO JOSE SEGUNDO AGUILAR

AMANUENSE sus funciones son el de lograr un adecuado control de los abastecimientos, mantenimiento, sanidad, transportes, de manera rápida y oportuna, así como su adquisición, almacenamiento y distribución .

Para cumplir con sus objetivos cuenta con un computador personal que consta de un monitor, una CPU, un mouse, teclado y una impresora compartida, y microsoft office con windows 95 estos activos son importante para la organización, además es la única persona encargado de logística.

La información que maneja es de tipo confidencial y personal.

Esta unidad se encuentra en el departamento de Jefatura Administrativa en la entrada principal de la ESPE-L . No han existido posibles situaciones conflictivas (internas o externas, accidentales o provocadas).

No existen salvaguardas en la unidad a su cargo.

UNIDAD PERSONAL

RESPONSABLES : SGOS LUIS GABILEMA, SGOS KLEVER MOREJON

Los dos son AMANUENSE sus funciones son la de administrar los procesos de selección capacitación y evolución, así como recomendar a la dirección de recursos humanos de la ESPEL la reclasificación, asensos y promoción del personal administrativo, civil, militar y docente del instituto.

Cada uno cuenta con un computador con sus respectivos periféricos, windows 95 y office y una impresora compartida con la unidad de logística, no tienen personal a su cargo cada uno actúa en forma dependiente del Jefe Administrativo.

La unidad de personal se encuentra igual que la unidad de logística en el Departamento de Jefatura Administrativa.

No existen salvaguardas, ni situaciones conflictivas.

UNIDAD DE SEGURIDAD

RESPONSABLE: TNTE EDISON HIDALGO

Para esto no cuenta con sistemas de información(Hardware, software, comunicaciones) por lo cual no se realizara el estudio adecuado.

UNIDAD DE FINANZAS

RESPONSABLE: DRA ALICIA NAVAS

Dirigir, coordinar todos los procesos financieros de la sede.
Para esto tiene el siguiente personal a su cargo:

CONTABILIDAD: Sra. María Elena Robayo , Sra. Katty Hurtado, Sra. Marcela Karolys.

PAGADURIA: Sra. Alexandra Saltos, Sra. María Zurita

PRESUPUESTOS: Sra. Silvana Herrera

Todo el personal a su cargo cuenta con un computador personal a su cargo con sus respectivos periféricos y 4 impresoras todas en red .

La información que maneja es de tipo confidencial y personal.

Esta unidad se encuentra en el Segundo piso de edificio principal de la ESPE-L

No han existido posibles situaciones conflictivas (internas o externas, accidentales o provocadas).

No existen salvaguardas en la unidad a su cargo.

Tarea 3 de Análisis de la información recogida

Todas los computadores de las unidades se encuentra conectadas en red con cableado estructurado a un servidor que se encuentra en el Departamento de Organización y Sistemas. Ubicado en la planta baja de la ESPEL al ingreso en el segundo bloque.

Las personas responsables del funcionamiento de los sistemas de información son:

Ing. Edison Espinoza	Jefe Departamento de Organización y Sistemas
Ing. Fabián Montaluiza	Responsable del Software
Ing José Rodríguez	Responsable del Hardware
Sra. Tatiana Mayorga	Responsable de Redes

El Departamento Financiero funciona con el Software Olympo para la contabilidad, CoaWin, Roles de pago y no esta definido un lugar de entorno definitivo dentro de la ESPEL.

4.5.- ACTIVIDAD 2: IDENTIFICACIÓN Y AGRUPACIÓN DE ACTIVOS

Descripción y objetivo:

En la etapa de definición del dominio se han descrito las funciones que se realizan, ponderadas además según su importancia para la misión de la organización. El objetivo de esta actividad es 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.

Actividad 2.2: Identificación y agrupación de ACTIVOS

Tras el análisis de la información recogida directa e indirectamente, realizado a la luz de los fundamentos de MAGERIT, particularizado para la ESPEL para el Departamento Administrativo

Tarea 2.2.1 para Identificar activos y grupos de activos.

UNIDAD DE LOGISTICA

ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN (HARDWARE)

FECHA DE CONSTATACION: 15/07/02

DESCRIPCION	MARCA	MODELO/TIPO	No SERIE
CPU	COMPAQ	compaq presario	X723BKTB0603
MONITOR	COMPAQ	A3LCQM430	707AG07GK558
TECLADO	COMPAQ	RT6L5CTWLA	25W39E1A00143
MOUSE	COMPAQ	MUS9J	B01920H67EM0240
IMPRESORA	HEWLETT P	C5876A	US7A9110R4
TARJETA DE RED PCI	3 COM	XT206C3	S610BC800600-AZ

Observaciones: Impresora única para todo la Jefatura Administrativa y se encuentra en red.

UNIDAD DE PERSONAL

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)

FECHA DE CONSTATACION: 16/07/2002

DESCRIPCION	MARCA	MODELO/TIPO	No SERIE
CPU	DTK	300	7385P46383M
MONITOR	DTK	MA1435	HG7M1435
TECLADO	DTK	F-21YR	069707Y024765

MOUSE	DTK	2900	606073397
IMPRESORA	HEWLETT P	C5876A	US7A9110R4
TARJETA DE RED PCI	3COM	10/100 PCI NIC 3C905-DX	DF63C905-TX

Observaciones: Impresora única para todo el departamento y se encuentra en red.

Responsable: Sgto. Morejón Klever

UNIDAD FINANCIERA

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)

FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD DE CONTABILIDAD

DESCRIPCION	**MARCA**	**MODELO/TIPO**	**No SERIE**
CPU	Clon		
MONITOR	LG	553V	ARSCM356v
TECLADO	Standard	101/102 teclas	
MOUSE	Genios	Fsugmzfr	01213104
IMPRESORA	EPSON	FX-1170	3KW1099316
TARJETA DE RED PCI	SIS	900PCI	

Responsable: Dra. Alicia Navas

ACTIVOS DE LOS SISTEMAS DE INFORMCION(HARDWARE)
FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD PAGADURIA

DESCRIPCION	**MARCA**	**MODELO/TIPO**	**No SERIE**
CPU	DTK	QUIN 50	7385p46106
MONITOR	DTK	Ma-1435	G131878
TECLADO	DTK	F-21YR	069707Y024

MOUSE	DTK	2900	606073157
TARJETA DE RED PCI	3com	Etherlink3	6jq1328c7b

Responsable: Sra. Alexandra Saltos.

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)
FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD DE CONTABILIDAD

DESCRIPCION	**MARCA**	**MODELO/TIPO**	**No SERIE**
CPU	PREMIUM		
MONITOR	PREMIUM		
TECLADO	PREMIUM	KPQ-E99ZC13	
MOUSE	PREMIUM	ECM-S3902	606073157
IMPRESORA			
TARJETA DE RED PCI	Incorporado	10/100	6jq1328c7b

Responsable: Marcela Karolys

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)

FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD DE PRESUPUESTO

DESCRIPCION	**MARCA**	**MODELO/TIPO**	**No SERIE**
CPU	DTK	Queen56	7385p46102m
MONITOR	DTK	Svga	6131878
TECLADO	DTK	Windows	0697074024084
MOUSE	DTK	3b	600090447804
TARJETA DE RED PCI	3com	Etherlink3	6jq1328c7b

Responsable: Sra. Silvana Herrera.

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)
FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD DE CONTABILIDAD

DESCRIPCION	MARCA	MODELO/TIPO	No SERIE
CPU	Clon	Toser	P7q9202232
MONITOR	Samsung	SYNC MASTER	HCEJ902999
TECLADO	Hacer	6512-TW	D5094239
MOUSE	Genios	Easy mouse ps/2	98153930
IMPRESORA	HP		
TARJETA DE RED PCI			

Responsable: Sra. María Robayo

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)
FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD DE PAGADURIA

DESCRIPCION	MARCA	MODELO/TIPO	No SERIE
CPU	Clon		
MONITOR	Lg		
TECLADO	Standard	101/102 teclas	
MOUSE	Genios	Fsugmzfr	

Responsable: Sra. María Zurita.

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)
FECHA DE CONSTATACION: 19/07/2002

UBICACION ACTUAL: UNIDAD DE CONTABILIDAD

DESCRIPCION	MARCA	MODELO/TIPO	No SERIE
CPU	DTK		F825K4TECH
MONITOR	DTK	G131922	G131922
TECLADO	DTK		
MOUSE	DTK		

Responsable: Sra. Katty Hurtado.

ORGANIZACION Y SISTEMAS

ACTIVOS DE LOS SISTEMAS DE INFORMACION(HARDWARE)

FECHA DE CONSTATACION: 20/07/2002

UBICACION ACTUAL: DEPARTAMENTO DE ORGANIZACIÓN Y SISTEMAS

DESCRIPCION	**MARCA**	**MODELO/TIPO**	**No SERIE**
SERVIDOR CPU	PREMIUM	A402HHB509	A402HHB509
MONITOR	PREMIUM	531-3456 A	
TECLADO	PREMIUM	KPQ-E99ZC-3	CMYKPPQ7461
MOUSE	PREMIUM	ECM-53902	EW4ECM-S3902
SWITCH	HP PROCURSE	2524	J4813A

Responsable: Ing. Edison Espinoza

Para realizar el estudio se ha agrupado considerando las 5 capas en el Submodelo de Elementos de MAGERIT, estos niveles a tomar en cuenta son:

1.- Entorno
2.- Sistemas de Información
3.- Información
4.- Funcionalidades
5.- Otros Activos

1.- Activos relacionados con el nivel del Entorno
- Unidad de Finanzas
- Unidad de Logística y Personal
- Unidad de Organización y Sistemas
- Personal

2.- Activos relacionados con el nivel de los Sistemas de Información
- Equipo Informático

- Servidor Central
- Software base
- Software de aplicación
- Red local
- Medios de Almacenamiento
- Comunicaciones

3.- Activos relacionados con el nivel de Información.

- Procesos financieros
- Procesos de Logística
- Procesos de Personal
- Disponibilidad de la información

4.- Activos relacionados con el nivel de Funciones

- Dirigir, coordinar y controlar los procesos financieros.
- Capacitación y Evaluación del Personal
- Abastecimiento y Servicios de la Unidad
- Control y Funcionamiento de la Red

ARBOL DE DEPENDENCIA

Dependencia entre activos

Se utilizara los siguientes

100% = total

90% = alta

50% = media

10% = baja

0% = nula

Tarea 2: Identificar los mecanismos de salvaguarda existentes

En el Departamento Administrativo no existen mecanismos de salvaguardas implantadas.

Tarea3: Valorar activos

VALORACION DE ACTIVOS

HARDWARE

Departamento de Logística

Activo	Marca	Fecha de Adquisición	Costo
CPU	Compaq	01/01/1997	160
Monitor	Compaq	01/01/1997	60
Teclado	Compaq	01/01/1997	30
Mouse	Compaq	01/01/1997	5
			TOTAL: 255

Departamento de Personal

Activo	Marca	Fecha de Adquisición	Costo
CPU	DTK	01/01/1997	50
Monitor	DTK	01/01/1997	70
Teclado	DTK	01/01/1997	6
Mouse	DTK	01/01/1997	4
CPU	Clon	11/04/1999	300
Monitor	StudioWork	11/04/1999	100
Teclado	Genérico	11/04/1999	7
Mouse	Genios	11/04/1999	6
Impresora	HP-DeskJet	03/25/1998	180
			TOTAL: 723

Observaciones: La impresora esta en red y es utilizado por el Departamento de Logística y de Personal.

Departamento Financiero

Activo	Marca	Fecha de Adquisición	Costo
CPU	DTK	01/01/1997	145

Monitor	DTK	01/01/1997	70
Teclado	DTK	01/01/1997	6
Mouse	DTK	01/01/1997	4
CPU	Clon	11/04/1999	300
Monitor	LG	11/04/1999	100
Teclado	Genérico	11/04/1999	7
Mouse	Genios	11/04/1999	6
CPU	DTK	01/01/1997	145
Monitor	DTK	01/01/1997	70
Teclado	DTK	01/01/1997	6
Mouse	DTK	01/01/1997	4
CPU	DTK	01/01/1997	145
Monitor	DTK	01/01/1997	70
Teclado	DTK	01/01/1997	6
Mouse	DTK	01/01/1997	4
CPU	Clon	11/04/1999	300
Monitor	Samsung	11/04/1999	100
Teclado	Acer	11/04/1999	7
Mouse	Genios	11/04/1999	6
CPU	Compaq	01/01/1997	145
Monitor	Compaq	01/01/1997	70
Teclado	Compaq	01/01/1997	6
Mouse	Compaq	01/01/1997	4
CPU	Clon	11/04/1999	300
Monitor	LG	11/04/1999	100
Teclado	Genérico	11/04/1999	7
Mouse	Genios	11/04/1999	6
Impresora	Epson	10/23/1998	350
Impresora	HP	03/25/1998	180
Impresora	Panasonic	03/25/1998	40
Impresora	Epson	10/23/1998	350

TOTAL: 3059

Observaciones: La impresora esta en red y es utilizado por todo el Departamento.

Departamento De Organización y Sistemas

Activo	**Marca**	**Fecha de Adquisición**	**Costo**
SERVIDOR	PREMIUM	02/06/1999	$ 5000
SWITCH	HP		$ 3500

Valoración de los activos en el Submodelo de MAGERIT

FINANCIERO

ACTIVOS	**VALOR**
DEPARTAMENTO	1650
OPERADORES	0
EQUIPO INFORMATICO	3059
RED	550
SOTWARE BASE	84
PROCESOS FINANCIEROS	0
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESO FINANCIEROS	0

PERSONAL Y LOGISTICO

ACTIVOS	**VALOR**
DEPARTAMENTO	1100
OPERADORES	0
EQUIPO INFORMATICO	978
RED	115
SOTWARE BASE	84
PROCESOS DE PERSONAL	0
PROCESOS DE LOGISTICA	0
CAPACITACION Y EVALUACION DEL	0

PERSONAL	
ABASTECIMIENTO Y SERVICIOS DE LA UNIDAD LOGISTICA	0

ORGANIZACION Y SISTEMAS

ACTIVOS	**VALOR**
DEPARTAMENTO	1100
OPERADORES	0
SERVIDOR CENTRAL	5000
RED LOCAL Y COMUNICACIONES	3500
SOTWARE BASE	1200
APLICACIONES	1950
DISPONIBILIDAD DE LA INFORMACIÓN	0
MEDIOS DE ALMACENAMIENTO	0
CONTROL Y FUNCIONAMIENTO DE LA RED	0

4.6 ACTIVIDAD 3: IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS

La Actividad permite identificar y evaluar las amenazas que sufren los activos del sistema. Cada Amenaza es un evento que potencialmente puede desencadenar otras amenazas. Todas juntas constituyen un 'escenario de amenazas', que desencadena un 'árbol de fallos' como subescenario de ataque real a un 'árbol de activos' (determinado en la Actividad anterior). La Vulnerabilidad asociada al 'árbol de Activos' y específica para el 'escenario de amenazas', propicia el desencadenamiento de éstas que producen **Impactos** (es decir deterioros) en los Activos afectados, con distintos grados posibles de profundidad.

Tarea 1: Identificar y agrupar amenazas

Los Escenarios cubren los siguientes grupos de Amenazas:

1.- ACCIDENTE NATURAL O INDUSTRIAL

A1: Accidente físico de origen industrial: incendio, explosión.

A3: Accidente físico de origen natural: riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe, ...

2.- INTERRUPCIÓN DE SERVICIO

A2: Avería: de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

A4: Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, fluidos y suministros diversos

A5: Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática

P5: Indisponibilidad de recursos humanos o técnicos (desvío de uso, bloqueo).

3.- ERRORES O INSUFICIENCIAS DE DISEÑO

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

E4: Monitorización/Trazabilidad/Registro inadecuados del Tráfico

4.- SUSTRACION FISICA

P1: Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura)

5.- SUSTRACCIÓN LÓGICA

P2: Acceso lógico no autorizado con intercepción pasiva simple de la información (requiere sólo su lectura)

P3: Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración (requiere lectura y escritura); es

decir, reducción de la confidencialidad del sistema para obtener bienes o servicios aprovechables (programas, datos ...)

6.- ATAQUE LÓGICO

P4: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración

4.7.- ACTIVIDAD 4: IDENTIFICACIÓN Y ESTIMACIÓN DE VULNERABILIDADES

Esta Actividad se centra en la Vulnerabilidad, característica conjunta de la Amenaza y el Activo (o propiedad de su relación, según se prefiera y convenga al análisis) que puede considerarse como la potencialidad o 'cercanía' previsible de la materialización de la Amenaza en Agresión. MAGERIT evalúa la vulnerabilidad como la frecuencia de ocurrencia de la amenaza sobre el activo correspondiente.

Tarea 1: Identificar Vulnerabilidades

Para cada Activo amenazable se ha identificado que todos son de *vulnerabilidad intrínseca,* ya que no incluyen ninguna salvaguarda (fuera de las naturales o implícitamente incorporadas en el activo considerado).

Tarea 2: Estimar Vulnerabilidades

Para la estimación se utilizo el siguiente cuestionario que proporciona MAGERIT que se encuentra en el anexo 1, y con los resultado de los responsables de los activos , de acuerdo a las amenazas encontradas.

Los cálculos de la vulnerabilidad se realizara utilizando el Anexo 2

ACTIVOS:

UNIDAD FINANCIERA

UNIDAD LOGISTICO Y PERSONAL

UNIDAD ORGANIZACION Y SISTEMAS

EQUIPO INFORMATICO

SERVIDOR CENTRAL

AMENAZA

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

CUESTIONARIO

Preg.1 de Vulnerabilidad

Para luchar contra accidentes de tipo incendio o explosión, ¿el personal tiene recursos y Entrenamiento.
*Sistematizado( ) suficientes( ) desaprovechados( ) escasos(**X**)?*

Preg.2 de Vulnerabilidad

Si no tiene, ¿hay focos indicadores de siniestro en el departamento o en su entorno cercano?
*No(**X**) SÍ( ) y además hay material inflamable cerca( )*

Si el encuestado marcó R4 en la Pregunta 1: Se toma para R4 x = 0,14 (vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R2 en la Pregunta 2 entonces: Res2 = R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS

EQUIPO INFORMATICO

RED LOCAL

SERVIDOR CENTRAL

COMUNICACIONES

AMENAZA

A2: AVERÍ0A (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

CUESTIONARIO

Preg.1 Vulnerabilidad

Para superar una avería (física o lógica, original o sobrevenida), ¿Hay mantenimientos y repuestos contratados y de eficacia demostrada?

Preventivos(x) sistematizados( ) suficientes( ) muy lentos( )

Si se contesta R1 se toma sin más el siguiente valore: Res1=R1 x = 0,0002 vulnerabilidad baja La vulnerabilidad por probabilidad será:

x = 0.0002 = 0.02% = Vulnerabilidad baja = Poco Frecuente

ACTIVOS

UNIDAD FINANCIERA

UNIDAD PERSONAL Y LOGISTICA

UNIDAD DE ORGANIZACIÓN Y SISTEMAS

AMENAZA

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

CUESTIONARIO

Preg.1 Vulnerabilidad

Para luchar contra un Accidente físico de origen natural, ¿el personal tiene recursos y entrenamiento?

*Sistematizados( ) suficientes( ) desaprovechados( ) escasos(**X**)*

Preg.2 Vulnerabilidad

Si no tienen, ¿hay focos de siniestro en el departamento o en su entorno cercano?
*No( ) SÍ (**X**) y además no hay contacto con protección civil( )*

Si el encuestado marcó R4 en la Pregunta 1, Se toma para R4 x = 0,14 (vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R3 en la Pregunta 2 entonces: Res2=R3 x = 0,02 vulnerabilidad alta

La vulnerabilidad por probabilidad será:
X = 0.02 = 2% = Vulnerabilidad alta = Frecuente

ACTIVOS

EQUIPO INFORMATICO

RED LOCAL

SERVIDOR CENTRAL

COMUNICACIONES

AMENAZA

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

CUESTIONARIO

Preg.1 Vulnerabilidad

Para neutralizar una Interrupción de servicios o de suministros esenciales, ¿Se tienen servicios y suministros alternativos?
*sistematizados( ) suficientes( ) desaprovechados( ) escasos(**X**)*

Preg.2 Vulnerabilidad

Si no tienen,¿hay motivos de interrupción en el departamento o en su entorno cercano?

No( ) SÍ(**X**) y además no hay instrucciones para un cierre ordenado( )

Si el encuestado marcó R4 en la Pregunta 1, Se toma para R4 x = 0,14 (vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R3 en la Pregunta 2 entonces: Res2=R3 x = 0,02 vulnerabilidad alta

La vulnerabilidad por probabilidad será:

X = 0.02 = 2% = Vulnerabilidad alta = Frecuente

ACTIVOS

EQUIPO INFORMATICO

RED LOCAL

SERVIDOR CENTRAL

COMUNICACIONES

AMENAZA

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

CUESTIONARIO

Preg.1 Vulnerabilidad

Para neutralizar un Accidente mecánico o electromagnético, ¿se tienen medidas de protección y de ubicación?

*sistematizadas( ) suficientes( ) desaprovechadas( ) escasas(**X**)*

Preg.2 Vulnerabilidad

Si no tienen, ¿hay motivos de accidente en el departamento o su entorno cercano?

*No(**X**) SÍ( ) y además no hay instrucciones para superar la situación( )*

Si el encuestado marcó R4 en la Pregunta 1, Se toma para R4 x = 0,14 (vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R2 en la Pregunta 2 entonces: Res2 = R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:
x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS
SOFTWARE BASE
APLICACIONES

AMENAZA
E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

CUESTIONARIO

Preg.1 Vulnerabilidad

Para detectar y neutralizar Errores de utilización en la recogida o la transmisión de datos o en su explotación, ¿se tienen medidas de protección?
*sistematizadas( ) suficientes( ) desaprovechadas( ) escasas(**X**)*

Preg.2 Vulnerabilidad

Si no tienen, ¿hay fuentes de estos incidentes en el departamento o su entorno cercano?
*No( ) SÍ(**X**) y además no hay instrucciones para superar la situación(**X**)*

Si el encuestado marcó R4 en la Pregunta 1, Se toma para R4 x = 0,14 (vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R4 en la Pregunta 2 entonces: Res2=R4 x = 0,2 vulnerabilidad muy alta

La vulnerabilidad por probabilidad será:

x = 0.2 = 20% = Vulnerabilidad muy alta = Muy Frecuente

ACTIVOS

APLICACIONES

AMENAZA

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

CUESTIONARIO

Preg.1 Vulnerabilidad

Para detectar y neutralizar los errores de diseño generados en el desarrollo del software, ¿se tienen medidas de protección?

*Sistematizadas( ) suficientes( ) desaprovechadas( ) escasas(**X**)*

Preg.2 Vulnerabilidad

Si no tienen, ¿hay motivos de accidente en el departamento o su entorno cercano?

*No(**X**) SÍ( ) y además no hay instrucciones para superar la situación( )*

Si el encuestado marcó R4 en la Pregunta 1, - Se toma para R4 x = 0,14

(vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R2 en la Pregunta 2 entonces: - Res2 = R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS

APLICACIONES

AMENAZA

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

CUESTIONARIO

Preg.1 Vulnerabilidad

Para neutralizar la Inadecuación de Monitorización, Trazabilidad o Registro del Tráfico de la información, ¿se tienen medidas de protección?

sistematizadas( ) *suficientes( )* *desaprovechadas( )* *escasas(**X**)*

Preg.2 Vulnerabilidad

Si no bastan, ¿hay motivos de accidente en el departamento o su entorno cercano?

No( ) *SÍ(**X**)* *y además no hay instrucciones para superar la situación(**X**)*

Si el encuestado marcó R4 en la Pregunta 1, Se toma para R4 x = 0,14 (vulnerabilidad aproximada entre alta y muy alta)

Pero como se respondió R4 en la Pregunta 2 entonces: Res2=R4 x = 0,2 vulnerabilidad muy alta

La vulnerabilidad por probabilidad será:

x = 0.2 = 20% = Vulnerabilidad muy alta = Muy Frecuente

ACTIVOS

EQUIPO INFORMATICO

RED LOCAL

SERVIDOR CENTRAL

COMUNICACIONES

MEDIOS DE ALMACENAMIENTO

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

Preg.1 Vulnerabilidad

Para detectar y neutralizar un Acceso físico con sustracción o destrucción, ¿Se tienen medidas de protección y ubicación?

sistematizados( ) *suficientes(**X**)* *desaprovechados( )* *escasos( )*

Si se contesta R2 se toma sin más el siguiente valor: Res1=R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS

PROCESOS FINANCIEROS

PROCESOS DE PERSONAL

PROCESOS DE LOGISTICA

DISPONIBILIDAD DE LA INFORMACION

AMENAZA

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

CUESTIONARIO

Preg.1 Vulnerabilidad

Para luchar contra los Accesos lógicos con escucha, ¿se han tomado precauciones

sistematizadas( ) *suficientes(**X**)* *desaprovechados( )* *escasos ( )*

Si se contesta R2 se toma sin más el siguiente valor: Res1=R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS

PROCESOS FINANCIEROS

PROCESOS DE PERSONAL

PROCESOS DE LOGISTICA

DISPONIBILIDAD DE LA INFORMACION

AMENAZA

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

CUESTIONARIO

Preg.1 Vulnerabilidad

Para detectar y neutralizar accesos lógicos con alteración o sustracción, ¿Se tienen medidas de protección?

sistematizadas( ) *suficientes(**X**)* *desaprovechadas( )* *escasas( )*

Si se contesta R2 se toma sin más el siguiente valor: Res1=R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS

EQUIPO INFORMATICO

RED LOCAL

SERVIDOR CENTRAL

COMUNICACIONES

MEDIOS DE ALMACENAMIENTO

AMENAZA

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

CUESTIONARIO

Preg.1 Vulnerabilidad

Para detectar y neutralizar accesos lógicos con corrupción o destrucción, ¿Se tienen medidas de protección?

sistematizadas( ) *suficientes(**X**)* *desaprovechadas( )* *escasas( )*

Si se contesta R2 se toma sin más el siguiente valor: Res1=R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

ACTIVOS

DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS.

CAPACITACIÓN Y EVALUACIÓN DEL PERSONAL.

ABASTECIMIENTO Y SERVICIOS DE LA UNIDAD.

CONTROL Y FUNCIONAMIENTO DE LA RED

AMENAZA

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

CUESTIONARIO

Preg.1 Vulnerabilidad

Para neutralizar situaciones de Indisponibilidad de recursos humanos o técnicos

¿Se tienen medidas de detección y sustitución?
*sistematizadas( ) suficientes(**X**) desaprovechadas( ) escasas( )*

Si se contesta R2 se toma sin más el siguiente valor: Res1=R2 x = 0,002 vulnerabilidad media

La vulnerabilidad por probabilidad será:

x = 0.002 = 0.2% = Vulnerabilidad media = Frecuente Normal

4.8.- ACTIVIDAD 5: IDENTIFICACIÓN Y VALORACIÓN DE IMPACTOS

Descripción y objetivo:

El objetivo de esta actividad es conocer el alcance del daño producido en el Dominio como consecuencia de la materialización de amenazas sobre los activos.

El **Impacto,** visto como característica del Activo que recoge el cambio de estado de su seguridad, permite apreciar la 'gravedad' de la consecuencia generada por la Agresión, en forma de reducción de niveles de los subestados de seguridad (ACID) del Activo afectado.

Tarea 1 Tipificar impactos

ACCIDENTE NATURAL O INDUSTRIAL

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

INTERRUPCIÓN DE SERVICIO

SD. Indisponibilidad: reducción de margen por falta de resultados; o bien gastos suplementarios para mantener la funcionalidad precedente a la amenaza

ERRORES O INSUFICIENCIAS DE DISEÑO

SD. Indisponibilidad: menor margen o gastos para mantener la funcionalidad

L2. Incumplimiento de obligaciones legales

L3. Perturbación o situación embarazosa político-administrativa (por ejemplo credibilidad, prestigio...)

SUSTRACION FISICA

N1: Pérdidas económicas

N2: Pérdidas inmateriales

SD. Disponibilidad

SUSTRACCIÓN LÓGICA

SC. Confidencialidad:

L2. Incumplimiento de obligaciones legales

L3. Perturbación o situación embarazosa político-administrativa

ATAQUE LÓGICO

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

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.

Tarea 2: Valorar impactos

ACTIVOS

UNIDAD FINANCIERA
UNIDAD LOGISTICO Y PERSONAL

UNIDAD ORGANIZACION Y SISTEMAS

EQUIPO INFORMATICO

SERVIDOR CENTRAL

AMENAZA

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

Preg.1 de Impacto

¿afecta a la misión de la organización? ¿con qué deterioro?
*medio( ) alto( ) muy alto(**X**)*

La Impacto o Degradación por probabilidad será: **Muy Alto = 0.95 = 95%**

ACTIVOS

EQUIPO INFORMATICO

SERVIDOR CENTRAL

AMENAZA

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

Preg.1 de Impacto

¿afecta a la misión de la organización? ¿con qué deterioro?
*medio( ) alto(**X**) muy alto( )*

La Impacto o Degradación por probabilidad será: **Alto = 0.50 = 50%**

ACTIVOS

RED LOCAL

COMUNICACIONES

AMENAZA

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

Preg.1 de Impacto

¿afecta a la misión de la organización? ¿con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Media = 0.25 = 25%**

ACTIVOS

UNIDAD FINANCIERA

UNIDAD PERSONAL Y LOGISTICA

UNIDAD DE ORGANIZACIÓN Y SISTEMAS

AMENAZA

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)
Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto( ) muy alto(**X**)*

La Impacto o Degradación por probabilidad será: **Muy Alto = 0.95 = 95%**

ACTIVOS

EQUIPO INFORMATICO

SERVIDOR CENTRAL

AMENAZA

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES

ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto(**X**) muy alto( )*

La Impacto o Degradación por probabilidad será: **Alto = 0.50 = 50%**

ACTIVOS

RED LOCAL

COMUNICACIONES

AMENAZA

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES

ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Medio = 0.25 = 25%**

ACTIVOS

EQUIPO INFORMATICO

RED LOCAL

SERVIDOR CENTRAL

COMUNICACIONES

AMENAZA

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Medio = 0.25 = 25%**

ACTIVOS

SOFTWARE BASE

APLICACIONES

AMENAZA

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto(**X**) muy alto( )*

La Impacto o Degradación por probabilidad será: **Alto = 0.50 = 50%**

ACTIVOS

APLICACIONES

AMENAZA

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Media = 0.25 = 25%**

ACTIVOS

APLICACIONES

AMENAZA

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
medio(x) alto( ) muy alto( )

La Impacto o Degradación por probabilidad será: **Media = 0.25 = 25%**

ACTIVOS

EQUIPO INFORMATICO

SERVIDOR CENTRAL

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto(**X**) muy alto( )*

La Impacto o Degradación por probabilidad será: **Alto = 0.50 = 50%**

ACTIVOS

RED LOCAL

COMUNICACIONES

MEDIOS DE ALMACENAMIENTO

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Media = 0.25 = 25%**

ACTIVOS

PROCESOS FINANCIEROS

PROCESOS DE PERSONAL

PROCESOS DE LOGISTICA

DISPONIBILIDAD DE LA INFORMACION

AMENAZA

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)
Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Media = 0.25 = 25%**

ACTIVOS

PROCESOS FINANCIEROS

PROCESOS DE PERSONAL

PROCESOS DE LOGISTICA

DISPONIBILIDAD DE LA INFORMACION

AMENAZA

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto(**X**) muy alto( )*

La Impacto o Degradación por probabilidad será: **Alto = 0.50 = 50%**

ACTIVOS

EQUIPO INFORMATICO

SERVIDOR CENTRAL

AMENAZA

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto(**X**) muy alto( )*

La Impacto o Degradación por probabilidad será: **Alto = 0.50 = 50%**

ACTIVOS

RED LOCAL

COMUNICACIONES

MEDIOS DE ALMACENAMIENTO

AMENAZA

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio(**X**) alto( ) muy alto( )*

La Impacto o Degradación por probabilidad será: **Media = 0.25 = 25%**

ACTIVOS

DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS.

CAPACITACIÓN Y EVALUACIÓN DEL PERSONAL.

ABASTECIMIENTO Y SERVICIOS DE LA UNIDAD.

CONTROL Y FUNCIONAMIENTO DE LA RED

AMENAZA

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

Preg.1 de Impacto

¿Afecta a la misión de la organización? ¿Con qué deterioro?
*medio( ) alto( ) muy alto(**X**)*

La Impacto o Degradación por probabilidad será: **Muy Alto = 0.95 = 95%**

4.9 ACTIVIDAD 6: EVALUACIÓN DEL RIESGO

Las informaciones sobre vulnerabilidad e impacto obtenidas en las Actividades anteriores permiten que esta Actividad establezca y estime los distintos tipos de riesgo.

La Vulnerabilidad y su Impacto sobre el Activo determinan conjuntamente el **Riesgo calculado.**

Tarea 1: Evaluar el riesgo intrínseco

- Construir el árbol de activos y calcular la dependencia acumulada.

ACTIVOS	**VALOR**
DEPARTAMENTO	12700
OPERADORES	0
EQUIPO INFORMATICO	4037
RED LOCAL Y COMUNICACIONES	4165
SOTWARE BASE	1284
PROCESOS FINANCIEROS	2000
APLICACIONES	1950
PROCEOS PERSONAL Y LOGISTICA	84
DISPONIBILIDAD DE LA INFORMACION	1200
MEDIOS DE ALMACENAMIENTO	250
SERVIDOR CENTRAL	5000
MANIPULACION Y CONTROL DE LA RED	1200
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICA	100
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESO FINANCIEROS	2034

ÁRBOL DE ACTIVOS

ACTIVO PADRE	ACTIVO HIJO	DEPENDENCIA
DIRIGIR, COORDINAR Y CONTROLAR PROCESOS FINANCIEROS	PROCESOS FINANCIEROS	100%
PROCESOS FINANCIEROS	RED LOCAL	50%
PROCESOS FINANCIEROS	EQUIPO INFORMATICO	100%
PROCESOS FINANCIEROS	SOFTWARE BASE	100%
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICA	PROCESOS PERSONAL Y LOGISTICA	100%
PROCESOS PERSONAL Y LOGISTICA	SOFTWARE BASE	90%
PROCESOS PERSONAL Y LOGISTICA	EQUIPO INFORMATICO	90%
PROCESOS PERSONAL Y LOGISTICA	RED LOCAL Y COMUNICACIONES	10%
MANIPULACION Y CONTROL DE LA RED	DISPONIBILIDAD DE LA INFORMACION	100%
DISPONIBILIDAD DE LA INFORMACION	MEDIOS DE ALMACENAMIENTO	90%
DISPONIBILIDAD DE LA INFORMACION	SOFTWARE BASE	100%
DISPONIBILIDAD DE LA INFORMACION	SERVIDOR CENTRAL	100%
MEDIOS DE ALMACENAMIENTO	DEPARTAMENTO	100%
MEDIOS DE ALMACENAMIENTO	OPERADORES	50%
MEDIOS DE ALMACENAMIENTO	SOFTWARE BASE	100%
DISPONIBILIDAD DE LA INFORMACION	RED LOCAL Y COMUNICACIONES	100%
RED LOCAL Y	DEPARTAMENTO	100%

COMUNICACIONES		
EQUIPO INFORMATICO	DEPARTAMENTO	100%
EQUIPO INFORMATICO	OPERADOR	50%
SOFTWARE BASE	OPERADOR	50%

• Cálculo de la dependencia acumulada(DA) en cada activo:

DA = Valor

Lista = Activos que Dependen de este activo

For = (i = 1...n)

DA += Lista[i].Activo.DA*Lista [i].grado

Activo: DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS

Ningún activo depende de este por lo tanto la:

DA = 2034

Activo: CAPACITACIÓN PERSONAL Y ABASTECIMIENTO LOGISTICA

Ningún activo depende de este por lo tanto la:

DA = 100

Activo: MANIPULACION Y CONTROL DE LA RED

Ningún activo depende de este por lo tanto la:

DA = 1200

Activo: PROCESOS FINANCIEROS

Con costo 2000;

DA = 2000 + 1*2034 DA = 4034

Activo: PROCESOS DE LOGISTICA Y LOGISTICA

Con costo 84;

DA = 84 + 1*100 DA = 184

Activo: DISPONIBILIDAD DE LA INFORMACION

Con costo 1200;

DA = 1200 + 1*1200 DA = 2400

Activo: APLICACIONES

Con costo de 1950;

DA = 1950 + 1 *4034 DA = 5984

Activo: EQUIPO INFORMATICO

Con costo 4037:

DA = 4037 + 1*5984 + 0.9 *184 DA = 10186.6

Activo: MEDIOS DE ALMACENAMIENTO

con costo de 250

DA = 250 + 0.9*2400 DA = 2410

Activo: SOFTWARE BASE

con costo de 1284

DA = 1284 + 0.9*184 + 1*5984 + 1*2400 + 1*2410 DA = 12243.6

Activo: RED LOCAL Y COMUNICACIONES

con costo de 4165

DA = 4165 + 0.1*184 + 0.5*5984 + 1*2400 DA = 9575.4

Activo: SERVIDOR CENTRAL

con costo de 5000

DA = 5000 + 1*2400 DA = 7400

Activo: DEPARTAMENTO

con costo de 12700

DA = 12700 + 1*9575 + 1*10187 + 1*2410 + 1*7400 DA = 42272

Activo: OPERADOR

con costo de 0

DA = 0 + 0.5*12243 + 0.5*10187 + 0.5*7400 + 0.5*2410 DA = 16120

ACTIVOS	**VALOR**	**DEPENDENCIA ACUMULADA**
DIRIGIR, COORDINAR Y CONTROLAR PROCESOS FINANCIEROS	2034	2.34
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICA	100	100
MANIPULACION Y CONTROL DE LA RED	1200	1200
PROCESOS PERSONAL Y LOGISTICA	84	184
DISPONIBILIDAD DE LA INFORMACION	1200	2400
PROCESOS FINANCIEROS	2000	4034
RED LOCAL Y COMUNICACIONES	4165	9575
APLICACIONES	1950	5984
EQUIPO INFORMATICO	4037	10187
SOFTWARE BASE	1284	12243
MEDIOS DE ALMACENAMIENTO	250	2410
SERVIDOR CENTRAL	5000	7400
DEPARTAMENTO	12700	42272
OPERADOR	0	16120

3 Relaciones con otros Elementos

• Funciones de salvaguarda asociadas a las amenazas:

AMENAZA:

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

FUNCION	**DISMINUCION DEL IMPACTO**	**DISMINUCION DE VULNERABILIDAD**
Limitar el Alcance de Incendio	75%	0

Prevenir el Incendio	0	75%

AMENAZA

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Limitar el Alcance de Averías	75%	0
Prevenir Avería	0	75%

AMENAZA

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Limitar Alcance de Incidente	75%	
Formación	75%	75%

AMENAZA

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Limitar el Alcance de Corte Eléctrico	75%	0

AMENAZA

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Procedimientos físicos	0	75%

AMENAZA

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Limitar el Alcance de Errores	75%	0
Prevenir Errores	0	75%

AMENAZA

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Prevenir Errores	0	75%

AMENAZA

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Procedimientos Lógicos	0	75%

AMENAZA

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Control de Acceso Físico	0	75%
Procedimientos Físicos	0	50%

AMENAZA

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Copias de Seguridad	75%	0

Control de Acceso Lógico	0	75%
Procedimientos Lógicos	0	50%

AMENAZA

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Control de Acceso Lógico	0	75%
Limitar Alcance de Ataque	75%	0

AMENAZA

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR ‘MAN IN THE MIDDLE’ DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Control de Acceso Físico	0	75%
Limitar alcance de Ataque	75%	0

AMENAZA

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

FUNCION	DISMINUCION DEL IMPACTO	DISMINUCION DE VULNERABILIDAD
Limitar alcance del Ataque	75%	0

- Establecimiento de la relación entre los Activos afectables por las Amenazas y éstas. Inclusión en la relación de la Vulnerabilidad del Activo a la Amenaza y

del Impacto como degradación del valor del Activo. Cálculo del riesgo intrínseco:

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
DEPARTAMENTO	0.2	95	40158.4	80.31
RED LOCAL Y COMUNICACIONES	0.2	95	9096.25	18.19
MEDIOS DE ALMACENAMIENTO	0.2	95	2289.5	4.57
SERVIDOR CENTRAL	0.2	95	7030	14.06
EQUIPO INFORMATICO	0.2	95	9677.65	19.35

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
SERVIDOR CENTRAL	0.02	50	3700	0.74
RED LOCAL Y COMUNICACIONES	0.02	25	2393.75	0.47
EQUIPO INFORMATICO	0.02	50	5093.5	1.01

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
OPERADORES	2	95	15314	306.28
DEPARTAMENTO	2	95	40158.4	803.16

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
SERVIDOR CENTRAL	2	50	3700	74
RED LOCAL Y COMUNICACIONES	2	25	2393.75	47.87
EQUIPO INFORMATICO	2	50	5093.5	101.87

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
SERVIDOR CENTRAL	0.2	25	1850	3.7
RED LOCAL Y COMUNICACIONES	0.2	25	2393.75	4.78
EQUIPO INFORMATICO	0.2	25	2546.75	5.09

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
APLICACIONES	20	50	2992	598.4
SOFTWARE BASE	20	50	6121.5	1224.3

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
APLICACIONES	0.2	25	1496	2.99

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
APLICACIONES	20	25	1496	299.2

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
SERVIDOR CENTRAL	0.2	50	3700	7.4
MEDIOS DE ALMACENAMIENTO	0.2	25	602.5	1.20
RED LOCAL Y COMUNICACIONES	0.2	25	2393.75	4.78
EQUIPO INFORMATICO	0.2	50	5093.5	10.18

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
PROCESOS PERSONAL Y LOGISTICA	0.2	25	46	0.09
DISPONIBILIDAD DE LA INFORMACION	0.2	25	300	0.6
PROCESOS FINANCIEROS	0.2	25	1008.5	2.01

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
PROCESOS PERSONAL Y LOGISTICA	0.2	50	92	0.18
DISPONIBILIDAD DE LA INFORMACION	0.2	50	600	1.2
PROCESOS FINANCIEROS	0.2	50	2017	4.03

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
SERVIDOR CENTRAL	0.2	50	3700	7.4
RED LOCAL	0.2	25	2393.75	4.78
EQUIPO INFORMATICO	0.2	50	5093.5	10.18

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

ACTIVOS	V %	DG %	IMP (DG*DA)	RI (IMP*V)
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICO	0.2	95	95	0.19
MANIPULACION Y CONTROL DE LA RED	0.2	95	1140	2.28
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS	0.2	95	1932.3	3.86

Tarea 2: Analizar las funciones de salvaguarda existentes

Control de Acceso Físico

Control de Acceso Lógico

Procedimientos Físicos

Procedimientos Lógicos

Prevenir Averías

Limitar el Alcance de un Corte Eléctrico

Limitar el Alcance de un Incendio

Prevenir Errores

Tarea 3: Evaluar el riesgo efectivo

Para realizar el Calculo del Riesgo Efectivo realizamos los siguientes:

Grado de implementación de los mecanismos existentes:

• Mecanismos que componen las funciones, con su grado IM de implementación propio y su grado CM de cumplimentación de aquéllas, de acuerdo los siguientes parámetros de valoración

100% = Muy Alta

90% = Alta

60% = Media

30% = Baja

0% = Nula

Función: Control de Acceso Físico

MECANISMOS EXISTENTES	IM%	CM%
Cerrar las puertas del área de seguridad en periodos de inactividad	90	3
Controlar todos los accesos por un guardia de seguridad o personal	30	3
Reducir el número de Accesos al área de seguridad	90	3
No poner ventanas ni paredes exteriores que permitan el paso a saboteadores	90	3
No permitir el acceso de las visitas a zonas estrictamente confidenciales	90	3
Construir pasillos y vestículos sin puertas falsas	90	3
No establecer indicadores sobre la ubicación del área de seguridad	90	3

Función: Control de Acceso Lógico

MECANISMOS EXISTENTES	IM%	CM%
Implantar sistemas de contraseñas	60	10
Implantar contraseñas difíciles de adivinar	60	2
Utilizar sistemas operativos con utilidades incorporadas para el control de acceso	60	2
Nombrar encargado de la administración y gestión de los derechos de acceso	60	2
Restringir el acceso a las utilidades del sistema	90	2
Asegurar que el software del sistema permita control de los privilegios	90	2
Proporcionar a los propietarios de la información los derechos de acceso	90	2
Asegurar contraseñas con un mínimo de cinco caracteres de longitud	100	2
Proporciona información a los usuarios de las normas respecto a las contraseñas	100	2
Asegurar desconexión en caso de un periodo de inactividad	60	2
Asegurar que el control de acceso funciona con lenguajes de selección	90	2
Asegurar solo que el usuario defina la contraseña	90	2

Función : Procedimientos Físicos

MECANISMOS EXISTENTES	IM%	CM%
Contratar Vigilancia nocturno permanente	30	24
Aislar el área de seguridad de zonas donde se realicen procesos peligrosos	90	2
Situar áreas de seguridad alejadas de líneas de alto voltaje	90	2
Situar áreas de seguridad alejadas de zonas de alto porcentaje de crimen	90	2
Situar áreas de seguridad alejadas de zonas de almacenamiento de productos peligrosos	90	2
Asegurar que todos los circuitos tienen su correspondiente toma tierra	90	2

Función: Procedimientos Lógicos

MECANISMOS EXISTENTES	IM%	CM%
Asegurar Software de red estándar, fiable y con mantenimiento	90	2
Utilizar aplicaciones estándar de versiones oficiales, mantenidas y documentas	90	2

Función : Prevenir Averías

MECANISMOS EXISTENTES	IM%	CM%
Instalar conexiones eléctricas con toma de tierra	60	3
Limpiar los suelos regularmente	90	3
Situar áreas de seguridad alejadas de aeropuertos	100	3
Situar áreas de seguridad alejadas de vías de tren	100	3
Situar áreas de seguridad alejadas de autopistas con tráfico denso	100	3
Establecer un programa de mantenimiento regular	60	5

Función :Limitar el alcance de un corte eléctrico

MECANISMOS EXISTENTES	IM%	CM%
Contar con fuentes de energía secundaria y generadores permanentes	60	34

Función :Prevenir Errores

MECANISMOS EXISTENTES	IM%	CM%
Implantar estándares de documentación para formatos de entrada y salida	60	1
Utilizar software de base experimentado	90	1
Obtener información sobre el proveedor de software	90	1

Función: Limitar el Alcance de incendio

MECANISMOS EXISTENTES	IM%	CM%
Construir subsuelo sólido de hormigón, no combustible	90	
Canalizar el Cableado subterráneo a través de conductos	60	
Canalizar a través de conductos los cables que conectan alumbrado del techo	90	

Función: Prevenir Incendios

MECANISMOS EXISTENTES	IM%	CM%
Aislar el área de seguridad de lugares con riesgo de fuego (cafetería, productos químicos, basura, etc.)	90	5
Situar áreas de seguridad alejadas de zonas con alto potencial de incendios	90	5
Situar áreas de seguridad alejadas de zonas de bosque denso	100	5

Función : Copias de seguridad

MECANISMOS EXISTENTES	IM%	CM%
Almacenar las copias de seguridad en un lugar alejado de áreas de seguridad	90	3
Guardar las copias de seguridad de los ficheros críticos en lugares alejados	90	3
Guardar una copia del sistema en un lugar	90	3

CÁLCULO DEL RIESGO EFECTIVO

• Evaluación de la EFEctividad (EFE) de las funciones de salvaguarda FNCi, considerando los mecanismos MECi existentes EFE = e e (CMi * IMEi).

Control de Acceso Físico

EFE = (0.03*0.9)+(0.03*0.3)+(0.03*0.9)+(0.03*0.9)+(0.03*0.9)+(0.03*0.9)+ (0.03*0.9)

EFE = 0.17 = 17%

Control de Acceso Lógico

EFE = (0.6*0.02)+ (0.6*0.02)+ (0.6*0.02)+ (0.6*0.02)+(0.9*0.02)+ (0.9*0.02)+ (0.9*0.02)+ (0.9*0.02)+ (0.9*0.02)+ (1*0.02)+(1*0.02)+(0.6+0.1)

EFE = 0.23.8 = 23.8%

Procedimientos Físicos

EFE = (0.24*0.3)+(0.02*0.9)+(0.02*0.9) +(0.02*0.9)+(0.02*0.9)+(0.02*0.9)

EFE = 0.162 = 16.2%

Procedimientos Lógicos

EFE = (0.02*0.9)+(0.02*0.9)

EFE = 0.036 = 3.6%

Prevenir Averías

EFE = (0.6*0.03)+(0.6*0.05)+(1*0.03) +(1*0.03) +(1*0.03)+(0.9*0.03)

EFE = 0.165 = 16.5%

Limitar el Alcance de un Corte Eléctrico

EFE = (0.34*0.6)

EFE = 0.204 = 20.4%

Prevenir Errores

EFE = (0.01*0.6)+(0.01*0.9)+(0.01*0.9)

EFE = 0.024 = 2.4%

Limitar el Alcance del Incendio

EFE = (0.02*0.6)+(0.02*0.9)+(0.02*0.9)

EFE = 0.048 = 4.8%

Prevenir Incendios

EFE = (0.9*0.05)+(0.9*0.05)+(1*0.05)

EFE= 0.14=14%

Copias de Seguridad

EFE = (0.9*0.03)+ (0.9*0.03)+ (0.9*0.03)

EFE = 0.081 = 8.1%

FUNCION	**EFECTIVIDAD MECANISMOS EXISTENTES(EFE)%**
Control de Acceso Físico	17
Control de Acceso Lógico	23.8
Procedimientos Físicos	16.2
Procedimientos Lógicos	3.6
Prevenir Averías	16.5

Limitar el Alcance de un Corte Eléctrico	20.4
Limitar el Alcance de un Incendio	4.8
Prevenir Incendios	14
Copias de Seguridad	8.1
Prevenir Errores	2.4

• Reevaluación de las disminuciones de vulnerabilidad DV y del impacto DI al aplicar la efectividad de las funciones de salvaguarda considerando los mecanismos existentes.

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Prevenir Incendios	0	75%	0%	75%*14%=10.5
Limitar el Alcance de Incendio	75%	0	75%*5% = 3.75%	0%

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Prevenir Avería	0	75%	0%	75%*17%=12.75%

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Limitar alcance de Corte Eléctrico	75%	0%	75%*20%=15%	0%

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Procedimientos físicos	0%	75%	0%	75%*16%=12%

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Prevenir Errores	0%	75%	0%	75% *2% = 1.5%

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Prevenir Errores	0%	75%	0%	75% *2% = 1.5%

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN AMENAZA

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Procedimientos Lógicos	0%	75%	0%	75% *4% = 3%

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Control de Acceso Físico	0%	75%	0%	75% *17% =12.75%
Procedimientos Físicos	0%	50%	0%	50%*16%=8%

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Control de acceso Lógico	0%	75%	0%	75%*24%=18%
Copias de Seguridad	75%	0%	75%*8%=6%	
Procedimientos Lógicos	0%	50%	0%	50%*4%=2%

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Control de acceso Lógico	0%	75%	0%	75%*24%=18%

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

FUNCION	DI	DV	DI aplicando EFE(DIE)	DV aplicando EFE(DVE)
Control de Acceso Físico	0%	75%	0%	75%*17%=12.75%

La mayor disminución de vulnerabilidad y la mayor disminución del impacto conseguidas para la amenazas corresponden a la aplicación de las funciones.

Aplicando las disminuciones en el cálculo del riesgo efectivo:

- Vulnerabilidad disminuida(VD) = Vulnerabilidad * (1 - DVE)
- Impacto disminuido(ID) = Impacto * (1 - DIE)
- Riesgo efectivo(RE) = Vulnerabilidad disminuida * Impacto disminuido

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

ACTIVOS	V %	IMP	VD %	ID	RE
DEPARTAMENTO	0.2	40158.4	0.17	38652.4	65.7
RED LOCAL Y COMUNICACIONES	0.2	9096.25	0.17	8755.1	14.88
MEDIOS DE ALMACENAMIENTO	0.2	2289.5	0.17	2203.6	3.7
SERVIDOR CENTRAL	0.2	7030	0.17	6766.3	11.5
EQUIPO INFORMATICO	0.2	9677.65	0.17	9314.7	15.8

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

ACTIVOS	V %	IMP	VD %	ID	RE
SERVIDOR CENTRAL	0.02	3700	0.01	3700	0.6
RED LOCAL Y COMUNICACIONES	0.02	2393.75	0.01	2393.75	0.4
EQUIPO INFORMATICO	0.02	5093.5	0.01	5093.5	0.8

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

ACTIVOS	V %	IMP	VD %	ID	RE
OPERADORES	2	15314	2	15314	306.28
DEPARTAMENTO	2	40158.4	2	40158.4	803.16

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

ACTIVOS	V %	IMP	VD %	ID	RE
SERVIDOR CENTRAL	2	3700	2	3145	62.9
RED LOCAL Y COMUNICACIONES	2	2393.75	2	2034.6	40.6
EQUIPO INFORMATICO	2	5093.5	2	4329.4	86.5

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

ACTIVOS	V %	IMP	VD %	ID	RE
SERVIDOR CENTRAL	0.2	1850	0.17	1850	3.2
RED LOCAL Y COMUNICACIONES	0.2	2393.75	0.17	2393.75	4.2
EQUIPO INFORMATICO	0.2	2546.75	0.17	2546.75	4.4

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

ACTIVOS	V %	IMP	VD %	ID	RE
APLICACIONES	20	2992	19.7	2992	589.4
SOFTWARE BASE	20	6121.5	19.7	6121.5	1205.9

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

ACTIVOS	V %	IMP	VD %	ID	RE
APLICACIONES	0.2	1496	0.19	1496	2.94

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

ACTIVOS	V %	IMP	VD %	ID	RE
APLICACIONES	20	1496	19.7	1496	294.7

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

ACTIVOS	V %	IMP	VD %	ID	RE
SERVIDOR CENTRAL	0.2	3700	0.17	3700	6.4
MEDIOS DE ALMACENAMIENTO	0.2	602.5	0.17	602.5	1.05
RED LOCAL Y COMUNICACIONES	0.2	2393.75	0.17	2393.75	4.17
EQUIPO INFORMATICO	0.2	5093.5	0.17	5093.5	8.8

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

ACTIVOS	V %	IMP	VD %	ID	RE
PROCESOS PERSONAL Y LOGISTICA	0.2	46	0.16	43.24	0.07
DISPONIBILIDAD DE LA INFORMACION	0.2	300	0.16	282	0.46
PROCESOS FINANCIEROS	0.2	1008.5	0.16	947.9	1.5

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

ACTIVOS	V %	IMP	VD %	ID	RE
PROCESOS PERSONAL Y LOGISTICA	0.2	92	0.16	92	0.15
DISPONIBILIDAD DE LA INFORMACION	0.2	600	0.16	600	0.9
PROCESOS FINANCIEROS	0.2	2017	0.16	2017	3.3

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

ACTIVOS	V %	IMP	VD %	ID	RE
SERVIDOR CENTRAL	0.2	3700	0.17	3700	6.4
RED LOCAL	0.2	2393.75	0.17	2393.75	4.17
EQUIPO INFORMATICO	0.2	5093.5	0.17	5093.5	8.8

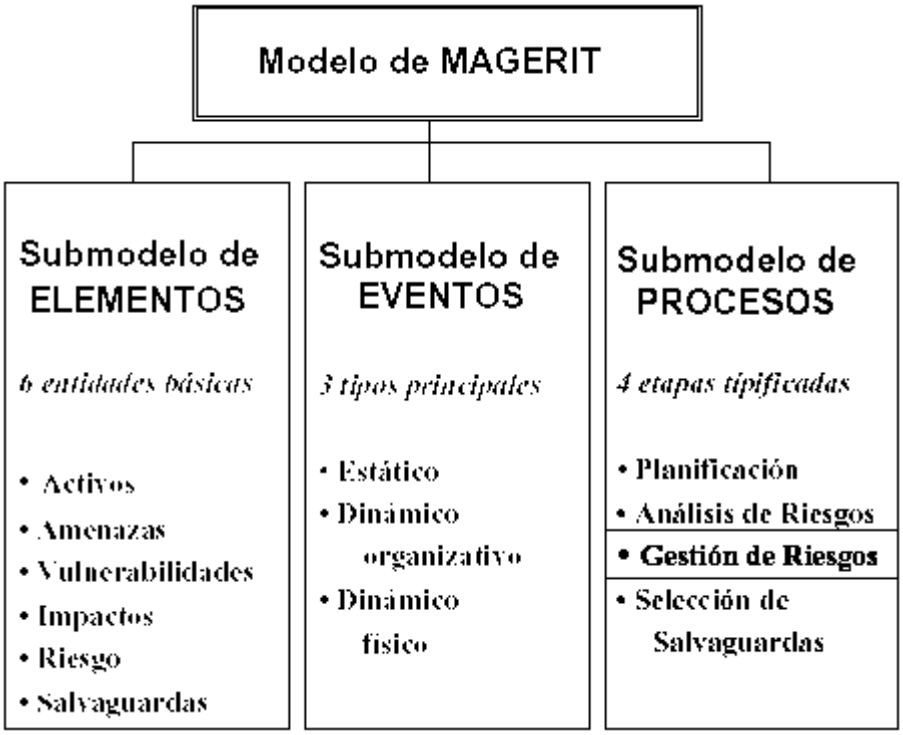
P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

ACTIVOS	V %	IMP	VD %	ID	RE
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICO	0.2	95	0.2	95	0.19
MANIPULACION Y CONTROL DE LA RED	0.2	1140	0.2	1140	2.28
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS	0.2	1932.3	0.2	1932.3	3.86

V.- ETAPA 3: GESTIÓN DEL RIESGO

5.1.- UBICACIÓN DE LA ETAPA 3 EN EL MODELO DE MAGERIT

Figura 5.1 Ubicación de la etapa 3 en el modelo de MAGERIT



5.2.- ESTRUCTURA DE LA ETAPA 3

GESTION DE RIESGOS

Interpretación del Riesgo

Identificación y Estimación de Funciones de Salvaguarda

Selección de Funciones de Salvaguarda

Cumplimiento de Objetivos

5.3.- VISIÓN GLOBAL DE LA ETAPA

Esta Etapa tiene por objeto identificar y seleccionar las funciones de salvaguarda apropiadas para reducir el riesgo a un nivel aceptable.

5.4 ACTIVIDAD 1: INTERPRETACIÓN DEL RIESGO

Los puntos de partida para esta Actividad están constituidos por la documentación de la Etapa anterior que describe los componentes del riesgo (activos, funciones y mecanismos de salvaguarda existentes, amenazas, vulnerabilidades e impactos) y los niveles de riesgos calculados.

Tarea única: Interpretar y manejar los riesgos

Riesgos Intrínseco y Riesgos Efectivos por orden Decreciente para identificar los riesgos más altos y sus amenazas.

Tabla 5.1 Riesgo Intrínseco y Efectivo por orden decreciente

AMENAZA	ACTIVOS	RI	RE
ERRORES	SOFTWARE BASE	1224	1202
FENÓMENOS SISMICOS	DEPARTAMENTO	800	800
ERRORES	APLICACIONES	598	588
FENÓMENOS SISMICOS	OPERADORES	306	306
ERRORES DE RUTA Y SECUENCIA	APLICACIONES	299	295
CORTE SUMINISTRO	EQUIPO INFORMATICO	102	86
INCENDIO	DEPARTAMENTO	80	70
CORTE SUMINISTRO	SERVIDOR CENTRAL	74	63
CORTE SUMINISTRO	RED LOCAL Y COMUNICACIONES	48	41
INCENDIO	EQUIPO INFORMATICO	19	17
INCENDIO	RED LOCAL Y COMUNICACIONES	18	16
INCENDIO	SERVIDOR CENTRAL	14	12
SUSTRACCIÓN FISICA	EQUIPO INFORMATICO	10	9

ATAQUE FISICO	EQUIPO INFORMATICO	10	9
SUSTRACCIÓN FISICA	SERVIDOR CENTRAL	7	6
ATAQUE FISICO	SERVIDOR CENTRAL	7	6
ACCIDENTES DIVERSOS	EQUIPO INFORMATICO	5	4
ACCIDENTES DIVERSOS	RED LOCAL Y COMUNICACIONES	5	4
SUSTRACCIÓN FISICA	RED LOCAL Y COMUNICACIONES	5	4
ATAQUE FISICO	RED LOCAL Y COMUNICACIONES	5	4
INDISPONIBILIDAD DE PERSONAL	DIRIRGIR, COORDINAR Y CONTROLAR PROCESOS FINAN.	4	4
INCENDIO	MEDIOS DE ALMACENAMIENTO	5	4
ATAQUE LOGICO	PROCESOS FINANCIEROS	4	3
ERRORES DE DISEÑO	APLICACIONES	3	3
ACCIDENTES DIVERSOS	SERVIDOR CENTRAL	4	3
SUSTRACIÓN LOGICA	PROCESOS FINANCIEROS	2	2
INDISPONIBILIDAD DE PERSONAL	MANIPULAR Y CONTROL DE LA RED	2	2
ATAQUE LOGICO	DISPONIBILIDAD DE LA INFORMACIÓN	2	2
FALLO DE EQUIPO FISICO	EQUIPO INFORMATICO	1	1
FALLO DE EQUIPO FISICO	SERVIDOR CENTRAL	1	1
SUSTRACCIÓN FISICA	MEDIOS DE ALMACENAMIENTO	1	1
SUSTRACCIÓN LOGICA	DISPONIBILIDAD DE LA INFORMACIÓN	1	1
FALLO DE EQUIPO FISICO	RED LOCAL Y COMUNICACIONES	0	0
SUSTRACCIÓN LOGICA	PROCESOS DE PERSONAL Y LOG	0	0
ATAQUE LÓGICO	PROCESOS DE PERSONAL Y LOG	0	0
INDISPONIBILIDAD DE PERSONAL	CAPACITACION PERSONAL Y ABASTECIMIENTO LOG.	0	0

5.5.- ACTIVIDAD 2: IDENTIFICACIÓN Y ESTIMACIÓN DE FUNCIONES Y SERVICIOS DE SALVAGUARDA

Esta Actividad permite identificar las funciones o servicios de salvaguarda que reducen el riesgo, así como estimar su eficacia para lograr dicha reducción.

Tarea 2.1: Identificar funciones y servicios de salvaguarda

Control de acceso físico
Limitar el alcance del acceso físico
Control de acceso lógico
Limitar el alcance del acceso lógico
Prevenir la divulgación
Copias de seguridad
Procedimientos físicos
Limitar el alcance de los incidentes con personal
Formación
Limitar el alcance del ataque físico
Procedimientos lógicos
Limitar el alcance del ataque lógico
Limitar el alcance de los errores
Limitar el alcance de las averías
Prevenir averías
Limitar el alcance de los cortes de suministro eléctrico
Limitar el alcance de un corte eléctrico
Prevenir errores
Transferir riesgo
Prevenir incendios
Limitar el alcance del incendio
Plan de contingencias
Prevenir inundaciones
Limitar el alcance de las inundaciones

Tarea 2.2: Estimar la efectividad de las funciones y servicios de salvaguarda

La estimación se lo realizo en él capitulo IV

Actividad 3: Selección de Funciones y Servicios de Salvaguarda
La Actividad permite seleccionar las funciones o servicios de salvaguarda convenientes y justificados como proporcionados a los riesgos que deben cubrir e incluso como óptimos.

Tarea 3.1: Aplicar los parámetros de selección

DIM = Disminución máximo del impacto

DVM = Disminución máximo de la vulnerabilidad

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

FUNCION	DIM	DVM	E%
Limitar el Alcance de Incendio	75%	0	4.80
Prevenir Incendio	0	75%	14

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN

O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

FUNCION	DIM	DVM	E%
Prevenir Avería	0	75%	7
Limitar el Alcance de Avería	75%	0	0

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

FUNCION	DIM	DVM	E%
Limitar el Alcance de Incidentes de Personal	0	75%	0
Formación	75%	75%	0

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA,

AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

FUNCION	DIM	DVM	E%
Limitar el Alcance de Corte Eléctrico	75%	0%	20.40

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

FUNCION	DIM	DVM	E%
Procedimientos físicos	0	75%	16.20

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

FUNCION	DIM	DVM	E%
Prevenir Errores	0	75%	2.40
Limitar Alcance de Errores	75%	0	0

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

FUNCION	DIM	DVM	E%
Prevenir Errores	0	75%	2.40

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

FUNCION	DIM	DVM	E%
Procedimientos Lógicos	0	75%	3.60

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN
DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU

INFRAESTRUCTURA)

FUNCION	DIM	DVM	E%
Control de Acceso Físico	0	75%	17.10
Procedimientos Físicos	0	50%	16.20

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

FUNCION	DIM	DVM	E%
Control de Acceso Lógicos	0	75%	23.60
Procedimientos Lógicos	0	50%	3.60
Copias de Seguridad	75%	0	8.10

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

FUNCION	DIM	DVM	E%
Control de Acceso Lógicos	0	75%	23.60
Limitar el Alcance de Ataque Lógico	75%	0	0

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN

REEMISOR ‘MAN IN THE MIDDLE’ DE LOS MENSAJES; REQUIERE LECTURA Y

ESCRITURA)

FUNCION	DIM	DVM	E%
Control de Acceso Físico	0	75%	17.10
Limitar Alcance de un Ataque Físico	75%	0	0

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO,

ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

FUNCION	DIM	DVM	E%
Limitar Alcance de un Ataque Físico	75%	0	0

Tarea 3.2: Reevaluar el riesgo

La máxima disminución de vulnerabilidad y la máxima disminución del impacto conseguidas para la amenazas corresponden a la aplicación de las funciones, y aplicando las disminuciones en el cálculo del riesgo efectivo que en este caso será el riesgo residual nos queda:

- Vulnerabilidad Máximo(VM) = Vulnerabilidad * (1 - DVM)
- Impacto Máximo(IM) = Impacto * (1 - DIM)
- Riesgo Residual(RR) = Vulnerabilidad Máximo * Impacto Máximo

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

ACTIVOS	V %	IMP	VM %	IM	RR
DEPARTAMENTO	0.2	40158	0.05	10039	5
RED LOCAL Y COMUNICACIONES	0.2	9096	0.05	2274	1
MEDIOS DE ALMACENAMIENTO	0.2	2289	0.05	572	0
SERVIDOR CENTRAL	0.2	7030	0.05	1757	1
EQUIPO INFORMATICO	0.2	9678	0.05	2419	1

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN
O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

ACTIVOS	V %	IMP	VM %	IM	RR
SERVIDOR CENTRAL	0.02	3700	0.005	925	0
RED LOCAL Y COMUNICACIONES	0.02	2394	0.005	598	0
EQUIPO INFORMATICO	0.02	5094	0.005	1274	0

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
OPERADORES	2	15314	0.5	3829	19
DEPARTAMENTO	2	40158	0.5	10040	50

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA,

AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
SERVIDOR CENTRAL	2	3700	2	925	18
RED LOCAL Y COMUNICACIONES	2	2394	2	599	12
EQUIPO INFORMATICO	2	5094	2	1274	25

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE,

CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
SERVIDOR CENTRAL	0.2	1850	0.05	1850	1
RED LOCAL Y COMUNICACIONES	0.2	2394	0.05	2394	1
EQUIPO INFORMATICO	0.2	2547	0.05	2547	1

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
APLICACIONES	20	2992	5	748	37
SOFTWARE BASE	20	6122	5	1531	77

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
APLICACIONES	0.2	1496	0.05	1496	1

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
APLICACIONES	20	1496	5	1496	75

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
SERVIDOR CENTRAL	0.2	3700	0.05	3700	2
MEDIOS DE ALMACENAMIENTO	0.2	603	0.05	603	0
RED LOCAL Y COMUNICACIONES	0.2	2394	0.05	2394	1
EQUIPO INFORMATICO	0.2	5094	0.05	5094	3

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
PROCESOS PERSONAL Y LOGISTICA	0.2	46	0.05	12	0
DISPONIBILIDAD DE LA INFORMACION	0.2	600	0.05	150	0
PROCESOS FINANCIEROS	0.2	1009	0.05	252	0

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN

(REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

ACTIVOS	**V %**	**IMP**	**VD %**	**ID**	**RR**
PROCESOS PERSONAL Y LOGISTICA	0.2	92	0.05	23	0
DISPONIBILIDAD DE LA INFORMACION	0.2	1200	0.05	300	0
PROCESOS FINANCIEROS	0.2	2017	0.05	504	0

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN
REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

ACTIVOS	**V %**	**IMP**	**VD %**	**ID**	**RR**
SERVIDOR CENTRAL	0.2	3700	0.05	925	0
RED LOCAL	0.2	2394	0.05	598	0
EQUIPO INFORMATICO	0.2	5094	0.05	1274	1

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

ACTIVOS	**V %**	**IMP**	**VM %**	**IM**	**RR**
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICO	0.2	95	0.2	24	0
MANIPULACION Y CONTROL DE LA RED	0.2	1140	0.2	285	1
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS	0.2	1932	0.2	483	1

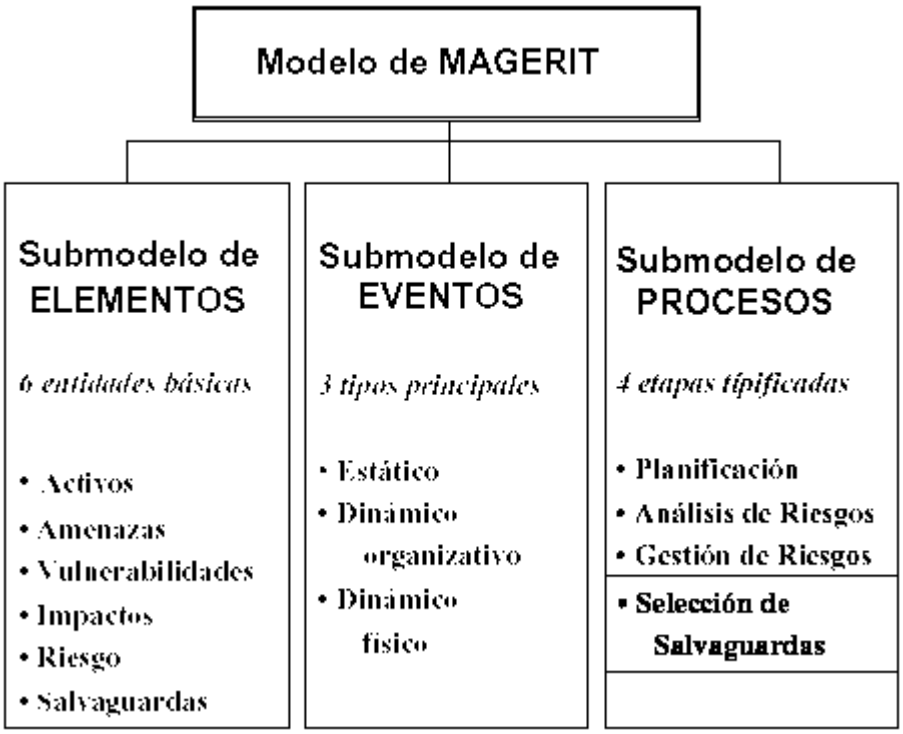
Actividad 4: Cumplimiento de objetivos

La actividad explora si los riesgos efectivos obtenidos por la aplicación sucesiva de las funciones y servicios de salvaguarda seleccionados se encuentran bajo los limites de riesgo elegidos.

VI.- PLAN DE CONTINGENCIA SELECCIÓN DE MECANISMOS DE SALVAGUARDA EN LA ESPEL

6.1.- UBICACIÓN DE LA ETAPA 4 EN EL MODELO DE MAGERIT

Figura 6.1 Ubicación de la etapa 4 en el modelo de MAGERIT



6.2.- ESTRUCTURA DE LA ETAPA 4

SELECCIÓN DE SALVAGUARDAS

Identificación de Mecanismos de Salvaguarda

Selección de Mecanismos de Salvaguarda

Especificación de los Mecanismos de Salvaguarda

Planificación de la Implantación

Integración de los resultados

6.3.- VISIÓN GLOBAL DE LA ETAPA 4

La Etapa tiene como Objetivo la Selección de los mecanismos de salvaguarda que materialicen las funciones y servicios de salvaguarda, respeten las restricciones y reduzcan los riesgos.

6.4.- ACTIVIDAD 1: IDENTIFICACIÓN DE MECANISMOS DE SALVAGUARDA

Tras seleccionar en la etapa anterior las Funciones y Servicios de salvaguarda capaces de mantener los riesgos, esta actividad procede a identificar y analizar los posibles mecanismos de salvaguarda que materialicen las mencionadas funciones.

Tarea 1: Identificar mecanismos posibles y mecanismos implantados

CM = Grado de Cumplimiento
ME = Mecanismo Existente
MS = Mecanismo Simulado
N = NO
S = SI

Tabla 6.1 Mecanismos por Función

Control de acceso físico

Mecanismo	**CM%**	**E**	**S**
Utilizar tarjetas identificativas personalizadas	3	N	S
Disponer de las fotos de todos los empleados con acceso	3	N	S
Permitir el acceso solamente a aquellas personas debidamente identificadas	3	N	S
No permitir acceso a acompañantes de las personas identificadas	3	N	S
Verificar la identidad de todo el personal que accede al edificio	3	N	S
No permitir que puerta del ascensor abra en el interior del área de seguridad	3	N	N
Construir pasillos y vestíbulos sin puertas falsas	3	S	S

Controlar los accesos al área de seguridad a través de las escaleras	3	N	N
Controlar los accesos al área de seguridad a través de los montacargas	3	N	N
Colocar rejas en las ventanas exteriores que estén al nivel de la calle	3	N	S
Cerrar las puertas del área de seguridad en periodos de inactividad	3	S	S
Establecer un procedimiento de control de visitantes	3	N	S
Numerar los pases temporales para controlar sus usuarios	3	N	N
Hacer pases temporales difíciles de duplicar	3	N	N
Registrar las entradas y salidas de los visitantes	3	N	S
Acompañar las visitas por personal del centro	3	N	S
No permitir el acceso de las visitas a zonas estrictamente confidenciales	3	S	S
Establecer controles físicos (tarjetas, torniquetes, etc.) al área de seguridad	3	N	S
Controlar todos los accesos por un guardia de seguridad o personal	3	S	S
Reducir el número de accesos al área de seguridad	3	S	S
Instalar mecanismos de cierre automático en todas las puertas internas	3	N	N
Establecer controles periódicos de seguridad para todo el personal	3	N	S
No poner ventanas ni paredes exteriores que permitan el paso a saboteadores	3	S	S
Establecer un sistema de control de firmas para controlar el acceso a los datos	3	N	S
No establecer indicadores sobre la ubicación del área de seguridad	3	S	S
No realizar el acceso a las zonas de servicio por las áreas de seguridad	3	N	N
Identificar al personal externo	3	N	S
Comprobar los requisitos de acceso y emplazamiento de los equipos locales	3	N	S
Comprobar los requisitos de acceso y emplazamiento de los equipos remotos	3	N	N
Implantar acceso a los terminales restringido por cerraduras	3	N	S
Comprobar periódicamente la rigidez del sistema de control de accesos	3	N	S
Asegurar encargados presentes durante la intervención	3	N	S
Implantar sistemas biométricos de autenticación	3	N	N

Control de acceso lógico

Bloquear acceso a ficheros de contraseñas	2	N	S
Comprobar periódicamente las listas de control de acceso	2	N	S
Implantar sistemas de contraseñas	10	S	S
Implantar contraseñas difíciles de adivinar	2	S	S
Utilizar sistemas operativos con utilidades incorporadas para control de acceso	2	S	S
Restringir el acceso a las utilidades del sistema	2	S	S
Proteger las contraseñas a prueba de modificaciones	2	N	S
Implantar intervalo de cambio de contraseñas adecuado	2	N	S
Combinar contraseñas con llaves físicas	2	N	S
Asegurar que software del sistema permite control de los privilegios	2	S	S
Asegurar acceso restringido a las listas de acceso y de privilegios	2	N	N
Controlar la utilización de procedimientos administradores	2	N	N
Asegurar el grado de control de acceso por usuario/aplicación/fichero	2	N	N

Asegurar sistema de control de acceso compatible con otras aplicaciones	2	N	S
Asegurar el sistema de control de acceso permite una carga progresiva	2	N	N
Implantar sistema de control de accesos fácil de gestionar	2	N	S
Proporcionar los propietarios de la información los derechos de acceso	2	S	S
Nombrar encargado de la administración y gestión de los derechos de acceso	2	N	N
Actualizar continuamente la lista de derechos de acceso ante cualquier cambio	2	N	S
Asegurar el constructor del sist. control de acceso proporciona nuevas versiones	2	N	N
Asegurar sist.control de accesos diferencia los accesos locales de los remotos	2	N	N
Asegurar sistema de identificación actualizado de cada usuario	2	N	S
Asegurar sistema de autenticación de cada usuario (contraseña, llave, ..)	2	N	S
Asegurar contraseñas con un mínimo de 5 caracteres de longitud	2	S	S
Asegurar contraseñas sin eco en pantalla	2	N	S
Asegurar solo el usuario define la contraseña	2	S	S
Asegurar que contraseña proporcionada por el sistema tiene una validez temporal	2	N	S
Asegurar que las contraseñas no se pueden reutilizar	2	S	S
Asegurar control periódico aleatorio de cuentas estratégicas	2	N	S
Almacenar las contraseñas de forma cifrada, con algoritmo irreversible	2	N	S
Proporcionar información a los usuarios de las normas respecto a las contraseñas	2	S	S
Implantar procedimiento de difusión, conservación y utilización de contraseñas	2	N	S
Asegurar desconexión en caso de un periodo de inactividad	2	S	S
Asegurar bloqueo del terminal en el caso de tres intentos infructuosos	2	N	S
Asegurar desbloqueo de terminales con intervención del administrador	2	N	S
Asegurar autorización de acceso con un plan horario y según un calendario	2	N	S
Realizar registro y seguimiento de los intentos infructuosos	2	N	S
Separar lógica y físicamente los terminales de acceso a diferentes redes	2	N	N
Utilizar los procedimientos de identificación del tipo de acceso	2	N	S
Utilizar el procedimiento de control de la identidad	2	N	S
Repudiar las conexiones donde no se establece la identificación del terminal	2	N	S
Utilizar subsistemas jerárquicos con acceso separado	2	N	S
Asegurar que el control de acceso funciona con lenguajes de selección	2	S	S
Implantar utilidades y herrami. del sistema con acceso restringido y controlado	2	N	S
Implantar procedimientos complementarios de autenticación en los programas	2	N	S
Implantar controles de acceso a las tablas limitando visibilidad y acceso	2	N	S

Copias de seguridad

Almacenar las copias de seguridad en un lugar alejado de áreas de	3	S	S

seguridad			
Guardar las copias de seguridad de los ficheros críticos en lugares alejados	3	S	S
Situar los duplicados en una área de seguridad diferente a la de los originales	3	N	S
Realizar inventario de las copias de seguridad	3	N	S
Comprobar las copias de seguridad	3	N	S
Realizar copias de seguridad de las aplicaciones en desarrollo	3	N	N
Realizar copias de seguridad frecuentes	13	N	S
Realizar duplicados de la documentación	3	N	S
Almacenar los duplicados en edificios separados de los originales	3	N	S
Revisar periódicamente los duplicados	3	N	S
Coordinar los procedimientos de copia de seguridad con la duplicación de la doc.	3	N	S
Duplicar los ficheros de back up	3	N	N
Guardar una copia del sistema en un lugar seguro	3	S	S
Revisar y probar las copias periódicamente	3	N	S
Establecer los pasos para duplicar ficheros, programas, software, etc.	3	N	S
Almacenar todas las copias de la documentación en un lugar seguro	3	N	S
Realizar estudio de cada elemento a incluir en la copia de seguridad	3	N	S
Implantar procedimiento de copias de seguridad	12	N	S
Realizar verificación periódica de las copias de seguridad	3	N	S
Asegurar contenido de las copias de seguridad cifrado	3	N	S
Almacenar copias de seguridad en áreas de seguridad distintas a originales	3	N	S
Asegurar que el almacenamiento de copias de seguridad se realiza puntualmente	3	N	S
Realizar duplicado document.explotación en área seguridad distinta a originales	3	N	N
Realizar duplicado document.desarrollo en área .seguridad distinta orig	3	N	N
Comparar ejecuciones de aplicaciones en explotación con la de las copias	3	N	N
Realizar reserva de seguridad de soportes en otro edificio	3	N	S
Realizar reserva de seguridad de los elementos no importantes	3	N	N

Procedimientos físicos

Aislar el área de seguridad de zonas donde se realicen procesos peligrosos	2	S	S
Asegurar las estanterías de cintas y demás equipamiento	2	N	S
Planificar el transporte de ficheros para casos de emergencia	2	N	S
Contratar vigilantes nocturnos permanentes	24	S	S
Colocar el equipo de aire acondicionado en un lugar alto y acceso restringido	2	N	N
Cubrir las tomas de aire con una pantalla protectora	2	N	N
Instalar voltaje suficiente para soportar el equipo a pleno rendimiento	2	N	S
Situar cuadro de mandos principal en lugar alejado y de acceso restringido	2	N	S
Asegurar que todos los circuitos están reforzados	2	N	S

Asegurar que todos los circuitos tienen su correspondiente toma de tierra	2	S	S
Situar áreas de seguridad alejadas de líneas de alto voltaje	2	S	S
Situar áreas de seguridad alejadas de zonas con alto porcentaje de crimen	2	S	S
Situar áreas de seguridad alejadas de zonas almacenamiento de productos peligrosos	2	S	S
No permitir la introducción de ningún objeto en el área de seguridad	2	N	S
Colocar cristales antibalas en las ventanas exteriores	2	N	N
Situar las zonas con ficheros en lugar estrictamente protegido	2	N	N
Limpiar regularmente las lentes de los circuitos cerrados de televisión	2	N	N
Detectar conflictos entre empleados	2	N	S
Realizar inspección periódica para identificar mejoras en normas de seguridad	2	N	S
No posibilitar a empleados acceso a las herramientas (destornilladores, etc.)	2	N	S
Situar la librería de soportes en una área de seguridad independiente	2	N	N
Mantener protección en el transporte	2	N	N
Asegurar coordinación entre departamentos para la gestión de la información	2	N	S
Asegurar coordinación entre departamentos para el reclutamiento de personal	2	N	S
Controlar la utilización del sistema de información	2	N	N
Controlar registro de las actividades que se realicen contra la información	2	N	S
Llevar a cabo controles de seguridad en la instalación	2	N	S
Crear un área de trabajo del cliente segura	2	N	S
Establecer procedimientos adecuados de control y operación	2	N	S
Registrar las comunicaciones realizadas	2	N	S
Nombrar administrador responsable de los datos	2	N	S
Nombrar administrador de la instalación, modificación y superv.estruc.ficheros	2	N	S
Implantar procedimientos escritos para el archivado y desarchivado	2	N	S
Ubicar archivos/librerías en áreas de seguridad	2	N	S
Implantar procedimiento de utilización de contenedores en caso de transporte	2	N	S
Asegurar acreditación del servicio de transporte	2	N	N
Asegurar que empresa de transporte no depende jurídicamente de la empresa destino	2	N	N
Implantar procedimientos para la prevención y protección (firmas)	2	N	N
Implantar procedimiento para aprovisionamiento, almacén. y gestión de soportes	2	N	N

Limitar el alcance de los incidentes con personal

Simular situaciones de desastre para ejercitar el plan de evacuación	7	N	S
Revisar y mantener disponibles los planes de evacuación	9	N	S
Liberar todas las puertas internas y pasillos de toda obstrucción	7	N	S
Colocar el equipamiento de tal manera que no obstruyan la apertura de puertas	7	N	S

Disponer de un botiquín o servicio médico próximo al área de seguridad	7	N	S
Hacer pública de forma notoria los planes de evacuación	7	N	S
Hacer pública de forma notoria los botiquines de primeros auxilios	7	N	S
Hacer pública de forma notoria las rutas y salidas de emergencia	7	N	S
Situar equipo de primeros auxilios fácilmente accesible	7	N	S
Nombrar encargados de supervisar las medidas de evacuación	7	N	S
Nombrar encargados de avisar a los servicios (ambulancias, bomberos, etc.)	7	N	S
Nombrar encargados de cortar la corriente eléctrica	7	N	S
Nombrar encargados de apagar el aire acondicionado	7	N	N
Nombrar encargados de atender al personal herido	7	N	N

Formación

Formar regularmente al personal en las técnicas de lucha contra el fuego	9	N	S
Formar al personal para actuar en caso de amenaza de bomba	9	N	S
Implantar programa continuado de formación en seguridad	10	N	N
Formar ante emergencias y evacuación	9	N	S
Realizar sesiones de orientación sobre procedimientos de emergencia	9	N	S
Realizar prácticas en temas de seguridad	9	N	S
Comprobar la formación en temas de seguridad	9	N	S
Asegurar el conocimiento de las normas de emergencia	9	N	S
Comprobar periódicamente el conocimiento de las normas de emergencia	9	N	S
Incluir el conocimiento de las normas de emergencia en el plan de formación	9	N	S
Formar al personal en primeros auxilios	9	N	S

Limitar el alcance del ataque físico

Almacenar sólo los soportes imprescindibles (cintas, discos) en áreas de seguridad	1	N	S
Reducir al mínimo las cintas almacenadas fuera de la biblioteca de cintas	1	N	N
Instalar una caja fuerte de datos alejada de áreas de seguridad	1	N	N
Seleccionar medios de almacenamiento alternativos	1	N	N
Almacenar en lugar alejado soportes con informes y formularios críticos	1	N	N
Realizar inspecciones regulares de sist. de protección y detección automática	1	N	N
Instalar equipos de detección óptica o rayos ultravioletas	1	N	N
Proveer a los equipos de detección de mecanismos de alarma automática	7	N	N
Colocar estratégicamente varios sistemas manuales de alarma	1	N	S
Apagar automáticamente el equipamiento crítico por los mecanismos de alarma	1	N	N
Analizar el sistema de detección por parte de expertos	1	N	N
Facilitar acceso a las instalaciones para los equipos de emergencia	1	N	S
Facilitar acceso sin demora por parte del equipo de emergencia	1	N	S
Proveer mapa con la localización de los dispositivos de alarma	1	N	S
Disponer de megáfono de emergencia	1	N	S

Conocer todo el personal su emplazamiento y cómo funciona el megáfono	1	N	S
Construir edificios resistentes a huracanes, tormentas de viento	1	N	N
Construir el edificio con unos cimientos sólidos	1	N	N
Disponer de accesos fáciles para el personal de emergencia y el equipamiento	1	N	S
Notificar al personal apropiado el advenimiento de un desastre	1	N	S
Establecer procedimientos para notificar a las autoridades civiles disturbios	1	N	S
Establecer políticas para monitorizar las amenazas	7	N	N
Instalar un circuito cerrado de televisión	7	N	N
Instalar detectores de metal a la entrada del área de seguridad	1	N	N
Establecer controles de inspección de cajas y paquetes enviados	7	N	N
Instalar mecanismos de alerta que avisen de cualquier anomalía	1	N	N
Establecer revisiones generales periódicas de todo el área de seguridad	7	N	S
Registrar todos los cambios planeados y realizados en materia de seguridad	1	N	S
Establecer reuniones trimestrales del departamento para revisar procedimientos	1	N	S
Instruir al personal de operaciones y de seguridad en reacción ante disturbios	1	N	S
Instalar sistemas de intercomunicaciones entre área de seguridad y otras áreas	1	N	N
Exámenes periódicos: seguridad, rendimiento, aptitud	1	N	S
Hacer pública de forma notoria los números de teléfonos de emergencia	1	N	S
Hacer pública de forma notoria la asignación de responsables en emergencia	1	N	S
Nombrar sustitutos de los responsables en situaciones de emergencia	1	N	S
Nombrar encargados de apagar el equipo	1	N	S
Nombrar encargado de la revisión de las normas con suficiente autoridad	1	N	S
Revisar las normas por parte de personal especializado	1	N	N
Nombrar encargado de una comprobación de seguridad semanal	7	N	N
Monitorizar las operaciones	1	N	S
Instalar detectores de campos magnéticos	1	N	N
Marcar los elementos que deban ser evacuados	1	N	S
Revisar regularmente el cumplimiento de los procedimientos	1	N	S
Almacenar los elementos en una área de seguridad independiente	1	N	N
Revisar y controlar los sistemas de seguridad	7	N	N
Establecer acuerdos contractuales	1	N	N
Asegurar existencia de una lista de teléfonos de emergencia	1	N	S
Verificar las técnicas de prevención de desastres	1	N	S
Asegurar sistemas de protección elaborados	1	N	N
Asegurar análisis periódico de la calidad de las líneas	1	N	N
Asegurar seguimiento específico de los incidentes en cada línea	1	N	N
Generar informe escrito por cada intervención en la línea	1	N	N
Asegurar detección de intrusos después de las horas normales	6	N	N
Instalar sistema de alarma en caso de extracción no autorizada de los	1	N	N

soportes			
Utilizar herramientas de control y seguimiento del funcionamiento de equipos	1	N	N
Considerar la documentación de explotación en acciones a realizar en incidentes	1	N	N
Asegurar que los técnicos de mantenimiento del proveedor son los habituales	1	N	S
Mantener registro actualizado y completo de los incidentes	1	N	N
Asegurar edificios resistentes a terremotos	1	N	N

Procedimientos lógicos

Nombrar encargados de los ficheros críticos	3	N	S
Verificar periodos de inactividad	3	N	S
Comprobar la ejecución de procesos en la lista de explotación	3	N	S
Ordenar los soportes	3	N	S
Mantener los soportes no utilizados en sus contenedores	3	N	S
Situar las aplicaciones, sistemas y documentación en un área de seguridad	3	N	S
Nombrar encargados de acceso a librerías de aplicaciones en áreas de seguridad	3	N	N
Implantar procedimiento de identificación y firma para la obtención de copias	3	N	S
Establecer niveles en la clasificación de seguridad	3	N	S
Crear una política de clasificación	3	N	S
Clasificar los elementos según su criticidad	3	N	S
Informar al personal de los requisitos legales asociados a la información	3	N	S
Nombrar un administrador de la seguridad	3	N	S
Asegurar el apoyo de la dirección	3	N	S
Asegurar existencia de una política de seguridad	3	N	S
Asegurar coordinación entre departamentos para planificación de servicios	3	N	S
Asegurar coordinación entre departamentos para el plan de seguridad	3	N	S
Establecer funciones de control separadas de las de organización	3	N	S
Implantar una filosofía general de la auditoría de control	3	N	S
Controlar la información de entrada para asegurar su completitud	3	N	S
Controlar las aplicaciones no salen a la línea de comandos del sistema operativo	2	N	S
Verificar el uso de los procedimientos de seguridad	2	N	S
Verificar la protección de los programas y los datos	2	N	S
Nombrar un responsable que será el interlocutor de la organización	2	N	S
Asegurar software de red estándar, fiable y con mantenimiento	2	S	S
Asegurar la red no da servicio después de las horas normales	2	N	S
Asegurar protocolos normalizados con funciones de protección integradas	2	N	S
Realizar las transacciones estratégicas solo desde terminales controlados	2	N	N
Asegurar utilización de fibra óptica	2	N	N

Realizar registro de la utilización de soportes	2	N	S
Verificar regularmente los soportes	2	N	S
Implantar procedimiento de justificación para cada lote de inform. a transferir	2	N	S
Realizar estudio de carga y rendimiento anterior a la instalación aplicaciones	2	N	S
Evitar ejecuciones remotas	2	N	N
Implantar procedimientos de explotación catalogados y con acceso restringido	2	N	S
Almacenar documentación de explotación en un área de seguridad	2	N	S
Descontaminar los soportes provenientes del exterior en equipos aislados	2	N	S
Nombrar encargado de mantenimiento a primer nivel de elementos no importantes	2	N	S
Utilizar aplicaciones estándar de versiones oficiales, mantenidas y documentadas	2	S	S
Controlar autenticación del origen e integridad del contenido de ampliaciones	2	N	

Limitar el alcance de los errores

Realizar los cambios en las copias, nunca en los originales	3	N	S
Obtener informe de errores y procedimientos de seguimiento	3	N	S
Probar todas las opciones de las aplicaciones	3	N	S
Monitorizar y controlar la depuración de los programas de seguridad	3	N	S
Comprobar la satisfacción de los usuarios	2	N	S
Utilizar vistas o bases de datos espejo	3	N	S
Analizar a diario de las operaciones de explotación	3	N	S
Verificar con periodicidad aleatoria del contenido de los procedimientos	2	N	S
Implantar procedimiento para detección de anomalías en software y en información	3	N	S
Documentar y asegurar el entorno en mantenimientos remotos	2	N	N
Mantener registro actualizado y completo de las intervenciones de proveedores	3	N	S
Implantar procedimientos de revisión en aplicaciones (creación o manten.)	3	N	S
Implantar procedimiento de revisión general antes de pasar a explotación	3	N	S
Asegurar que los desarrollos externos pasan un periodo de prueba	3	N	S
Asegurar que el procedimiento de revisión incluye los estudio iniciales	3	N	S
Asegurar que el procedimiento de revisión incluye los juegos de pruebas	3	N	S
Asegurar que el procedimiento de revisión incluye los mecanismos de seguridad	3	N	S
Asegurar que procedimiento de revisión incluye la documentación de explotación	3	N	S
Asegurar que procedimiento de revisión incluye el régimen de copias de seguridad	3	N	S
Asegurar que procedimiento de revisión incluye funcionamiento en modo degradado	3	N	S
Asegurar que el procedimiento de revisión incluye los estimadores	3	N	S

técnicos			
Asegurar que procedimiento de revisión cumple los estándares de la metodología	3	N	S
Asegurar que el procedimiento para pruebas cumple la metodología	3	N	S
Asegurar juegos de pruebas exhaustivos	3	N	S
Asegurar juegos de pruebas definidos por los usuarios	3	N	S
Asegurar procedimiento de pruebas incluye la revisión anual de los proc. en exp.	3	N	S
Asegurar control y actualización periódica (semanal) de la planificación	3	N	S
Nombrar responsable de calidad de trabajos respecto a normas de análisis/prog.	3	N	S
Verificar que los controles asociados a los datos se reproducen en todos prog.	3	N	S
Implantar proced. autom. asociado al dicc. y al esquema de integración	3	N	N
Centralizar los incidentes detectados por usuarios y no controlados	3	N	S
Realizar auditoría periódica de la validez de los controles	3	N	S
Realizar verificación aleatoria de los controles con datos de prueba	3	N	S
Realizar actualización de datos estratégicos realizada en diferido	3	N	S
Realizar pruebas del software externo	2	N	S
Disponer de los fuentes de las aplicaciones externas	1	N	S

Limitar el alcance de las averías

Registrar las características de los equipos	30	N	S
Asegurar que la red está gestionada al menos por dos servidores	40	N	N
Instalar elementos con autodiagnóstico	40	N	N

Prevenir averías

Instalar conexiones eléctricas con toma de tierra	3	S	S
Limpiar regularmente la zona que se encuentra debajo del falso suelo	3	N	S
Instalar tomas de aire que eviten la polución	3	N	N
Realizar chequeos periódicos por parte del personal de seguridad	3	N	S
Comprobar el estado del cableado que se encuentra bajo el falso suelo	3	N	S
Situar áreas de seguridad alejadas de autopistas con tráfico denso	3	S	S
Situar áreas de seguridad alejadas de vías de tren	3	S	S
Situar áreas de seguridad alejadas de aeropuertos	3	S	S
Prohibir la introducción de comida y bebida en el área de seguridad	3	N	S
Limpiar regularmente la superficie del equipamiento ubicado en el área de seguri	3	N	S
Limpiar los suelos regularmente	3	S	S
Conservar limpias y ordenadas las zonas de mantenimiento	5	N	S
Limpiar debajo del falso suelo del área de seguridad	3	N	S
Establecer un procedimiento riguroso de limpieza	3	N	S
Planificar actividades de mantenimiento de los equipos	3	N	S
Comprobar la realización del mantenimiento de los equipos	3	N	S
Realizar mantenimiento de las unidades de almacenamiento	3	N	S
Examinar el funcionamiento de los equipos trimestralmente	3	N	S
Establecer un programa de mantenimiento regular	5	S	S

Asegurar acuerdos con proveedores para servicios de limpieza	3	N	S
Asegurar contrato anual con una organización de servicio de mantenimiento	3	N	N
Comprobar periódicamente el equipo de comunicaciones	3	N	S
Realizar seguimiento de los procedimientos para la conservación y restauración	3	N	S
Contratar mantenimiento de todos los elementos, con periodo de reemplazamiento	3	N	S
Fijar por contrato la duración de la intervención en el mantenimiento	3	N	S
Fijar en contrato de mantenimiento cláusulas en caso de incumplimiento	3	N	S
Establecer mantenimiento periódico fijado	3	N	S
Establecer garantía en las piezas reemplazadas	3	N	S
Limitar por contrato las responsabilidades en implantación, desplazamiento,...	3	N	S
Realizar contrato de mantenimiento de las aplicaciones	3	N	S
Establecer por contrato la disposición de nuevas versiones y/o correcciones	3	N	S

Limitar el alcance de un corte eléctrico

Instalar mecanismos de encendido automático de las luces de emergencia	3	N	N
Proveer de mecanismos manuales a los sistemas automáticos	3	N	S
Instalar sistemas de alimentación ininterrumpida para accesos controlados eleclectrónicamente	3	N	N
Contar con fuentes de energía secundarias y generadores permanentes	34	S	S
Instalar sistemas de alimentación ininterrumpida (sai)	35	N	N
Proporcionar al personal de mantenimiento y seguridad una copia del cableado	3	N	S
Instalar un sistema de alumbrado de emergencia	3	N	N
Probar con regularidad el sistema de alumbrado de emergencia	3	N	N
Comprobar que las luces de emergencia iluminan el área deseada	3	N	N
Disponer de fuentes de energía de emergencia para activar luces de emergencia	3	N	N
Proporcionar una copia del trazado de la iluminación al depart. de mantenimiento	1	N	S
Disponer de linternas de pila seca en el área de seguridad para uso de emergencia	3	N	S
Establecer procesos manuales durante el periodo de recuperación	3	N	S

Prevenir errores

Realizar pruebas a nuevos empleados: seguridad, sicológicas, referencias, aptitud	1	N	S
Existencia de responsables alertas respecto a empleados disgustados	1	N	S
Detectar insatisfacciones	1	N	S
Detectar posibles problemas familiares	1	N	S
Hacer pública una política de personal severa ante las infracciones	1	N	S
Conocer los responsables profundamente a sus subordinados	1	N	S

Nombrar encargado de la revisión de las normas con suficiente autoridad	1	N	S
Exigir responsable presente cuando se realizan mantenimientos	1	N	S
Mantener lista de personal externo para el servicio de mantenimiento	1	N	S
Supervisar las actividades del personal externo	1	N	S
Comprobar periódicamente las utilidades del software de seguridad	1	N	S
Documentar las modificaciones de las aplicaciones	1	N	S
Controlar las modificaciones de las aplicaciones	1	N	S
Controlar los cambios en las aplicaciones	1	N	S
Registrar los cambios en las aplicaciones	1	N	S
Asegurar que la documentación cumple los estándares de operación	1	N	S
Implantar estándar de documentación para diagramas de flujo y modelos lógicos	1	N	S
Implantar estándar de documentación para listados	1	N	S
Implantar estándar de documentación para formatos de entrada y de salida	1	S	S
Implantar estándar de documentación para ejemplos	1	N	S
Implantar estándar de documentación para usuario	1	N	S
Implantar estándar de documentación para pruebas	1	N	S
Implantar estándar de documentación para explicación de códigos, tablas, etc.	1	N	S
Implantar estándar de documentación para mensajes de error	1	N	S
Implantar estándar de documentación para descripción de ficheros	1	N	S
Implantar estándar de documentación para explotación	1	N	S
Realizar cambios coordinados en aplicaciones y en documentación	1	N	S
Revisar cambios en la documentación por un auditor interno	1	N	S
Participar propietarios de la información en su clasificación	1	N	S
Implantar procedimientos de identificación de la documentación	1	N	S
Implantar procedimientos de clasificación de la documentación	1	N	S
Asegurar coordinación entre departamentos para la asesoría legal	1	N	N
Asegurar coordinación entre departamentos para la auditoría	1	N	S
Asegurar que la información de salida cumple los estándares	1	N	S
Implantar control de calidad	1	N	S
Asegurar el control de las modificaciones en las aplicaciones	1	N	S
Asegurar control de las conversiones	1	N	S
Separar responsabilidades	1	N	S
Asegurar que los sistemas son auditables	1	N	S
Implicar al auditor en la fase de diseño de sistemas	1	N	N
Controlar terminales remotos solo disponibles para el personal seleccionado	1	N	N
Llevar a cabo auditorías e inspecciones sorpresa	1	N	S
Determinar la legalidad del equipamiento, datos y servicios utilizados	1	N	S
Disponer de mensajeros eficientes y fiables	1	N	S
Utilizar software de base experimentado	1	S	S
Probar las alternativas con cargas simuladas	1	N	S
Ser miembro de alguna asociación de usuarios	1	N	S
Participar regularmente en las reuniones de las asociaciones de usuarios	1	N	S
Instalar equipo de comunicaciones en un área de seguridad	1	N	S

Seleccionar la red por un estudio comparativo	1	N	S
Utilizar redes profesionales específicas (tipo swift)	1	N	N
Generar informe escrito con las modificaciones estructurales	1	N	S
Visar la utilización por el jefe de explota., responsable de operaciones,... r	1	N	S
Nombrar responsable de la gestión de los soportes	1	N	S
Reducir la intervención manual	1	N	S
Realizar auditoría no programada de procedimientos de utilización de soportes	1	N	S
Tener en consideración en el estudio, el entorno, las pruebas y los desarrollos	1	N	S
Actualizar el plan de copias de seguridad ante modificaciones en las aplicac.	1	N	S
Almacenar y actualizar los informes de actividad	1	N	S
Analizar y almacenar el informe de actividad del operador	1	N	S
Utilizar el informe de cargas y rendimiento para ampliaciones	1	N	S
Nombrar encargados de la preparación y planificación de los trabajos	1	N	S
Realizar preparación y planificación sistemática de todos los trabajos	1	N	S
Realizar planificación diaria, semanal, mensual y anual	1	N	S
Utilizar sistema de preparación y planificación automática	1	N	S
Implantar procedimientos escritos para la ejecución de pruebas	1	N	S
Documentar completamente las aplicaciones o mantenimiento. al pasar a explotación	1	N	S
Recompilar las aplicaciones en el entorno de explotación	1	N	S
No realizar personal de explotación modificaciones de procedimientos, aplicac.	1	N	S
Realizar documentación de explotación completa de cada aplicación	1	N	S
Realizar actualización sistemática de la documentación de explotación	1	N	S
Implantar documentación de explotación jerarquizada por función	1	N	S
Realizar documentación actualizada de los elementos instalados	1	N	S
Realizar seguimiento y control de las versiones	1	N	S
Realizar actualización de la documentación de las aplicaciones	1	N	S
Considerar en procedimientos docum. firmado por usuario y desarrollador	1	N	S
Asegurar procedimiento de revisión forma parte de documentación de aplicación	1	N	S
Asegurar que los mantenimientos se realizan a partir de un documento formalizado	1	N	S
Asegurar que los mantenimientos de realizan solo en el entorno de desarrollo	1	N	S
Asegurar que jefe de explot. remite a desar.y usuarios un doc. con pases a exp.	1	N	S
Implantar protocolo para comparar versiones de modificaciones importantes	1	N	S
Asegurar que las nuevas aplicaciones generan una documentación de	1	N	S
Implantar procedimiento para definir el juego de pruebas	1	N	S
Asegurar proyecto iniciado con un estudio previo y un cuaderno de carga	1	N	S
Asegurar cuaderno de carga respaldado por los usuarios y desarrolladores	1	N	S

Asegurar planificación de todos los proyectos en desarrollo	1	N	S
Aplicar una metodología para el análisis funcional	1	N	S
Asegurar que metodología de desarrollo permite integrar metodología de seguridad	1	N	S
Asegurar metodología permite definir clasificación de datos con aspectos de seg.	1	N	S
Deducir especificaciones de seguridad por la clasificación de datos y procesos	1	N	S
Asegurar clasificación de los procedimientos de seguridad	1	N	S
Aplicar una metodología para el análisis orgánico	1	N	N
Implantar método de programación estructurada, con reglas de utilización	1	N	S
Asegurar para los desarrollos externos se estipula la metodología de desarrollo	1	N	S
Realizar prototipo de las especificaciones antes de generar el análisis deta.	1	N	S
Utilizar generador de programas, pantallas e informes	1	N	S
Utilizar un diccionario de datos o repositorio	1	N	S
Asegurar que el dicc. de datos permite clasif. de seg. en las descripciones	1	N	S
Asegurar documentación de la aplicación actualizada y acorde con la metodología	1	N	S
Asegurar que la documentación incluye los esquemas de integración	1	N	S
Asegurar que la doc. incluye los esquemas de circulación de la información	1	N	S
Asegurar que la documentación incluye las referencias cruzadas	1	N	S
Asegurar que la doc. incluye las opciones técnicas, organigramas, ...	1	N	N
Asegurar en desarrollos externos la entrega de la doc.conforme a met.	1	N	N
Asegurar referencias cruzadas de controles/datos	1	N	N
Implantar procedimiento asociado al diccionario datos para analizar dependenc.	1	N	N
Generar las refs. cruzadas controles/programas para cada dato	1	N	N
Asegurar que los controles se sitúan en los programas en párrafos estructurados	1	N	N
Asegurar controles básicos (cuadre, límite de valores)	1	N	N
Asegurar controles de validación directa (condiciones)	1	N	N
Asegurar controles de validación indirecta (fórmulas)	1	N	N
Asegurar controles de coherencia (evolución, base estadística)	1	N	N
Implantar procedimiento para modificación de controles con documentación visada	1	N	N
Realizar selección del software por estudios comparativos	1	N	N
Obtener información sobre el proveedor del software	1	S	S
Seleccionar el soft teniendo en cuenta la capacidad del proveedor	1	N	N

Prevenir incendios

Aislar las áreas de seguridad de lugares con riesgo de fuego (cafeterías, productos químicos, basura, etc.)	5	S	S

Almacenar el papel y otros soportes lejos de áreas de seguridad	5	N	S
No albergar productos de limpieza inflamables o cáusticos en arreas de seguridad	5	N	S
Guardar productos inflamables (si se permiten), en contenedores seguros	5	N	S
Limpiar regularmente el subsuelo	5	N	S
No colocar percheros en el interior de áreas de seguridad	5	N	S
Mantener los medios destructores de papel alejados de áreas de seguridad	5	N	S
No almacenar piezas de plástico en el interior de áreas de seguridad	5	N	S
No decorar áreas de seguridad con posters, ni carteles	5	N	S
Prohibir fumar en áreas de seguridad y en la biblioteca de medios	5	N	S
Realizar inspecciones periódicas por parte del cuerpo de bomberos	5	N	S
Instalar equipos de detección de humos y fuentes de calor	5	N	S
Instalar detectores de productos de combustión	5	N	N
Instalar detectores de la temperatura del aire	5	N	N
Situar áreas de seguridad alejadas de zonas con alto potencial de incendios	5	S	S
Situar áreas de seguridad alejadas de zonas de bosque denso	5	S	S
No acumular basura en el área de seguridad	5	N	S
Realizar el vaciado de las papeleras fuera del área de seguridad	5	N	S
Utilizar enmoquetado y alfombrado antiestático	5	N	N
Utilizar ceniceros de agua si se permite fumar	5	N	N

Limitar el alcance del incendio

Instalar materiales no combustibles y resistentes al fuego en arreas criticas	8	N	S
Construir subsuelo sólido de hormigón, no combustible	2	S	S
Construir suelo del área de seguridad de aluminio o materiales no combustibles	2	N	N
Canalizar el cableado subterráneo a través de conductos	2	S	S
Instalar puertas, marcos y particiones de metal	2	N	N
Utilizar pinturas retardantes o resistentes al fuego en arreas de seguridad	2	N	N
Construir el techo de áreas de seguridad con materiales no combustibles	2	N	N
Canalizar a través de conductos los cables que conectan el alumbrado del techo	2	S	S
Cubrir o rociar los aislantes de sonido con materiales resistentes al fuego	2	N	N
Compartimentar áreas de seguridad para evitar propagación del fuego	2	N	N
Construir los compartimientos con materiales no combustibles	2	N	N
Extender paredes de áreas de seguridad por encima del falso techo hasta el techo real	2	N	N
Ventilar áreas de seguridad permitiendo la disipación del calor	2	N	N
Distribuir correctamente sensores de detección y agentes de extinción de incendios	2	N	N
Instalar mobiliario y elementos de decoración no combustibles	2	N	S
Colocar todos los muebles de metal	2	N	S
Separar la biblioteca de cintas de las cajas fuertes de datos	2	N	S
Mantener actualizados regularmente los procedimientos contra incendios	2	N	S

Disponer de un equipamiento adecuado de lucha contra incendios	2	N	S
Asignar responsabilidades individuales en caso de incendio	2	N	S
Probar regularmente el sistema de detección de incendios	2	N	S
Realizar pruebas frecuentes con el sistema de alarma antiincendios	2	N	S
Instalar equipos de detección de humos y fuentes de calor	2	N	S
Colocar detectores de humo que funcionen correctamente en áreas de seguridad	2	N	S
Probar el equipo detección de humos sobre unas bases programadas	2	N	S
Conectar los sistemas de detección de incendios con el panel de control general	2	N	N
Conectar los sistemas de detección de incendios con la policía	2	N	N
El dispositivo de alarma informa del emplazamiento del fuego a los responsables	2	N	S
Instalar extintores portátiles para incendios de origen eléctrico	2	N	S
Colocar extintores portátiles estratégica y perfectamente señalizados	2	N	S
Utilizar agua u otros agentes de extinción para los incendios no eléctricos	2	N	S
Instalar mecanismos de interrupción automát. de fuentes de energía en incendio	2	N	N
Instalar mecanismos de interrupción automática del aire acondic. en incendio	2	N	N
Instalar mecanismos de cierre automát. de conductos de aire en caso de incendio	2	N	N
Implantar sellado automático de las puertas contra incendios	2	N	N
Implantar procedimientos para rearmar cualquier equipo contra incendios	2	N	S
Facilitar acceso al edificio para personal y equipamiento contra incendio	2	N	S
Facilitar máscaras antigás para el personal de emergencia	2	N	S
Instalar líneas y filtros de los conductos no combustibles	2	N	N
Proteger sistema de refrigeración contra incendios	2	N	N
Reducir al mínimo la existencia de materiales inflamables	2	N	S
Las paredes del área de seguridad deben estar construidas de aluminio	2	N	N
Colocar papeleras de metal	2	N	S
Hacer pública de forma notoria la localización de extintores	2	N	S
Nombrar encargados de la utilización de las medidas antincendio	2	N	S
Almacenar copias en armarios ignífugos	2	N	S
Almacenar los duplicados en armarios ignífugos	2	N	S

Limitar el alcance del ataque lógico

Otorgar prioridad de evacuación a todos los discos y cintas con ficheros críticos	8	S	S
Almacenar los ficheros de acuerdo con su prioridad de evacuación	8	N	S
Establecer rangos de tiempos de ejecución	8	N	S
Comprobar que los tiempos de ejecución se corresponden con los rangos	8	N	S
Comprobar que el tiempo de utilización se corresponde con el tiempo asignado	8	N	S
Comprobar aleatoriamente los resultados	8	N	S
Mantener inventario contabilizado de los soportes magnéticos	8	N	S
Realizar inventario anual de los documentos	8	N	S

Implantar procedimiento de control visual de informes de actividad de	8	N	S
Establecer medidas periódicas del rendimiento del sistema	12	N	S
Implantar sistema de registro de eventos en cadenas estratégicas	8	N	S
Implantar sistema de vigilancia de las cadenas estratégicas	8	N	S

6.5.- ACTIVIDAD 2: SELECCIÓN DE MECANISMOS DE SALVAGUARDA

Esta Actividad permite identificar y seleccionar los mecanismos a implantar, considerando las restricciones detectadas e incorporadas en la tarea anterior. Los mecanismos identificados y seleccionados provisionalmente se estudian en cuanto a su efectividad reductora del riesgo.

Esta Actividad es iterativa, pues se repite tantas veces como sea necesario hasta obtener el conjunto de mecanismos a implantar definitivamente.

Tarea 1: Identificar mecanismos a implantar

Se identificaron todos los mecanismos a implantar en la Actividad 1

Tarea 2: Evaluar el riesgo con los mecanismos elegidos

• Evaluación de la EFEctividad simulada(EFS) de las funciones de salvaguarda FNCi, considerando los mecanismos MECi simulados EFS = Σ (CMi * IMSi).

Grado de Implementación del Mecanismo de la Simulación (1 si el mecanismo ha sido seleccionado para la simulación, 0 si no lo ha sido)

Función : Control de Acceso Físico

EFS = (0.03*1)*21 = 0.63

Función : Control de acceso lógico

EFS = (0.02*1) * 36 + (0.10*1) = 0.82

Función : Procedimientos físicos

EFS = (0.02*1) * 27+ (0.24*1) = 0.78

Función : Limitar el alcance de incidentes personales

EFS = (0.07*1) * 12 + (0.09*1) = 0.93

Función : Formación

EFS = (0.09*1) * 10 = 0.90

Función : Limitar el alcance de ataque físico

EFS = (0.01*1) * 26 + (0.07*1) = 0.33

Función : Procedimientos Lógicos

EFS = (0.02*1) * 16 + (0.03*1) * 19 = 0.89

Función : Limitar el alcance del ataque lógico

EFS = (0.08*1)+ (0.08*1)= 0.16

Función : Limitar el alcance de los errores

EFS = (0.02*1) * 3 + (0.01*1) * 2 + (0.03*1) * 28 = 0.92

Función : Limitar el alcance de las averías

EFS = (0.3*1)= 0.3

Función : Prevenir averías

EFS = (0.03*1) * 28 + (0.05*1) * 2 = 0.94

Función : Limitar el alcance de un corte eléctrico

EFS = (0.03*1) * 4 + (0.34*1)+(0.01*1) = 0.47

Función : Prevenir errores

EFS = (0.01*1) * 97 = 0.97

Función : Prevenir Incendios

EFS = (0.05*1) * 16 = 0.80

Función : Limitar el alcance del incendio

EFS = (0.02*1) * 27 + (0.08*1) = 0.62

EFECTIVIDAD SIMULADA

FUNCION	**EFECTIVIDAD MECANISMOS SIMULADOS(EFS)%**
Control de Acceso Físico	63
Control de Acceso Lógico	82

Procedimientos Físicos	78
Procedimientos Lógicos	89
Prevenir Averías	94
Limitar el Alcance de Incidentes Personales	93
Limitar el Alcance de Ataque Físico	33
Limitar el Alcance de Ataque Lógico	16
Limitar el Alcance de Errores	92
Limitar el Alcance de Averías	30
Formación	90
Limitar el Alcance de un Corte Eléctrico	47
Limitar el Alcance de un Incendio	62
Prevenir Incendios	80
Copias de Seguridad	82
Prevenir Errores	97

• Reevaluación de las disminuciones de vulnerabilidad DV y del impacto DI al aplicar la efectividad de las funciones de salvaguarda considerando los mecanismos simulados.

La mayor disminución de vulnerabilidad y la mayor disminución del impacto conseguido para las amenazas corresponden a la aplicación de las funciones.
Por lo tanto la amenaza queda:

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

Disminución del impacto por mecanismos simulados(DIS)	**Disminución de la vulnerabilidad por mecanismos simulados (DVS)**
46%	60%

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

Disminución del impacto por mecanismos simulados (DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
22%	70%

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

Disminución del impacto por mecanismos simulados(DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
69%	67%

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

Disminución del impacto por mecanismos simulados (DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
35%	0%

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

Disminución del impacto por mecanismos simulados(DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
0%	58%

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

Disminución del impacto por mecanismos simulados(DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
69%	72%

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

Disminución del impacto por mecanismos simulados(DIS)	**Disminución de la vulnerabilidad por mecanismos simulados (DVS)**
0%	72%

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

Disminución del impacto por mecanismos simulados(DIS)	**Disminución de la vulnerabilidad por mecanismos simulados (DVS)**
0%	66%

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

Disminución del impacto por mecanismos simulados(DIS)	**Disminución de la vulnerabilidad por mecanismos simulados (DVS)**
0%	47%

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

Disminución del impacto por mecanismos simulados(DIS)	**Disminución de la vulnerabilidad por mecanismos simulados (DVS)**
61%	61%

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

Disminución del impacto por	**Disminución de la vulnerabilidad por**

mecanismos simulados(DIS)	mecanismos simulados (DVS)
12%	61%

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

Disminución del impacto por mecanismos simulados(DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
24%	47%

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

Disminución del impacto por mecanismos simulados(DIS)	Disminución de la vulnerabilidad por mecanismos simulados (DVS)
24%	0%

Aplicando las disminuciones en el cálculo del riesgo efectivo:

- Vulnerabilidad disminuida(VD) = Vulnerabilidad * (1 - DVS)
- Impacto disminuido(ID) = Impacto * (1 - DIS)
- Riesgo efectivo(RS) = Vulnerabilidad disminuida * Impacto disminuido

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

ACTIVOS	V %	IMP	VD %	ID	RS
DEPARTAMENTO	0.2	40158	0.08	21685	17
RED LOCAL Y COMUNICACIONES	0.2	9096	0.08	4912	4
MEDIOS DE ALMACENAMIENTO	0.2	2289	0.08	1236	1
SERVIDOR CENTRAL	0.2	7030	0.08	3796	3
EQUIPO INFORMATICO	0.2	9678	0.08	5226	4

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

ACTIVOS	V %	IMP	VD %	ID	RS
SERVIDOR CENTRAL	0.02	3700	0.01	2886	0
RED LOCAL Y COMUNICACIONES	0.02	2394	0.01	1867	0
EQUIPO INFORMATICO	0.02	5093	0.01	3972	0

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

ACTIVOS	V %	IMP	VD %	ID	RS
OPERADORES	2	15314	0.65	4747	31
DEPARTAMENTO	2	40158	0.65	12448	80

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

ACTIVOS	V %	IMP	VD %	ID	RS
SERVIDOR CENTRAL	2	3700	2	2405	48
RED LOCAL Y COMUNICACIONES	2	2394	2	1556	31
EQUIPO INFORMATICO	2	5093	2	3290	66

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

ACTIVOS	V %	IMP	VD %	ID	RS
SERVIDOR CENTRAL	0.2	1850	0.08	1850	2
RED LOCAL Y COMUNICACIONES	0.2	2394	0.08	2394	2
EQUIPO INFORMATICO	0.2	2547	0.08	2547	2

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

ACTIVOS	V %	IMP	VD %	ID	RS
APLICACIONES	20	2992	5.6	927	52
SOFTWARE BASE	20	6122	5.6	1897	105

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

ACTIVOS	V %	IMP	VD %	ID	RS
APLICACIONES	0.2	1496	0.056	1496	1

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

ACTIVOS	V %	IMP	VD %	ID	RS
APLICACIONES	20	1496	6.8	1496	100

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

ACTIVOS	V %	IMP	VD %	ID	RS
SERVIDOR CENTRAL	0.2	3700	0.1	3700	4
MEDIOS DE ALMACENAMIENTO	0.2	602	0.1	602	1
RED LOCAL Y COMUNICACIONES	0.2	2394	0.1	2394	3
EQUIPO INFORMATICO	0.2	5093	0.1	5093	5

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

ACTIVOS	V %	IMP	VD %	ID	RS
PROCESOS PERSONAL Y LOGISTICA	0.2	46	0.078	17	0
DISPONIBILIDAD DE LA INFORMACION	0.2	600	0.078	234	0
PROCESOS FINANCIEROS	0.2	1008	0.078	393	0

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

ACTIVOS	V %	IMP	VD %	ID	RS
PROCESOS PERSONAL Y LOGISTICA	0.2	92	0.078	80	0
DISPONIBILIDAD DE LA INFORMACION	0.2	1200	0.078	1056	1
PROCESOS FINANCIEROS	0.2	2017	0.078	1774	1

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

ACTIVOS	V %	IMP	VD %	ID	RS
SERVIDOR CENTRAL	0.2	3700	0.1	2812	3
RED LOCAL Y COMUNICCIONES	0.2	2394	0.1	1819	2
EQUIPO INFORMATICO	0.2	5093	0.1	3870	4

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

ACTIVOS	V %	IMP	VD %	ID	RS
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICO	0.2	95	0.2	72	0
MANIPULACIÓN Y CONTROL DE LA RED	0.2	1140	0.2	866	2
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS	0.2	1932	0.2	1468	3

6.6.- ACTIVIDAD 3: ESPECIFICACIÓN DE LOS MECANISMOS A IMPLANTAR

Tarea única: Especificar los mecanismos a implantar

Los siguientes son los mecanismos a implantar como Plan de Contingencia

Los costos se los colocan de acuerdo a estos parámetros.

1000 = muy alto

300 = alto

100 = media

30 = bajo

0 = nulo

Prevenir incendios

Mecanismo	Costos
Aislar las áreas de seguridad de lugares con riesgo de fuego (cafeterías, productos químicos, basura, etc.)	30
Almacenar el papel y otros soportes lejos de áreas de seguridad	0
No albergar productos de limpieza inflamables o cáusticos en arreas de seguridad	0
Guardar productos inflamables (sí se permiten), en contenedores seguros	0
Limpiar regularmente el subsuelo	30
No colocar percheros en el interior de áreas de seguridad	0
Mantener los medios destructores de papel alejados de áreas de seguridad	0
No almacenar piezas de plástico en el interior de áreas de seguridad	0
No decorar áreas de seguridad con posters, ni carteles	0
Prohibir fumar en áreas de seguridad y en la biblioteca de medios	0

Realizar inspecciones periódicas por parte del cuerpo de bomberos	30
Instalar equipos de detección de humos y fuentes de calor	300
Situar áreas de seguridad alejadas de zonas con alto potencial de incendios	300
Situar áreas de seguridad alejadas de zonas de bosque denso	300
No acumular basura en el área de seguridad	0
Realizar el vaciado de las papeleras fuera del área de seguridad	0
TOTAL	**990**

Limitar el alcance del incendio

Mecanismo	Costos
Instalar materiales no combustibles y resistentes al fuego en arreas criticas	300
Construir subsuelo sólido de hormigón, no combustible	300
Canalizar el cableado subterráneo a través de conductos	100
Canalizar a través de conductos los cables que conectan el alumbrado del techo	100
Instalar mobiliario y elementos de decoración no combustibles	100
Colocar todos los muebles de metal	100
Separar la biblioteca de cintas de las cajas fuertes de datos	0
Mantener actualizados regularmente los procedimientos contra incendios	30
Disponer de un equipamiento adecuado de lucha contra incendios	300
Asignar responsabilidades individuales en caso de incendio	0
Probar regularmente el sistema de detección de incendios	0
Realizar pruebas frecuentes con el sistema de alarma antiincendios	0
Instalar equipos de detección de humos y fuentes de calor	300
Colocar detectores de humo que funcionen correctamente en áreas de seguridad	300
Probar el equipo detección de humos sobre unas bases programadas	30
Detectar el dispositivo de alarma informa del emplazamiento del fuego a los responsables	100
Instalar extintores portátiles para incendios de origen eléctrico	300
Colocar extintores portátiles estratégica y perfectamente señalizados	30
Utilizar agua u otros agentes de extinción para los incendios no eléctricos	30
Implantar procedimientos para rearmar cualquier equipo contra incendios	100
Facilitar acceso al edificio para personal y equipamiento contra incendio	0
Facilitar máscaras antigás para el personal de emergencia	100
Reducir al mínimo la existencia de materiales inflamables	0
Colocar papeleras de metal	30
Hacer pública de forma notoria la localización de extintores	30
Nombrar encargados de la utilización de las medidas antincendio	0

Almacenar copias en armarios ignífugos	100
Almacenar los duplicados en armarios ignífugos	100
TOTAL	**2880**

Prevenir averías

Mecanismo	**Costos**
Instalar conexiones eléctricas con toma de tierra	30
Limpiar regularmente la zona que se encuentra debajo del falso suelo	30
Realizar chequeos periódicos por parte del personal de seguridad	0
Comprobar el estado del cableado que se encuentra bajo el falso suelo	0
Situar áreas de seguridad alejadas de autopistas con tráfico denso	300
Situar áreas de seguridad alejadas de vías de tren	300
Situar áreas de seguridad alejadas de aeropuertos	300
Prohibir la introducción de comida y bebida en el área de seguridad	0
Limpiar regularmente la superficie del equipamiento ubicado en el área de seguridad	0
Limpiar los suelos regularmente	0
Prohibir comer en el área de seguridad	0
Conservar limpias y ordenadas las zonas de mantenimiento	0
Limpiar debajo del falso suelo del área de seguridad	30
Establecer un procedimiento riguroso de limpieza	0
Planificar actividades de mantenimiento de los equipos	0
Comprobar la realización del mantenimiento de los equipos	0
Realizar mantenimiento de las unidades de almacenamiento	30
Examinar el funcionamiento de los equipos trimestralmente	0
Establecer un programa de mantenimiento regular	0
Asegurar acuerdos con proveedores para servicios de limpieza	0
Comprobar periódicamente el equipo de comunicaciones	0
Realizar seguimiento de los procedimientos para la conservación y restauración	0
Contratar mantenimiento de todos los elementos, con periodo de reemplazamiento	300
Fijar por contrato la duración de la intervención en el mantenimiento	0
Fijar en contrato de mantenimiento cláusulas en caso de incumplimiento	0
Establecer mantenimiento periódico fijado	300
Establecer garantía en las piezas reemplazadas	30
Limitar por contrato las responsabilidades en implantación, desplazamiento,...	0
Realizar contrato de mantenimiento de las aplicaciones	0
Establecer por contrato la disposición de nuevas versiones y/o correcciones	0

TOTAL	**1650**

Limitar el alcance de las averías

Mecanismo	Costos
Registrar las características de los equipos	30
TOTAL	**30**

Limitar el alcance de los incidentes con personal

Mecanismo	Costos
Simular situaciones de desastre para ejercitar el plan de evacuación	0
Revisar y mantener disponibles los planes de evacuación	0
Liberar todas las puertas internas y pasillos de toda obstrucción	0
Colocar el equipamiento de tal manera que no obstruyan la apertura de puertas	0
Disponer de un botiquín o servicio médico próximo al área de seguridad	100
Hacer pública de forma notoria los planes de evacuación	30
Hacer pública de forma notoria los botiquines de primeros auxilios	30
Hacer pública de forma notoria las rutas y salidas de emergencia	30
Situar equipo de primeros auxilios fácilmente accesible	0
Nombrar encargados de supervisar las medidas de evacuación	0
Nombrar encargados de avisar a los servicios (ambulancias, bomberos, etc.)	0
Nombrar encargados de cortar la corriente eléctrica	0
TOTAL	**190**

Formación

Mecanismo	Costos
Formar regularmente al personal en las técnicas de lucha contra el fuego	30
Formar al personal para actuar en caso de amenaza de bomba	30
Formar ante emergencias y evacuación	30
Realizar sesiones de orientación sobre procedimientos de emergencia	30
Realizar prácticas en temas de seguridad	30
Comprobar la formación en temas de seguridad	30
Asegurar el conocimiento de las normas de emergencia	30
Comprobar periódicamente el conocimiento de las normas de emergencia	30

Incluir el conocimiento de las normas de emergencia en el plan de formación	30
Formar al personal en primeros auxilios	30
TOTAL	**300**

Limitar el alcance de un corte eléctrico

Mecanismo	Costos
Proveer de mecanismos manuales a los sistemas automáticos	30
Contar con fuentes de energía secundarias y generadores permanentes	300
Proporcionar al personal de mantenimiento y seguridad una copia del cableado	30
Proporcionar una copia del trazado de la iluminación al depart. de mantenimiento	30
Disponer de linternas de pila seca en el área de seguridad para uso de emergencia	30
Establecer procesos manuales durante el periodo de recuperación	30
TOTAL	**450**

Prevenir errores

Mecanismo	Costos
Realizar pruebas a nuevos empleados: seguridad, sicológicas, referencias, aptitud	30
Existencia de responsables alertas respecto a empleados disgustados	0
Detectar insatisfacciones	0
Detectar posibles problemas familiares	0
Hacer pública una política de personal severa ante las infracciones	0
Conocer los responsables profundamente a sus subordinados	0
Nombrar encargado de la revisión de las normas con suficiente autoridad	0
Exigir responsable presente cuando se realizan mantenimientos	0
Mantener lista de personal externo para el servicio de mantenimiento	0
Supervisar las actividades del personal externo	0
Comprobar periódicamente las utilidades del software de seguridad	0
Documentar las modificaciones de las aplicaciones	30
Controlar las modificaciones de las aplicaciones	0
Controlar los cambios en las aplicaciones	0
Registrar los cambios en las aplicaciones	30
Asegurar que la documentación cumple los estándares de operación	0
Implantar estándar de documentación para diagramas de flujo y modelos lógicos	30
Implantar estándar de documentación para listados	30

Implantar estándar de documentación para formatos de entrada y de salida	30
Implantar estándar de documentación para ejemplos	30
Implantar estándar de documentación para usuario	30
Implantar estándar de documentación para pruebas	30
Implantar estándar de documentación para explicación de códigos, tablas, etc.	30
Implantar estándar de documentación para mensajes de error	30
Implantar estándar de documentación para descripción de ficheros	30
Implantar estándar de documentación para explotación	30
Realizar cambios coordinados en aplicaciones y en documentación	0
Revisar cambios en la documentación por un auditor interno	100
Participar propietarios de la información en su clasificación	0
Implantar procedimientos de identificación de la documentación	0
Implantar procedimientos de clasificación de la documentación	0
Asegurar coordinación entre departamentos para la auditoría	0
Asegurar que la información de salida cumple los estándares	0
Implantar control de calidad	100
Asegurar el control de las modificaciones en las aplicaciones	0
Asegurar control de las conversiones	0
Separar responsabilidades	0
Asegurar que los sistemas son auditables	30
Llevar a cabo auditorías e inspecciones sorpresa	30
Determinar la legalidad del equipamiento, datos y servicios utilizados	100
Disponer de mensajeros eficientes y fiables	30
Utilizar software de base experimentado	1000
Probar las alternativas con cargas simuladas	0
Ser miembro de alguna asociación de usuarios	0
Participar regularmente en las reuniones de las asociaciones de usuarios	0
Instalar equipo de comunicaciones en un área de seguridad	100
Seleccionar la red por un estudio comparativo	100
Generar informe escrito con las modificaciones estructurales	30
Visar la utilización por el jefe de explota., responsable de operaciones,... r	0
Nombrar responsable de la gestión de los soportes	0
Reducir la intervención manual	0
Realizar auditoría no programada de procedimientos de utilización de soportes	30
Tener en consideración en el estudio, el entorno, las pruebas y los desarrollos	0
Actualizar el plan de copias de seguridad ante modificaciones en las aplicac.	30
Almacenar y actualizar los informes de actividad	100
Analizar y almacenar el informe de actividad del operador	100
Utilizar el informe de cargas y rendimiento para ampliaciones	0
Nombrar encargados de la preparación y planificación de los trabajos	0

Realizar preparación y planificación sistemática de todos los trabajos	100
Realizar planificación diaria, semanal, mensual y anual	30
Utilizar sistema de preparación y planificación automática	30
Implantar procedimientos escritos para la ejecución de pruebas	30
Documentar completamente las aplicaciones o mantenimiento. al pasar a explotación	100
Recopilar las aplicaciones en el entorno de explotación	100
No realizar personal de explotación modificaciones de procedimientos, aplicac.	0
Realizar documentación de explotación completa de cada aplicación	30
Realizar actualización sistemática de la documentación de explotación	100
Implantar documentación de explotación jerarquizada por función	0
realizar documentación actualizada de los elementos instalados	30
realizar seguimiento y control de las versiones	0
realizar actualización de la documentación de las aplicaciones	30
Considerar en procedimientos docum. firmado por usuario y desarrollador	0
asegurar procedimiento de revisión forma parte de documentación de aplicación	30
asegurar que los mantenimientos se realizan a partir de un documento formalizado	0
asegurar que los mantenimientos de realizan solo en el entorno de desarrollo	0
Asegurar que jefe de explot. Remite a desar.y usuarios un doc. Con pases a exp.	30
implantar protocolo para comparar versiones de modificaciones importantes	100
asegurar que las nuevas aplicaciones generan una documentación de	0
implantar procedimiento para definir el juego de pruebas	100
asegurar proyecto iniciado con un estudio previo y un cuaderno de carga	0
asegurar cuaderno de carga respaldado por los usuarios y desarrolladores	0
asegurar planificación de todos los proyectos en desarrollo	0
aplicar una metodología para el análisis funcional	100
asegurar que metodología de desarrollo permite integrar metodología de seguridad	0
Asegurar metodología permite definir clasificación de datos con aspectos de seg.	0
deducir especificaciones de seguridad por la clasificación de datos y procesos	30
asegurar clasificación de los procedimientos de seguridad	0
implantar método de programación estructurada, con reglas de utilización	100
asegurar para los desarrollos externos se estipula la metodología de	0

desarrollo	
Realizar prototipo de las especificaciones antes de generar el análisis deta.	100
utilizar generador de programas, pantallas e informes	100
utilizar un diccionario de datos o repositorio	100
Asegurar que el dicc. De datos permite clasif. de seg. en las descripciones	0
Asegurar documentación de la aplicación actualizada y acorde con la metodología	0
Asegurar que la documentación incluye los esquemas de integración	0
Asegurar que la doc. incluye los esquemas de circulación de la información	0
Asegurar que la documentación incluye las referencias cruzadas	0
Obtener información sobre el proveedor del software	0
TOTAL	**3640**

Limitar el alcance de los errores

Mecanismo	**Costos**
Realizar los cambios en las copias, nunca en los originales	0
Obtener informe de errores y procedimientos de seguimiento	30
Probar todas las opciones de las aplicaciones	0
Monitorizar y controlar la depuración de los programas de seguridad	100
Comprobar la satisfacción de los usuarios	0
Utilizar vistas o bases de datos espejo	100
Analizar a diario de las operaciones de explotación	300
Verificar con periodicidad aleatoria del contenido de los procedimientos	0
Implantar procedimiento para detección de anomalías en software y en información	100
Mantener registro actualizado y completo de las intervenciones de proveedores	30
Implantar procedimientos de revisión en aplicaciones (creación o manten.)	100
Implantar procedimiento de revisión general antes de pasar a explotación	30
Asegurar que los desarrollos externos pasan un periodo de prueba	0
Asegurar que el procedimiento de revisión incluye los estudio iniciales	0
Asegurar que el procedimiento de revisión incluye los juegos de pruebas	0
Asegurar que el procedimiento de revisión incluye los mecanismos de seguridad	0
Asegurar que procedimiento de revisión incluye la documentación de explotación	0

Asegurar que procedimiento de revisión incluye el régimen de copias de seguridad	0
Asegurar que procedimiento de revisión incluye funcionamiento en modo degradado	0
Asegurar que el procedimiento de revisión incluye los estimadores técnicos	0
Asegurar que procedimiento de revisión cumple los estándares de la metodología	0
Asegurar que el procedimiento para pruebas cumple la metodología	0
Asegurar juegos de pruebas exhaustivos	0
Asegurar juegos de pruebas definidos por los usuarios	0
Asegurar procedimiento de pruebas incluye la revisión anual de los proc. en exp.	0
Asegurar control y actualización periódica (semanal) de la planificación	0
Nombrar responsable de calidad de trabajos respecto a normas de análisis/prog.	0
Verificar que los controles asociados a los datos se reproducen en todos prog.	0
Centralizar los incidentes detectados por usuarios y no controlados	100
Realizar auditoría periódica de la validez de los controles	30
Realizar verificación aleatoria de los controles con datos de prueba	0
Realizar actualización de datos estratégicos realizada en diferido	100
Realizar pruebas del software externo	0
Disponer de los fuentes de las aplicaciones externas	300
TOTAL	**1320**

Control de acceso físico

Mecanismo	**Costos**
Utilizar tarjetas identificativas personalizadas	30
Disponer de las fotos de todos los empleados con acceso	30
Permitir el acceso solamente a aquellas personas debidamente identificadas	0
No permitir acceso a acompañantes de las personas identificadas	0
Verificar la identidad de todo el personal que accede al edificio	0
Colocar rejas en las ventanas exteriores que están al nivel de la calle	30
Cerrar las puertas del área de seguridad en periodos de inactividad	0
Establecer un procedimiento de control de visitantes	0
Registrar las entradas y salidas de los visitantes	0
Acompañar las visitas por personal del centro	0
No permitir el acceso de las visitas a zonas estrictamente confidenciales	0
Establecer controles físicos (tarjetas, torniquetes, etc.) al área de seguridad	30
Controlar todos los accesos por un guardia de seguridad o personal	0

Reducir el número de accesos al área de seguridad	0
Establecer controles periódicos de seguridad para todo el personal	30
No poner ventanas ni paredes exteriores que permitan el paso a saboteadores	100
Establecer un sistema de control de firmas para controlar el acceso	300
No establecer indicadores sobre la ubicación del área de seguridad	0
Comprobar los requisitos de acceso y emplazamiento de los equipos locales	30
Comprobar periódicamente la rigidez del sistema de control de accesos	0
Asegurar encargados presentes durante la intervención	0
Identificar al personal externo	0
Implantar acceso a los terminales restringidos por cerradura	30
TOTAL	**610**

Procedimientos físicos

Mecanismo	**Costos**
aislar el área de seguridad de zonas donde se realicen procesos peligrosos	30
asegurar las estanterías de cintas y demás equipamiento	0
planificar el transporte de ficheros para casos de emergencia	30
contratar vigilantes nocturnos permanentes	30
instalar voltaje suficiente para soportar el equipo a pleno rendimiento	300
situar cuadro de mandos principal en lugar alejado y de acceso restringido	0
asegurar que todos los circuitos están reforzados	0
asegurar que todos los circuitos tienen su correspondiente toma de tierra	0
Situar áreas de seguridad alejadas de líneas de alto voltaje	300
situar áreas de seguridad alejadas de zonas con alto porcentaje de crimen	300
situar áreas de seguridad alejadas de zonas almacenamiento de productos peligrosos	300
no permitir la introducción de ningún objeto en el área de seguridad	0
detectar conflictos entre empleados	0
realizar inspección periódica para identificar mejoras en normas de seguridad	30
no posibilitar a empleados acceso a las herramientas (destornilladores, etc.)	0
asegurar coordinación entre departamentos para la gestión de la información	0
asegurar coordinación entre departamentos para el reclutamiento de personal	0
Controlar registro de las actividades que se realicen contra la	0

información	
Llevar a cabo controles de seguridad en la instalación	0
Crear un área de trabajo del cliente segura	100
Establecer procedimientos adecuados de control y operación	0
Registrar las comunicaciones realizadas	30
Nombrar administrador responsable de los datos	0
Nombrar administrador de la instalación, modificación y superv.estruc.ficheros	0
Implantar procedimientos escritos para el archivado y desarchivado	0
Ubicar archivos/librerías en áreas de seguridad	0
Implantar procedimiento de utilización de contenedores en caso de transporte	0
Situar las zonas con ficheros en lugar estrictamente protegidos	300
Controlar la utilización del sistema de información	0
Implantar procedimientos para la prevención y protección (firmas)	100
Implantar procedimientos para aprovisionamiento, almacenamiento y gestión de Información	30
TOTAL	**1880**

Control de acceso lógico

Mecanismo	**Costos**
Bloquear acceso a ficheros de contraseñas	100
Comprobar periódicamente las listas de control de acceso	0
Implantar sistemas de contraseñas	300
Implantar contraseñas difíciles de adivinar	0
Utilizar sistemas operativos con utilidades incorporadas para control de acceso	300
Restringir el acceso a las utilidades del sistema	30
Proteger las contraseñas a prueba de modificaciones	30
Implantar intervalo de cambio de contraseñas adecuado	100
Combinar contraseñas con llaves físicas	100
Asegurar que software del sistema permite control de los privilegios	0
Asegurar sistema de control de acceso compatible con otras aplicaciones	0
Implantar sistema de control de accesos fácil de gestionar	300
Proporcionar los propietarios de la información los derechos de acceso	0
Actualizar continuamente la lista de derechos de acceso ante cualquier cambio	30
Asegurar sistema de identificación actualizado de cada usuario	0
Asegurar sistema de autenticación de cada usuario (contraseña, llave, ..)	0
Asegurar contraseñas con un mínimo de 5 caracteres de longitud	0
Asegurar contraseñas sin eco en pantalla	0
Asegurar solo el usuario define la contraseña	0

Asegurar que contraseña proporcionada por el sistema tiene una validez temporal	0
Asegurar que las contraseñas no se pueden reutilizar	0
Asegurar control periódico aleatorio de cuentas estratégicas	0
Almacenar las contraseñas de forma cifrada, con algoritmo irreversible	0
Proporcionar información a los usuarios de las normas respecto a las contraseñas	0
Implantar procedimiento de difusión, conservación y utilización de contraseñas	0
Asegurar desconexión en caso de un periodo de inactividad	0
Asegurar bloqueo del terminal en el caso de tres intentos infructuosos	0
Asegurar desbloqueo de terminales con intervención del administrador	0
Asegurar autorización de acceso con un plan horario y según un calendario	0
Realizar registro y seguimiento de los intentos infructuosos	30
Utilizar los procedimientos de identificación del tipo de acceso	0
Utilizar el procedimiento de control de la identidad	0
Repudiar las conexiones donde no se establece la identificación del terminal	100
Asegurar que el control de acceso funciona con lenguajes de selección	100
Implantar utilidades y herrami. del sistema con acceso restringido y controlado	100
Asegurar acceso restringido a las listas de acceso y de privilegios	0
Asegurar el sistema de control de acceso permita una carga progresiva	0
Implantar procedimientos complementarios de autenticación en los procesos	100
Implantar control de acceso a las tablas limitando visibilidad y acceso	100
TOTAL	**1820**

Copias de seguridad

Mecanismo	**Costos**
Almacenar las copias de seguridad en un lugar alejado de áreas de seguridad	0
Guardar las copias de seguridad de los ficheros críticos en lugares alejados	0
Situar los duplicados en una área de seguridad diferente a la de los originales	30
Realizar inventario de las copias de seguridad	30
Comprobar las copias de seguridad	0

Realizar copias de seguridad frecuentes	0
Realizar duplicados de la documentación	30
Almacenar los duplicados en edificios separados de los originales	30
Revisar periódicamente los duplicados	0
Coordinar los procedimientos de copia de seguridad con la duplicación de la doc.	0
Guardar una copia del sistema en un lugar seguro	30
Revisar y probar las copias periódicamente	0
Establecer los pasos para duplicar ficheros, programas, software, etc.	0
Almacenar todas las copias de la documentación en un lugar seguro	0
Realizar estudio de cada elemento a incluir en la copia de seguridad	0
Implantar procedimiento de copias de seguridad	30
Realizar verificación periódica de las copias de seguridad	0
Asegurar contenido de las copias de seguridad cifrado	0
Almacenar copias de seguridad en áreas de seguridad distintas a originales	300
Asegurar que el almacenamiento de copias de seguridad se realiza puntualmente	0
Realizar reserva de seguridad de soportes en otro edificio	100
Realizar copias de seguridad de las aplicaciones en desarrollo	30
Duplicarlos ficheros de back up	30
Realizar duplicados documentos desarrollo en área de seguridad distinta a la original	30
Comprobar ejecuciones de aplicaciones en explotación con las copias	0
Realizar reserva de seguridad de los elementos no importantes	30
TOTAL	**830**

Procedimientos lógicos

Mecanismo	**Costo**
Nombrar encargados de los ficheros críticos	0
Verificar periodos de inactividad	0
Comprobar la ejecución de procesos en la lista de explotación	0
Ordenar los soportes	0
Mantener los soportes no utilizados en sus contenedores	0
Situar las aplicaciones, sistemas y documentación en un área de seguridad	30
Implantar procedimiento de identificación y firma para la obtención de copias	30
Establecer niveles en la clasificación de seguridad	0
Crear un política de clasificación	0
Clasificar los elementos según su criticidad	0
Informar al personal de los requisitos legales asociados a la información	0
Nombrar un administrador de la seguridad	0

Asegurar el apoyo de la dirección	0
Asegurar existencia de una política de seguridad	0
Asegurar coordinación entre departamentos para planificación de servicios	0
Asegurar coordinación entre departamentos para el plan de seguridad	0
Establecer funciones de control separadas de las de organización	100
Implantar una filosofía general de la auditoría de control	0
Controlar la información de entrada para asegurar su completitud	0
Controlar las aplicaciones no salen a la línea de comandos del sistema operativo	0
Verificar el uso de los procedimientos de seguridad	0
Verificar la protección de los programas y los datos	0
Nombrar un responsable que será el interlocutor de la organización	0
Asegurar software de red estándar, fiable y con mantenimiento	1000
Asegurar protocolos normalizados con funciones de protección integradas	300
Realizar registro de la utilización de soportes	30
Verificar regularmente los soportes	0
Implantar procedimiento de justificación para cada lote de inform. a transferir	0
Realizar estudio de carga y rendimiento anterior a la instalación aplicaciones	100
Implantar procedimientos de explotación catalogados y con acceso restringido	100
Almacenar documentación de explotación en un área de seguridad	30
Descontaminar los soportes provenientes del exterior en equipos aislados	30
Nombrar encargado de mantenimiento a primer nivel de elementos no importantes	0
Utilizar aplicaciones estándar de versiones oficiales, mantenidas y documentadas	1000
Controlar autenticación del origen e integridad del contenido de ampliaciones	0
Realizar las transacciones estratégicas solo desde terminales controlados	100
TOTAL	**2850**

Limitar el alcance del ataque lógico

Mecanismo	*Costo*
Otorgar prioridad de evacuación a todos los discos y cintas con ficheros críticos	0
Almacenar los ficheros de acuerdo con su prioridad de evacuación	0
Establecer rangos de tiempos de ejecución	100

Comprobar que los tiempos de ejecución se corresponden con los rangos	0
Comprobar que el tiempo de utilización se corresponde con el tiempo asignado	0
Comprobar aleatoriamente los resultados	0
Mantener inventario contabilizado de los soportes magnéticos	30
Realizar inventario anual de los documentos	30
Implantar procedimiento de control visual de informes de actividad de	300
Establecer medidas periódicas del rendimiento del sistema	30
Implantar sistema de registro de eventos en cadenas estratégicas	300
Implantar sistema de vigilancia de las cadenas estratégicas	300
TOTAL	**1390**

Limitar el alcance del ataque físico

Mecanismo	**Costos**
Almacenar sólo los soportes imprescindibles (cintas, discos) en áreas de seguridad	0
Colocar estratégicamente varios sistemas manuales de alarma	100
Facilitar acceso a las instalaciones para los equipos de emergencia	0
Facilitar acceso sin demora por parte del equipo de emergencia	0
Proveer mapa con la localización de los dispositivos de alarma	30
Disponer de megáfono de emergencia	30
Conocer todo el personal su emplazamiento y cómo funciona el megáfono	0
Disponer de accesos fáciles para el personal de emergencia y el equipamiento	0
Notificar al personal apropiado el advenimiento de un desastre	0
Establecer procedimientos para notificar a las autoridades civiles disturbios	0
Establecer revisiones generales periódicas de todo el área de seguridad	100
Registrar todos los cambios planeados y realizados en materia de seguridad	30
Establecer reuniones trimestrales del departamento para revisar procedimientos	0
Instruir al personal de operaciones y de seguridad en reacción ante disturbios	30
Exámenes periódicos: seguridad, rendimiento, aptitud	30
Hacer pública de forma notoria los números de teléfonos de emergencia	30
Hacer pública de forma notoria la asignación de responsables en emergencia	30
Nombrar sustitutos de los responsables en situaciones de emergencia	0

Nombrar encargados de apagar el equipo	0
Nombrar encargado de la revisión de las normas con suficiente autoridad	0
Monitorizar las operaciones	100
Marcar los elementos que deban ser evacuados	30
Revisar regularmente el cumplimiento de los procedimientos	30
Asegurar existencia de una lista de teléfonos de emergencia	0
Verificar las técnicas de prevención de desastres	0
Asegurar que los técnicos de mantenimiento del proveedor son los habituales	0
Seleccionar medios de almacenamiento alternativo	30
Instalar una caja fuerte de datos alejada de área de seguridad	100
Almacenar en lugar alejado soportes con informes y formularios críticos	0
Realizar inspecciones regulares de sistemas de protección y detección automática	0
Proveer a los equipos de detección de mecanismos de alarma automática	300
Apagar automáticamente el equipamiento crítico	300
Analizar el sistema de detección por parte de expertos	100
Establecer controles de inspecciones de cajas y paquetes enviados	0
Establecer políticas para monitorizar las amenazas	0
Instalar mecanismos de alerta que avisen de cualquier anomalía	300
Instalar sistemas de intercomunicación entre el área de seguridad y operación	100
Revisar las normas por parte del personal especializado	30
Nombrar encargado de una comprobación de seguridad semanal	0
Almacenar los elementos en un área de seguridad independiente	30
Revisar y controlar los sistemas de seguridad	0
Establecer acuerdos contractuales	0
Asegurar sistemas de protección elaborados	30
Asegurar análisis periódico de la calidad de las líneas	30
Asegurar seguimiento específico de los incidentes en cada línea	100
Generar informe escrito por cada intervención en l línea	100
Asegurar detección de intrusos después de las horas normales	30
Instalar sistema de alarmas en caso de extracción no autorizada	300
Utilizar herramientas de control y seguimiento del funcionamiento	1000
Considerar la documentación de explotación en acciones a realizarse	100
Mantener registro actualizado y completo de los incidentes	30
Asegurar edificios resistentes a terremotos	100
TOTAL	**3680**

6.7.- ACTIVIDAD 4: PLANIFICACIÓN DE LA IMPLANTACIÓN

Esta actividad no se contempla como objetivos de la implantación.
El responsable del Departamento Administrativo debe organizar la implantación de los mecanismos.

6.8 ACTIVIDAD 5: INTEGRACIÓN DE RESULTADOS

Esta última Actividad recopila los informes producidos en las diversas Etapas y Actividades del proyecto, para confeccionar el "**Informe final del Análisis y Gestión de Riesgos".**

Tarea única: Integrar los resultados

A11: ACCIDENTE FÍSICO DE ORIGEN INDUSTRIAL TIPO INCENDIO O EXPLOSIÓN.

ACTIVOS	**V** %	**IMP**	**RI**	**RE**	**RR**	**RS**
DEPARTAMENTO	0.2	40158	80	70	5	17
RED LOCAL Y COMUNICACIONES	0.2	9096	18	16	1	4
MEDIOS DE ALMACENAMIENTO	0.2	2289	5	4	0	1
SERVIDOR CENTRAL	0.2	7030	14	12	1	3
EQUIPO INFORMATICO	0.2	9678	19	17	1	4

A2: AVERÍA (DE ORIGEN FÍSICO O LÓGICO, DEBIDA A UN DEFECTO DE ORIGEN O SOBREVENIDA DURANTE EL FUNCIONAMIENTO DEL SISTEMA)

ACTIVOS	**V** **%**	**IMP**	**RI**	**RE**	**RR**	**RS**
SERVIDOR CENTRAL	0.02	3700	1	1	0	0
RED LOCAL Y COMUNICACIONES	0.02	2394	0	0	0	0
EQUIPO INFORMATICO	0.02	5093	1	1	0	0

A3: ACCIDENTE FÍSICO DE ORIGEN NATURAL (RIADA, FENÓMENO SÍSMICO O VOLCÁNICO, METEORO, RAYO, CORRIMIENTO DE TIERRAS, AVALANCHA, DERRUMBE, ...)

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
OPERADORES	2	15314	306	306	19	31
DEPARTAMENTO	2	40158	803	803	50	80

A4: INTERRUPCIÓN DE SERVICIOS O DE SUMINISTROS ESENCIALES ENERGÍA, AGUA, TELECOMUNICACIÓN, FLUIDOS Y SUMINISTROS DIVERSOS)

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
SERVIDOR CENTRAL	2	3700	74	63	18	48
RED LOCAL Y COMUNICACIONES	2	2394	48	41	12	31
EQUIPO INFORMATICO	2	5093	102	86	25	66

A5: ACCIDENTES MECÁNICOS O ELECTROMAGNÉTICOS (CHOQUE, CAÍDA, CUERPO EXTRAÑO, RADIACIÓN, ELECTROSTÁTICA ...)

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
SERVIDOR CENTRAL	0.2	1850	4	3	1	2
RED LOCAL Y COMUNICACIONES	0.2	2394	5	4	1	2
EQUIPO INFORMATICO	0.2	2547	5	4	1	2

E1: ERRORES DE UTILIZACIÓN OCURRIDOS DURANTE LA RECOGIDA Y TRANSMISIÓN DE DATOS O EN SU EXPLOTACIÓN POR EL SISTEMA.

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
APLICACIONES	20	2992	598	589	37	52
SOFTWARE BASE	20	6122	1224	1206	77	105

E2: ERRORES DE DISEÑO EXISTENTES DESDE LOS PROCESOS DE DESARROLLO DEL SOFTWARE (INCLUIDOS LOS ERRORES DE DIMENSIONAMIENTO CON POSIBLE SATURACIÓN):

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
APLICACIONES	0.2	1496	3	3	1	1

E4: INADECUACIÓN DE MONITORIZACIÓN, TRAZABILIDAD, REGISTRO DEL TRÁFICO DE LA INFORMACIÓN

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
APLICACIONES	20	1496	299	295	75	100

P1: ACCESO FÍSICO NO AUTORIZADO CON DESTRUCCIÓN O INUTILIZACIÓN DEL EQUIPO POR SUSTRACCIÓN (ROBO DE ÉSTE, DE SUS PIEZAS O DE SU INFRAESTRUCTURA)

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
SERVIDOR CENTRAL	0.2	3700	7	6	2	4
MEDIOS DE ALMACENAMIENTO	0.2	602	1	1	0	1
RED LOCAL Y COMUNICACIONES	0.2	2394	5	4	1	3
EQUIPO INFORMATICO	0.2	5093	10	9	3	5

P2: ACCESO LÓGICO NO AUTORIZADO CON INTERCEPCIÓN PASIVA SIMPLE DE LA INFORMACIÓN (REQUIERE SÓLO LECTURA)

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
PROCESOS PERSONAL Y LOGISTICA	0.2	46	0	0	0	0
DISPONIBILIDAD DE LA INFORMACION	0.2	600	1	1	0	0
PROCESOS FINANCIEROS	0.2	1008	2	2	0	0

P3: ACCESO LÓGICO NO AUTORIZADO, CON ALTERACIÓN O SUSTRACCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN

(REQUIERE LECTURA Y ESCRITURA) O sea, uso del sistema para obtener bienes o servicios aprovechables, sean programas, datos, etc.

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
PROCESOS PERSONAL Y LOGISTICA	0.2	92	0	0	0	0
DISPONIBILIDAD DE LA INFORMACIÓN	0.2	1200	2	2	0	1
PROCESOS FINANCIEROS	0.2	2017	4	3	0	1

P4: ACCESO LÓGICO NO AUTORIZADO CON CORRUPCIÓN O DESTRUCCIÓN DE LA INFORMACIÓN EN TRÁNSITO O DE CONFIGURACIÓN (USANDO O NO UN REEMISOR 'MAN IN THE MIDDLE' DE LOS MENSAJES; REQUIERE LECTURA Y ESCRITURA)

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
SERVIDOR CENTRAL	0.2	3700	7	6	0	3
RED LOCAL Y COMUNICACIONES	0.2	2394	5	4	0	2
EQUIPO INFORMATICO	0.2	5093	10	9	1	4

P5: INDISPONIBILIDAD DE RECURSOS, SEAN HUMANOS (HUELGA, ABANDONO, ROTACIÓN) O TÉCNICOS (DESVÍO DEL USO DEL SISTEMA, BLOQUEO).

ACTIVOS	**V %**	**IMP**	**RI**	**RE**	**RR**	**RS**
CAPACITACION PERSONAL Y ABASTECIMIENTO LOGISTICO	0.2	95	0	0	0	0
MANIPULAR Y CONTROL DE LA RED	0.2	1140	2	2	1	2
DIRIGIR, COORDINAR Y CONTROLAR LOS PROCESOS FINANCIEROS	0.2	1932	4	4	1	3

VII.- CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El desarrollo de la presente tesis ha sido totalmente oportuno, pues se ha detectado que existe un gran número de salvaguardas que necesitan ser implementadas de inmediato.
- La metodología de análisis y gestión de riesgos MAGERIT, ayuda a enfocar el problema de la seguridad desde una perspectiva completa, y evolucionable en el tiempo.
- Los activos son los elementos físicos, lógicos y organizativos que dan soporte a la realización del análisis y gestión de riesgos.

En el Departamento Administrativo no existe muchos mecanismos de salvaguarda.

- El riesgo principal en el Departamento Administrativo es Errores de utilización en la recogida y transmisión de datos o en su explotación en el software de base y paquetes.
- Como riesgo secundario se encuentra Accidente Físico de origen natural (fenómeno sísmico o volcánico) en el Departamento, seguido por un tercer riesgo en Errores de monitorización, trazabilidad en la red.
- Los Mecanismos de Salvaguarda como Plan de Contingencia disminuyen en un 75% la vulnerabilidad de las Amenazas.

RECOMENDACIONES

- Realizar la implantación de los Mecanismos de Salvaguarda simulados en el análisis y gestión de riesgos como Plan de Contingencia en el Departamento Administrativo.
- Los riegos y las salvaguardas del Departamento Administrativo se deben revisar cuando sea adecuado y periódicamente como una parte más de la gestión de riesgos.

- Utilizar opcionalmente la herramienta de distribución libre CHICHÓN para el análisis y gestión de riesgos.
- Identificar correctamente los activos y realizar adecuadamente el árbol de dependencia para el análisis de riesgos.

Latacunga, Octubre del 2003

Wellington Bladimir Montes Taco
050226480-7
AUTOR

Eduardo Gabriel Balarezo Vargas
050222024-7
AUTOR

Ign. Eddie Galarza Zambrano
DECANO DE LA FACULTAD
DE SISTEMAS E INFORMATICA

Dr. Mario Lozada Paredes
SECRETARIO ACADEMICO
ESPE SEDE LATACUNGA