



UNIVERSIDAD NACIONAL DE LA MATANZA
ESCUELA DE POSGRADO

MAESTRIA EN INFORMÁTICA

TESIS DE MAESTRÍA

Título de Tesis:

**Diseño de un Sistema de Gestión de Planes de
Contingencia y Gestión de Riesgos basado en Análisis de
Procesos de Negocio**

Autor: Domingo Donadello

Director: Jorge Eterovic

Buenos Aires, 21 de julio de 2009

INDICE

Capítulo 0 - Agradecimientos	7
CAPITULO I - INTRODUCCION	10
Área de Trabajo	10
Descripción del problema	10
Importancia del problema	11
Conceptos generales sobre Seguridad y Contingencia y riesgos de la información	11
La Tecnología informática (TI) en la Organización:	12
Objetivos, Motivación e Hipótesis de la Tesis	17
Breve esbozo de la solución	19
CAPITULO II - Estado de la Cuestión	22
¿Qué es la información?	22
Objetivos de la seguridad	28
Recursos y metodologías disponibles para contrarrestar las amenazas:	39
Vulnerabilidades	43
Descripción de soluciones de gestión de riesgos y planes basado en el modelo de análisis de procesos.	44
Framework ejemplo de modelización de procesos	49
Reglas de modelización de procesos	51
Se detalla a continuación un árbol parcial de categorías de riesgos basados en ISO 27001:	55
PLAN DE CONTINGENCIAS	69
Gestión de Riesgos	75
CAPITULO III - Planteamiento del Problema	81
Problemas para implementar Planes de contingencia y Gestión de riesgos	81
Se establece la Evaluación de Riesgos de la Seguridad	81
Cuantitativo vs. Cualitativo	82
Un ejemplo de establecimiento de plan de contingencias (RB 13):	88
Definición de Plan de contingencias:	90
CAPITULO IV – Solución	93
Diseño y especificación de una solución para elaborar planes de contingencia y gestión de riesgos basados en análisis de procesos críticos y sistemas Web Services.	93

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Modelo de un Sistema de Gestión de riesgos basado en Procesos	103
Diseño del sistema de software	105
Diseño del sistema de gestión de riesgos y planes de contingencia	106
Asistente para la formulación de plan de contingencia y Gestión de riesgos	124
Resultado	129
CAPITULO V - Conclusiones y Futuros trabajos	187
CAPITULO VI – Bibliografía	193
Referenciada	193
Complementaria	196
ANEXOS	209

CAPITULO 0
AGRADECIMIENTOS

CAPÍTULO 0 - AGRADECIMIENTOS

Al profesor Jorge Eterovic que durante el transcurso del dictado del curso sobre Seguridad informática, despertó mi interés por el tema de la vulnerabilidad de los sistemas de información y me hizo recordar experiencias profesionales pasadas, en diversas organizaciones empresarias donde desarrolle actividades, referidas a la gestión de los riesgos y los planes de contingencia informáticos y me permitió pensar en proponer una solución que integre las nuevas tecnologías de desarrollo de sistemas de software que yo mismo enseñé en la Universidad, para obtener soluciones aplicables a los métodos de planeamiento de recuperación de catástrofes y contingencia informáticos en las distintas organizaciones, tanto empresas como Gobierno y ONG.

A la Profesora Elisa Basanta que me contagio su entusiasmo y metodología.

A Hebe que me genera impulso vital todas las mañanas y me permite continuar recorriendo el largo y sinuoso camino de la vida. Y a mis nietos Andrés y Alejandro, por quienes sigo adelante y que son el motivo fundamental de mi vida en estos días.

A la UNLM y sus directivos, que me permiten disfrutar del ser profesor en la universidad.

A IRAM que me permitió desarrollar la actividad de auditor de sistemas de gestión de la seguridad y de la calidad, experiencia que me permite no solo exponer conceptos teóricos sino también los que se deducen de la práctica concreta en organizaciones.

A la empresa Siemens que me permitió la experiencia de gestionar seguridad de la información y administración de auditorías y a Cesar Ozán que me autorizó a utilizar los ejemplos presentados.

A la Mg. Alicia Mon que siempre intentó generarme entusiasmo por finalizar este trabajo.

CAPITULO I

INTRODUCCIÓN

CAPITULO I - INTRODUCCION

En este primer capítulo se realiza una introducción al contexto general de la Tesis, incluyendo la descripción de algunos elementos fundamentales, que permitan su íntegra comprensión.

ÁREA DE TRABAJO

El área de trabajo de la presente tesis es la referida a la seguridad de la información, en particular a los Sistemas de gestión de la seguridad de la información, que presenta dos ejes centrales para la concreción de una efectiva gestión, estos son:

- conceptos referidos a la implementación de planes de contingencia, que involucran planes de recuperación de desastres y planes de continuidad de negocio
- la gestión de riesgos, es decir el análisis de amenazas, sobre las debilidades que presentan los activos de la información, su evaluación y determinación del riesgo asociado para el establecimiento de salvaguardas o medidas que permitan eliminar, disminuir o aceptar el riesgo.

DESCRIPCIÓN DEL PROBLEMA

El problema se plantea al analizar los métodos y técnicas utilizadas en la práctica para gestionar riesgos y establecer los planes de contingencia, dado que al analizar distintas implementaciones, las mismas presentan una estructura rígida, basada en Procedimientos estáticos, que conforman el denominado Manual de Contingencias.

Como su nombre lo indica, se trata de documentos textuales que se utilizan como referencia para actuar en caso de incidentes a la seguridad, donde se describen las acciones y responsables de implementar las mismas ante situaciones que requieran la puesta en marcha de los mecanismos y salvaguardas establecidas.

En general, el Manual de Contingencias es una fotografía estática de un momento de la organización, que si bien puede ser exhaustivo en su forma de ser producido, el paso del tiempo tiende a que los procedimientos establecidos no contemplen todas las situaciones que día a día se presentan en la gestión informacional de la organización, que en sí es altamente cambiante por la característica que presentan los sistemas de información, la gestión y en particular los sistemas informáticos con cambio tecnológico continuo.

IMPORTANCIA DEL PROBLEMA

El problema planteado es de importancia relevante para la gestión de la organización, tanto en el nivel estratégico, táctico como operacional, es decir abarca todos los aspectos referidos a la gestión de la organización, en particular la gestión organizacional basada en uso de tecnología de información.

La importancia radica en que el componente informático presenta cada día mayor incidencia en los procesos de gestión organizacional, esto se visualiza en el uso de TI en gestión bancaria, trámites por Internet en organismos oficiales, llegando en algunos casos a un cien por cien de actividades totalmente automatizadas con mínima intervención humana como el caso de una planta industrial robotizada.

Asimismo, el cambio continuo tecnológico, la globalización, la interacción de los actores que participan de la gestión de la organización como clientes, proveedores, organismos y otros, requieren que la organización esté abierta al acceso de los mismos a su información, ya que la base de las operaciones, las decisiones y las políticas es la información que reciben, procesan y producen los sistemas de información.

Para entender la importancia del problema se desarrollan a continuación los conceptos presentados arriba:

CONCEPTOS GENERALES SOBRE SEGURIDAD Y CONTINGENCIA Y RIESGOS DE LA INFORMACIÓN

La dependencia de los procesos organizacionales de las empresas y organizaciones respecto de sus sistemas de información y de la tecnología informática,

se acrecientan día tras día y resulta indispensable tener estrategias para garantizar su recuperación y continuidad operativa ante cualquier contingencia que implique la no disponibilidad de los servicios informáticos y por ende de la gestión tanto operativa como de decisión.

LA TECNOLOGÍA INFORMÁTICA (TI) EN LA ORGANIZACIÓN:

Cada día es más la importancia que cobra el uso de la tecnología informática en todos los aspectos tanto en el ámbito laboral como personal y profesional. Si se utiliza la Internet con frecuencia para los procesos de gestión, cosa que ocurre sobre todo en el ámbito de la empresa, en el momento en que no puede acceder al buzón de correo, o conectarse a la Web, se percibe como que algo hace falta y que estamos momentáneamente paralizados sin posibilidad de realizar nuestras tareas. De igual manera cuando las líneas de comunicación en una empresa se interrumpen, desconectando los sistemas, o cuando se daña un disco duro, o se pierde el acceso al centro de cómputos, se corre el riesgo de grandes pérdidas, pues la información almacenada en los sistemas es un bien (activo de la información) cada día más importante y fundamental para el funcionamiento normal de las organizaciones.

Según mi experiencia personal, en la realización de tareas en sistemas desde hace mas de 37 años, resulta que desde aquella lejana época, algunos años atrás, (décadas del 60, 70 y 80), cuando el proceso de la información no dependía tanto del tiempo de respuesta y velocidad del proceso, ni tampoco la necesidad de la información era tan dependiente en su inmediatez, era muy sencillo también establecer un plan de contingencia, pues los sistemas informáticos generalmente tenían el respaldo de un sistema manual alternativo, de hecho muchos sistemas

informáticos solo procesaban información tomada de transacciones manuales, volcadas a formularios y por lo tanto, la pérdida de información resultaba prácticamente imposible que ocurriera ya que si se perdía una transacción digital, siempre quedaba el respaldo del formulario integrado manualmente.

Si era factible el no poder controlar adulteraciones, denegación o robo de la información.

Las aplicaciones trabajaban por lotes, y por lo general la interacción entre cada uno de lo que hoy se conocen como módulos (agrupaciones funcionales del software) se efectuaba mediante archivos que estarían disponibles al terminar uno de los procesos y al iniciar el otro. El concepto de diseño estaba orientado a utilizar de la mejor manera posible el espacio en disco y memoria (realmente limitados) de todas maneras había ganancia, porque se reemplazaba un proceso manual (que tomaba varias semanas) por uno computarizado que procesaría el mismo monto de información en pocos días.

Realmente solo intervenían tres componentes en el proceso de la información: el equipo de cómputos, los programas (software), y los datos (transacciones y archivos) y solo a estos tres componentes se remontaba la posible falla técnica o humana. Las razones externas que podrían causar una falla incluían un problema laboral (como una huelga que impedía el acceso al centro de cómputos), o un desastre natural y en ciertos casos aislados, motivado por disconformidad del personal de programación para con la empresa, alguna remota posibilidad de acciones delictivas como por ejemplo destruir información de archivos o modificar la lógica de programas con el fin de perjudicar a la organización.

Generalmente, existía un Centro de cómputos centralizado, con un área de control de la información de entrada y de salida del proceso, un área de registración de la información y un área de proceso de datos.

Los backups de archivos generalmente se mantenían en cajas fuertes ignífugas y el centro de cómputos tenía en su construcción incluidas medidas de seguridad contra incendios, inundación y otras.

En la actualidad, las denominadas salas cofre (RB 3) pretenden replicar en parte estos centros de cómputos de las décadas iniciales del proceso de datos por computadora.

Una descripción de estas salas se agrega como anexo VIII.

Hoy se mantienen los mismos problemas externos, pero se ha complicado y aumentado el número de componentes que se pueden ver afectados por una falla, incluyendo las redes de comunicación, las estaciones de trabajo, y la multiplicidad de equipos de almacenamiento distribuido, diversidad de plataformas de hardware y de software de base, los protocolos y componentes de comunicación multiplataforma. Las implicaciones de una falla, pueden ser de cuantía menor para una persona que trabaje con una PC pero igualmente desastrosas para la continuidad de su trabajo.

Lo único que realmente permite que una empresa (o una persona) pueda reaccionar adecuadamente a una falla en un proceso de gestión crítico, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia. El plan es precisamente lo que su nombre indica, una serie de actividades, procesos, normas, métodos y procedimientos de control, tendientes a restablecer la operación normal, en el evento de una calamidad o desastre interno o externo a la organización.

A manera de comparación, cuando el sistema era centralizado, el proceso era por lotes, y la interfase con la máquina era una Terminal, lo único que se requería para tener en pie y activo, un plan de contingencia de fácil ejecución, era un contrato de reciprocidad con una empresa que tuviera un equipo similar al de uno, y una copia alterna de la información más reciente, de tal manera que se pudiera trasladar el proceso a la instalación de la empresa recíproca. Normalmente se utilizaban horarios nocturnos o los fines de semana, que por lo general no se ocupaban en el proceso cotidiano de la empresa que prestaba el servicio y como las transacciones se procesaban off line, prácticamente estaba garantizada la continuidad de la gestión de los procesos de negocio.

El proceso de la información era ejecutado en su mayoría, por no decir en su totalidad, por personal del Departamento de Sistemas, por lo que no se requería mayor contenido en un plan de contingencia y se puede decir que tampoco ningún entrenamiento, excepto horas de trabajo adicional del personal de sistemas y básicamente del sector de operaciones, quienes ejecutarían las actividades necesarias para restablecer el servicio. Por último, la información era un reflejo de actividades históricas, no necesariamente se requería de la información para la toma de decisiones.

Para que hoy en día, con lo complejo de los sistemas de información actuales, además de la responsabilidad del usuario en el proceso de su información, los Planes de Contingencia formalizados y probados cobran una importancia máxima al interior de las empresas, e inclusive en el ámbito personal. Resulta tan dependiente nuestro trabajo de la información que tengamos a la mano, que se reducen los espacios en los que se puede estar sin acceso a la misma, existen actividades totalmente

informatizadas donde la falta del recurso informático hace imposible la ejecución normal de las tareas de las personas.

Además no solo se trata de personal interno y sistemas internos, también actualmente las empresas recurren a los proveedores de prestaciones y servicios realizando outsourcing total o parcial de sus tareas y procesos los que también pueden verse afectados para brindar sus servicios.

La Norma IRAM / ISO 17799 (actual 27002) (RB – 1) utilizada hoy en día, es una compilación de recomendaciones de las mejores prácticas para garantizar la seguridad de la información, que toda organización puede aplicar, independientemente de su tamaño o sector de actividad, la norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la adoptasen, para que prefieran una solución de seguridad específica. Las recomendaciones de la Norma Técnica ISO 17799 (hoy 27002), son neutrales.

El Plan de Contingencia (RB 4) debe obedecer a un proceso formal y debe ser la conclusión de un proyecto de elaboración del mismo que incluya la identificación de los factores críticos, recursos y procesos claves, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba real del mismo plan, la capacitación de las personas involucradas y una constante y continua actualización.

La Organización del comercio mundial, establece 9 principios rectores respecto de la información y la seguridad de la información que deben respetar las organizaciones que realizan transacciones comerciales y de gestión en el mercado global que se describen a continuación:

9 Principios de la Gestión de la seguridad de la información de la OECD Organización para la cooperación y el desarrollo económicos

- 1- Concientización
- 2- Responsabilidad
- 3- Respuesta
- 4- Ética
- 5- Democracia
- 6- Evaluación del riesgo
- 7- Diseño e implementación de seguridad
- 8- Administración de la seguridad
- 9- Reevaluación

Las normas, métodos y técnicas referidas a gestión de la información, tienden a establecer procesos de gestión de la información que permitan a las organizaciones cumplir con estos postulados.

OBJETIVOS, MOTIVACIÓN E HIPÓTESIS DE LA TESIS

La intención del estudio es establecer que los sistemas basados en Internet agilizan, facilitan y optimizan la gestión de sistemas de seguridad de la información, que de otra manera resultarían costosos y que en lugar de mantenerse actualizados van perdiendo vigencia, como sería el denominado plan de contingencias en una organización y por ende la gestión de los riesgos asociados a los procesos de negocios y activos de la información, que en general parten de un proyecto con recursos humanos y técnicos asignados, tiempo para dedicar a establecer el plan por parte de la alta Dirección y generalmente finaliza en el denominado Manual de procedimientos de contingencia, que por su característica tiende a quedar obsoleto con el paso del tiempo.

La participación del autor en el Proyecto, para el cumplimiento de la Ley Sarbanes Oxley de implementación de un sistema de gestión de auditorías de controles de los activos de información para la empresa Siemens, durante 2005 y 2006, permitió al mismo, constatar como se pueden mantener actualizados a través del uso de sistemas Web Services, el análisis de riesgos, los procedimientos de contingencia y los

controles cuando los activos son determinados a partir del estudio y análisis de los procesos claves de negocio y los riesgos asociados a los activos que se utilizan en las actividades de los procesos.

El trabajo desarrollado comienza con la presentación de los conceptos básicos referidos a Seguridad informática, análisis de riesgos y Planes de contingencia, exponiendo el estado actual en la materia, incluyendo normas, métodos y procedimientos habituales utilizados en las organizaciones, para dar satisfacción a la necesidad de contar con estrategias de atención a los riesgos y salvaguardas sobre los activos de la información e informáticos de las mismas, en particular determinar los activos de la información a partir del denominado análisis de procesos de negocio claves de la organización, que son los que deben estar en condiciones de ser procesados, ante situaciones que no permitan la continuidad normal de las operaciones, aplicando sobre los mismos las denominadas salvaguardas.

El segundo ítem conceptual a desarrollar a manera de introducción, es el referido a sistemas basados en la arquitectura de servicios Web, para lo cual se describen y se desarrollan conceptos y los elementos técnicos mínimos necesarios de aplicaciones basadas en servicios Web, en particular presentando la solución que provee el Framework de Microsoft, denominado .Net, en el Anexo I de la tesis.

El objetivo fundamental del trabajo presentado es formular el diseño de sistemas basados en Web para acompañar la gestión de la seguridad de la información, mediante la definición y aplicación de salvaguardas en los activos que administran los procesos clave de la organización, para lo cual:

Se presenta el diseño de software de tres sistemas en formato navegable, que permitirán:

Formular los proyectos de desarrollo de planes de contingencia y gestión de riesgos.

Administrar los activos, amenazas, riesgos y salvaguardas como un sistema de gestión una vez finalizado el proyecto de implementación del plan de contingencias.

Controlar y monitorear es estado de riesgos sobre los activos de información que se manejan con el sistema de gestión y administración anterior.

Este proyecto tendrá dos ámbitos de estudio: el de la Seguridad informática, el análisis de riesgos y los Planes de Contingencia, mediante el estudio y análisis de los procesos de negocio claves y el de los sistemas de software basados en servicios Web, utilizando computación distribuida para intranets e Internet, de manera de facilitar la accesibilidad a los procedimientos, métodos y técnicas utilizadas para realizar la gestión de riesgos y el proceso de los planes de contingencia organizacionales.

BREVE ESBOZO DE LA SOLUCIÓN

La solución que se presenta en esta tesis de Maestría, consiste en tres Diseños de productos de software, denominados Web Services, navegables, que tienen los siguientes objetivos:

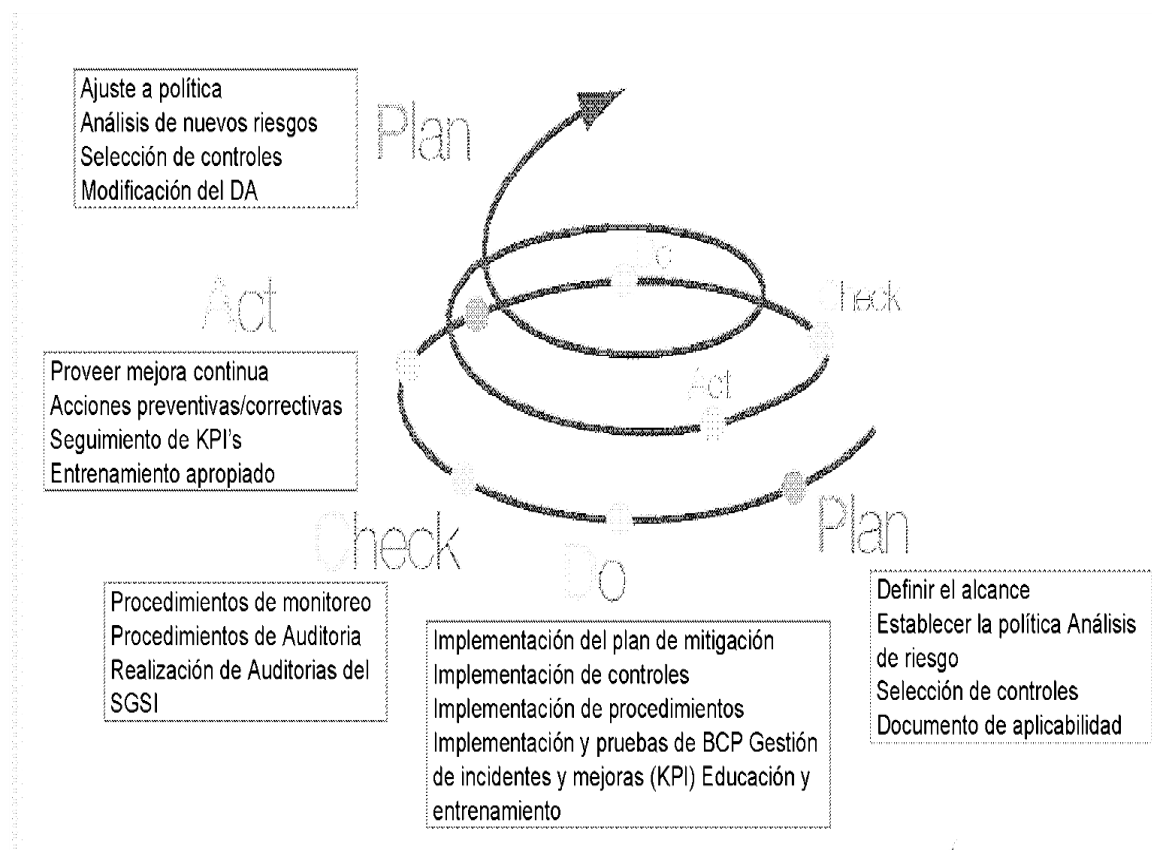
Que la Dirección y alta gerencia de una organización disponga de una ayuda en intranet o Internet para los Gerentes de proyectos que tienen a su cargo llevar adelante la implementación de la gestión de riesgos y elaborar los planes de contingencia de las organizaciones.

La ayuda consiste en brindar una metodología prescriptiva, es decir por fases, divididas en actividades y estas en tareas, con ayudas de plantillas, métodos, técnicas y herramientas necesarias para la realización y documentación del sistema a implementar.

La estructura del proyecto se basa en la realización de la reingeniería de procesos de negocio claves de la organización, para determinar los procesos críticos

en cuanto a los riesgos, económicos, financieros, de información, de infraestructura y todo aquel que afecte la continuidad del negocio.

Uno de los objetivos fundamentales de los sistemas diseñados, presentados en esta tesis, es que la organización pueda implementar el modelo Plan – Do – Check – Act (base de los sistemas de gestión orientados procesos) aplicado a los sistemas de gestión de la seguridad de la información:



Además, que la utilización de los sistemas Web diseñados acompañen el proyecto de implementación de la seguridad, faciliten la construcción de dos sistemas:

- Sistema de gestión de los riesgos
- Sistema de monitoreo del estado de aplicación de los controles sobre los riesgos de los activos
-

CAPITULO II

ESTADO DE LA CUESTIÓN

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

CAPITULO II - ESTADO DE LA CUESTIÓN

INTRODUCCIÓN CONCEPTUAL SOBRE CONCEPTOS REFERIDOS A INFORMACIÓN, GESTIÓN DE LA INFORMACIÓN Y SEGURIDAD DE LA INFORMACIÓN.

Todo lo que se expone a continuación, forma parte de los cursos de capacitación TI 01 – Introducción a la norma IRAM – ISO/IEC 27002, TI 02 – Introducción a la norma IRAM – ISO/IEC 27001 y TI 05 Auditoria de los sistemas de gestión de la información, que el autor de esta tesis dicta para IRAM desde 2006, que pueden ser consultados en www.iram.org.ar ingresando a capacitación en TI, allí están los programas de los cursos y sus cronogramas de fechas.

A partir de aquí se desarrollan los conceptos fundamentales que dan sustento a la solución planteada por el autor en la presente Tesis.

¿QUÉ ES LA INFORMACIÓN?

Esta pregunta debe resolverse antes de comenzar cualquier proyecto de implementación de la gestión de la seguridad.

“La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida.”

“La información es un activo que, como todo activo importante de negocio, tiene valor para la organización y por consiguiente debe ser protegido adecuadamente ”

Cuales son los Tipos de información que una organización debe resguardar para garantizar su normal operación:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida por correo o utilizando medios electrónicos
- Presentada en imágenes
- Expuesta en conversaciones
- Almacenada en la inteligencia del personal operativo, de mandos medios y de alta gerencia.

Cada día más las organizaciones de todos los tamaños y tipos, depende de la tecnología de la información para gestionarse adecuadamente, es decir la TI está cada

vez más dentro de los procesos de negocio en todos los niveles, operativos, tácticos y de decisión.

Esto hace que la dependencia de la gestión organizacional sea cada vez más alta, llegándose en algunos casos a no poder ejecutar operaciones en el caso de caída de los sistemas de información.

En este sentido es que es necesario que las organizaciones implementen sus sistemas de gestión de la seguridad de la información, pero no existe la "verdad absoluta" en Seguridad de la Información y por ende en gestión de la seguridad Informática. Si hay algunas premisas que deben ser tenidas en cuenta:

La información es vulnerable y no es posible eliminar todos los riesgos.

No se puede contar en forma permanente con un especialista en todos los temas, por ello se recurre a servicios de apoyo puntuales.

La Dirección no está convencida de que la Seguridad en TI hace al Objetivo del negocio de la compañía.

Cada vez los riesgos y el impacto de la TI en los negocios son mayores.

No se puede dejar de hacer algo en este tema de la seguridad de la información.

La justificación de implementar la Seguridad de la información en una organización se desprende de algunos datos como que según una encuesta del Departamento de Defensa de USA:

Sobre aproximadamente 9000 computadores atacados, 7,900 fueron dañados.
400 detectaron el ataque.

Sólo 19 informaron el ataque.

En general todos coinciden en que el 80% de los incidentes/fraudes/ataques son efectuados por personal interno

Fuentes:

The Computer Security Institute

Cooperative Association for Internet Data Analysis (CAIDA)

CERT

SANS

Siendo que la información debe considerarse como un recurso con el que cuentan y necesitan las Organizaciones y por lo tanto tiene valor para éstas, al igual que el resto de los activos, debe estar debidamente protegida.

¿Qué se debe asegurar?

La Seguridad de la Información, protege a ésta de una amplia gama de amenazas, tanto de orden fortuito como destrucción, incendio o inundaciones, como de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, etc.

Entonces podemos contestar:

¿Qué es la seguridad de la información?

La seguridad de la información protege la información de una amplia gama de amenazas con el fin de asegurar la continuidad del negocio, minimizar el daño al negocio y maximizar el retorno de la inversión y las oportunidades de negocio.

En este sentido, ¿qué debe garantizar la gestión de la seguridad de la información?:

Confidencialidad: Se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

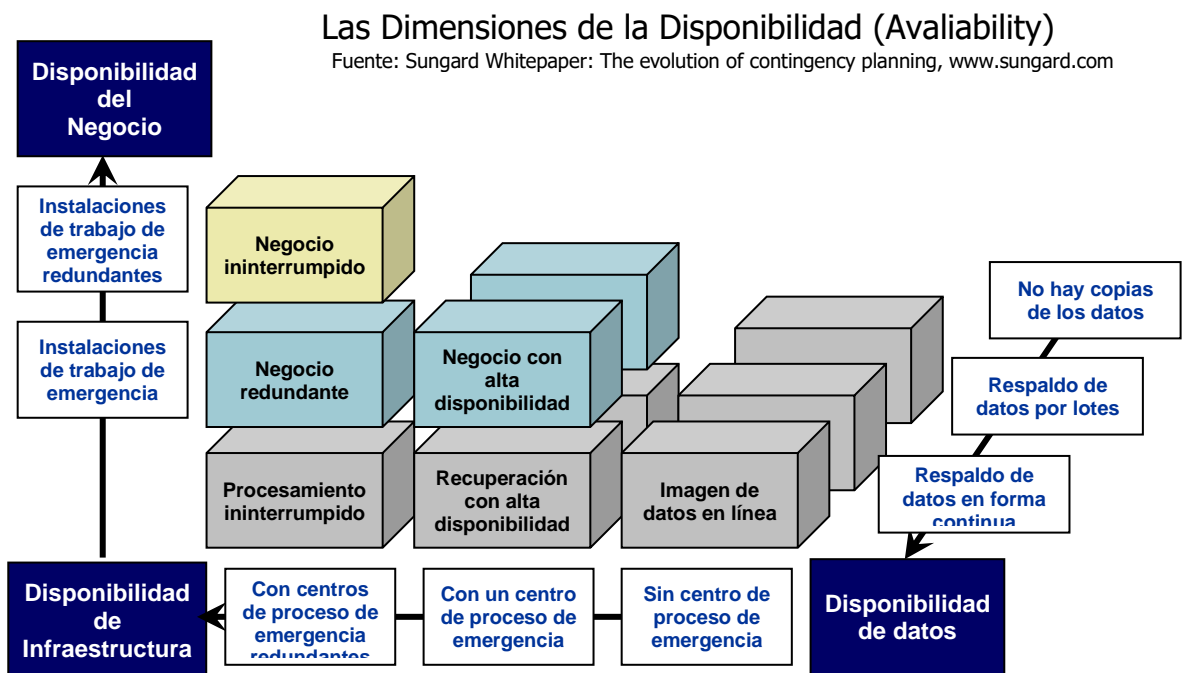
Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma toda vez que se requiera.

El siguiente cuadro muestra que preserva la gestión de la seguridad de la información:



En el siguiente cuadro se detallan las variables intervinientes en la disponibilidad de la información:



¿Cómo se logra la seguridad de la información?

La seguridad de información se logra mediante la implementación de un adecuado conjunto de controles, los que podrían ser:

Políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software.

Se necesita establecer estos controles para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

¿Por qué es necesaria la Seguridad de Información?

Las organizaciones y sus sistemas de información y redes están enfrentados en forma creciente a las amenazas de la seguridad desde una amplia gama de fuentes, incluyendo:

- Fraudes apoyados por computador
- Espionaje
- Sabotaje
- Vandalismo
- Fuego o inundación (y otros desastres naturales o sociales).

Las fuentes de daño (RB 5 Portales de la seguridad de la información) tales como los virus computacionales, hacking por computador y ataques de denegación de servicio, han llegado a ser más comunes, más ambiciosas y cada vez más sofisticadas como la denominada ingeniería social.

La dependencia en los sistemas de información y de servicios implica que las organizaciones son más vulnerables a las amenazas de la Seguridad.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que se puede lograr a través de dispositivos técnicos es limitada, y debería ser apoyada por procedimientos y una gestión apropiada. Identificar qué controles y en qué lugar deberían estar, requiere una planificación cuidadosa y una atención detallada.

Actualmente es posible incluir controles en el software a nivel código como requisitos de la seguridad de la información en los sistemas (RB 6) y auditarse

mediante la normas ISO referenciadas 15408 basada en el Common Criteria suscripto por más de 20 países de Europa, Asia y Estados Unidos.

La gestión de seguridad de la información necesita, como mínimo, la participación de los proveedores, clientes y accionistas.

También pueden ser necesarias las opiniones de especialistas de organizaciones externas. Los controles de seguridad de la información son considerablemente más baratos y más efectivos si son incorporados en la etapa de diseño y especificación de los requisitos de los sistemas de información a desarrollar.

El siguiente cuadro muestra los elementos y factores que definen el contexto de la seguridad de la información:



Finalmente la la seguridad de la información es el análisis e implantación de un grupo de controles apropiados para resguardar la información,

Incluye:

- Políticas
- Practicas (herramientas)
- Procedimientos

Se requiere establecer controles para asegurar los objetivos específicos de seguridad de la organización que minimizan los riesgos potenciales sobre los activos de la información.

Objetivos de la seguridad

Tres componentes a tener en cuenta para la seguridad

1) Ataques a la seguridad:

Cualquier acción que compromete la seguridad de la información perteneciente a la organización.

2) Mecanismos de seguridad:

Es un mecanismo diseñado para detectar, prevenir y/o recuperar frente a un ataque a la seguridad.

3) Prestación de seguridad:

Es un servicio que mejora la seguridad de un sistema de procesamiento de datos y de la información que transfiere la organización. El servicio enfrenta los ataques a la seguridad utilizando para poder hacerlo, uno o más mecanismos de seguridad.

¿Cómo establecer los requisitos de Seguridad?

Es esencial que una organización identifique sus requisitos de seguridad

Existen tres fuentes principales:

La primera fuente se obtiene de evaluar los riesgos de la organización. A través de esta evaluación, se identifican las amenazas a los bienes y procesos, la vulnerabilidad, se evalúa la probabilidad de ocurrencia y se estima el impacto potencial.

La segunda fuente es legal, estatutaria, regulatoria y los requisitos contractuales que tiene que satisfacer tanto la organización, como sus socios comerciales, los proveedores y personal externo de servicios.

La tercera fuente es un conjunto particular de principios, objetivos y requisitos para el procesamiento de la información que una organización ha desarrollado para el apoyo a sus Operaciones.

Como ya expresamos, las Organizaciones son cada vez más dependientes de sus Sistemas y Servicios de Información, por lo tanto podemos afirmar que son cada vez más vulnerables a las amenazas concernientes a su seguridad.

Entre otras causas, el crecimiento exponencial de las Redes y Usuarios Interconectados, la profusión de las Base de datos On-Line, la inmadurez de las Nuevas Tecnologías, la alta disponibilidad de Herramientas Automatizadas de Ataques y las nuevas Técnicas de Ataque distribuido (Ej.: DDoS), también se destacan las técnicas de Ingeniería Social.

¿Cuáles son las amenazas?

Accidentes: Averías, Catástrofes, Interrupciones,...

Errores: de Uso, de Diseño, de Control,....

Intencionales presenciales: Atentado con acceso físico no autorizado

Intencionales Remotas: Requieren acceso al canal de comunicación

Y se destacan las siguientes:

Interceptación pasiva de la información (amenaza a la CONFIDENCIALIDAD).

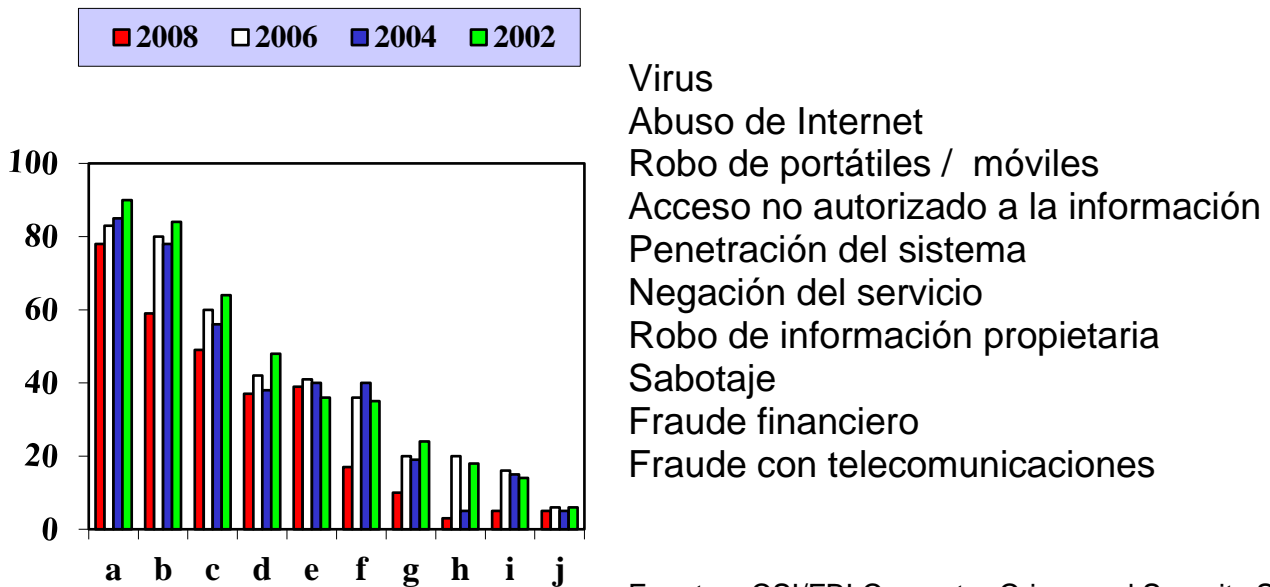
Corrupción o destrucción de la información (amenaza a la INTEGRIDAD).

Suplantación de origen (amenaza a la AUTENTICACIÓN).

Más del 90 % de las compañías se enfrentan a peligros en la continuidad del negocio, pero sólo del 25 % han invertido en planes de continuidad. Estas cifras deberían cambiar.

El siguiente cuadro muestra el estado de ataques y tipos de ataque:

TIPOS DE ATAQUES (%)



- Virus
- Abuso de Internet
- Robo de portátiles / móviles
- Acceso no autorizado a la información
- Penetración del sistema
- Negación del servicio
- Robo de información propietaria
- Sabotaje
- Fraude financiero
- Fraude con telecomunicaciones

Fuentes: CSI/FBI Computer Crime and Security Survey

Lo desconocido ya está aquí. Puede ser un hacker que trata de destruir un sistema de computadoras o un empleado descontento que intenta sabotear una base de datos; o pudiera ser un tren de mercaderías que descarrila cerca de las oficinas centrales de la compañía produciendo una liberación de gases tóxicos que fuerza a evacuar a los empleados; o un tornado que arranca el techo de una planta haciendo que lluvias torrenciales destrocen los productos almacenados y dañen los computadores; o pudiera ser una ruptura de la seguridad informática que ponga en peligro información financiera confidencial de varios miles de clientes.

Estos escenarios –todos ellos reales- son sólo un pequeño ejemplo de los desafíos que una organización debe estar dispuesta a afrontar para evitar grandes pérdidas que pudieran dañarla o, incluso, destruirla.

Tal como el mundo ha conocido dolorosamente, la amenaza del terrorismo planea sobre las empresas y sus empleados. Reconociendo una vulnerabilidad en aumento, las compañías están incrementando sus inversiones en seguridad corporativa.

Hoy, una corporación típica abarca entornos globales, tiene una red extensa de asociados y depende fuertemente de la tecnología para transferir los productos desde el diseño hasta el cliente. En el siglo XXI el énfasis ha cambiado desde “si” el fallo

puede ocurrir a "cuándo ocurrirá la falla?". Y cuando lo haga, ¿lo notarán los clientes?, ¿cuánto costará reparar la actividad? y ¿cuál será el impacto a largo plazo sobre nuestra organización?.

Resulte la seguridad de una compañía en peligro por un acto terrorista, un ataque informático, un empleado descontento o una simple falla de sistemas, mantener funcionando el negocio es vital para evitar daños financieros o la extinción de la compañía. Cada año el impacto económico de los aspectos de continuidad y seguridad asciende a miles de millones de dólares debido a que las compañías no están preparadas para lo inesperado. Las amenazas a la continuidad de los negocios no son raras; de hecho, están presentes en el 90 % de las compañías. Pero con la preparación correcta, las empresas se pueden posicionar para soslayar amenazas a sus operaciones y protegerse de una hecatombe potencialmente desastrosa.

No hace mucho tiempo los programas de continuidad de los negocios eran definidos como la prevención de pérdidas catastróficas y planes de recuperación en casos de desastres informáticos. Pero esta definición, sencillamente, ya no vale en este momento tal aseveración. Mientras que la continuidad de las empresas se extiende más allá de la seguridad y recuperación en caso de desastres tradicionales, ya no se trata sólo de sistemas informáticos y de tecnología, se trata de la supervivencia organizacional.

Las operaciones globales, la sofisticación de la cadena de valor y una tecnología omnipresente han aumentado exponencialmente los puntos de falla y riesgo a lo largo de la empresa. La cadena tradicional de valor en el negocio se ha hecho cada vez más compleja y susceptible de fallar. Aún así, sólo el 25 % de compañías han invertido en planes de continuidad del negocio. Desgraciadamente, un abrumador 40 % de empresas medianas que sufren un problema serio nunca vuelve a abrir, y de las que lo hacen, el 40 % desaparece a los tres años.

Cuando una empresa se enfrenta a una crisis, la clave para su supervivencia es detener o minimizar la interrupción del negocio. Cuando una organización se ve forzada a cerrar por alguna razón, los efectos típicos incluyen:

- pérdidas de ingresos
- demanda de responsabilidades
- pérdida de la imagen de marca
- pérdida del valor accionario
- retrasos en los cobros y facturaciones
- penalizaciones fiscales
- costo del reemplazo de los equipos.

No es sólo en lo relativo a desastres y catástrofes sobre lo que las compañías tienen que planificar. Aunque un huracán puede conducir a una pérdida de 20.000 Millones de dólares, destruir los negocios y hacer que las primas de seguros se disparen, algo tan simple como un virus de computadora o problemas del hardware tiene el potencial de ser igual de dañino.

En un pasado inmediato, el virus "I love you" demostró el inmenso daño que un simple virus puede producir. La revista Computer Economics estima que el impacto económico a escala mundial del virus del amor fue de 8.750 Millones de dólares y algunas compañías tuvieron que cerrar durante días para limpiar sus sistemas de este "gusano" persistente. Desde luego, nuevos virus están surgiendo continuamente y producen daños no cuantificables ni públicos a compañías que carecen del software antivirus más actualizado.

Normalmente las áreas más preparadas para la continuidad de los negocios son la tecnológica y la informática. Aún así, la protección de los sistemas no ha ido a la misma velocidad que su vulnerabilidad. La tecnología de la información se ha convertido en una parte integral de todas las operaciones de negocio con una dependencia respecto a los sistemas de los asociados que va en aumento. Una encuesta reciente de Information Week realizada a cien profesionales de tecnología de los negocios indica que mientras casi todas sus compañías tienen estrategias para la continuidad en los negocios y la contingencia de las tecnologías de la información, la mayoría de ellas no respondería adecuadamente ante un caso de emergencia real.

A la vez que la conectividad con socios de negocio y clientes aumenta, también lo hacen los puntos de entrada y, por ello, la posibilidad de tener problemas. Las rupturas de seguridad, únicamente, se han multiplicado por diez desde 1997. Los retos informáticos más normales incluyen robo de información y fraude, sabotaje de empleados o hackers, espionaje industrial, etc. Los costos directamente cuantificables de atentados informáticos en el año 2001 se estimaron en, al menos, 377 Millones de dólares, un aumento de seis veces en sólo cuatro años.

Los desastres y los acontecimientos del 11 de septiembre han permitido centrar la atención de las compañías de seguros en la posibilidad de ocurrencia de interrupciones importantes en las operaciones de negocio. Las primas totales aumentaron más de un 15 por 100 en el año 2002 colocando a la industria en su mayor nivel de crecimiento desde 1986. Y las tarifas del 2002 para reaseguros catastróficos parece han crecido entre el 20 % y el 30 %. Los reaseguros industriales contra riesgos han crecido en un 50 %.

Claramente, la importancia de la planificación en la continuidad de los negocios y la protección de la seguridad continuará creciendo. Algunas tendencias clave tendrán un efecto envolvente en la preparación para la continuidad en el negocio y la posibilidad de sufrir fallas o interrupciones.

Según las compañías continúan uniendo sus sistemas con los de sus asociados y clientes, y buscan oportunidades de outsourcing, deben también adaptarse a un control descentralizado.

A la vez que las compañías se fusionan y los mercados se consolidan, surgen dos áreas de preocupación. Las fusiones afectan a las relaciones, operaciones y tecnologías existentes; son siempre incómodas y frecuentemente fracasan en la creación del valor accionario esperado. Y según los mercados se consolidan en menos y mayores entidades, las economías se concentran más, con un impacto de falla mayor y una más alta probabilidad de convertirse en una catástrofe.

Los problemas laborales, la inestabilidad política, el sentimiento antiglobalización y las operaciones de diversificación, todo hace aumentar el peligro de interrupción de los negocios.

Según la información va reemplazando a la moneda y a los activos, las salvaguardas de la información deben aumentar. El robo, sabotaje o simplemente una interrupción temporal del flujo de información pueden causar el pánico en un negocio o en sus clientes y proveedores.

La continua expansión del alcance de la tecnología conduce a una complejidad en aumento y a más puntos de falla potencial, haciendo que los negocios estén expuestos a peligros inesperados. Los problemas en la seguridad del software de uso común, la transmisión de virus y los accesos a datos confidenciales de la corporación por Internet, ya crean de forma rutinaria alertas de interrupción de los negocios.

Con el crecimiento rápido del comercio virtual, el entorno regulatorio continuará evolucionando y afectando a la falta de preparación de las empresas, especialmente en las áreas de privacidad de los clientes y empleados y en el fraude en el comercio on-line. El año pasado, por ejemplo, las compañías financieras gastaron más de 400 Millones de dólares preparando políticas de privacidad que satisficieran los requisitos regulatorios.

Las empresas que proporcionan un acceso sin trabas de sus clientes a sus sitios Web y entornos de negocio on-line, están sujetas a la impredecibilidad de la reacción de los clientes. Fluctuaciones en la demanda, interrupción de los sistemas, las carreras inesperadas de los compradores de fin de semana o un acontecimiento informático popular a lo bruto, pueden resaltar las vulnerabilidades de quienes no están preparados creando las versiones-siglo XXI de las carreras a sacar dinero los bancos.

Según van creciendo las complejidades e incertidumbres que amenazan a los negocios, la continuidad de las empresas y la seguridad corporativa se están convirtiendo en una cuestión esencial para los máximos ejecutivos. A la vez que las compañías necesitan una percepción y visibilidad más altas de los principales riesgos del negocio, también deben tener un plan de acción bien pensado, sólido y fácilmente adaptable.

No solamente ha aumentado la tipología de los peligros y sus consecuencias, sino que la anatomía de las crisis típicas de los negocios también ha evolucionado. Más que una catástrofe única, a menudo hay muchos acontecimientos en cadena que

forman las crisis modernas. De hecho, a menudo no son reconocidos en un principio y los desastres reales son raras veces directos u obvios.

Mala planificación, análisis erróneos y comunicaciones deficientes pueden hacer que una situación mala empeore. Una agencia de negocios aprendió muy bien esta lección. En la mañana de un lunes, habiéndose producido problemas de red después de que el responsable de los computadores se hubiera ido a su casa el viernes, la compañía era incapaz de realizar transacciones. Aunque inicialmente hubo sospechas de sabotaje, la diagnosis final fue una ejecución errónea de los procedimientos de cambio de control diseñados para proteger la continuidad del negocio. En otros casos, sin embargo, el sabotaje es el origen del problema. Por ejemplo, un empleado de Verizon destruyó datos que causaron 200.000 dólares de pérdidas en daños y terminó con una confesión criminal.

Los planes más eficaces para asegurar la continuidad del negocio incluyen a la vez los peligros y los efectos potenciales. Un banco institucional con base en Australia desarrolló un plan que necesitaba ser probado antes de que el país fuera sede de los Juegos Olímpicos de verano en el 2000. El banco requería que en la situación más extrema pudiera ser dispuesta una sala de contingencia de transacciones equipada de personal como máximo en dos horas después de que hubiera ocurrido un desastre potencial. La colaboración estrecha entre las unidades de comercio y las oficinas centrales fue clave en determinar qué funciones y procesos precisaban ser soportados. El resultado final fue que la prueba del plan de contingencia constituyó un éxito. Afortunadamente no se produjeron emergencias, pero los directivos del banco y los clientes estuvieron más tranquilos sabiendo que sus operaciones no sufrirían interrupciones.

¿Cómo se puede resolver el problema de la seguridad de la información?

Las tres primeras tecnologías de protección más utilizadas son el control de acceso / passwords (100%), software antivirus (97%) y firewall (86%)

Los ataques más comunes durante el último año fueron los virus informáticos (27%) y el spamming de correo electrónico (17%) seguido de cerca (con un 10%) por los ataques de denegación de servicio y el robo de notebook.

El problema de la Seguridad Informática está en su Gerenciamiento y no en las tecnologías disponibles.

La propuesta de esta tesis es utilizar los conceptos de la Reingeniería por procesos y sistemas como soporte a la implementación de la gestión de la seguridad de la información.

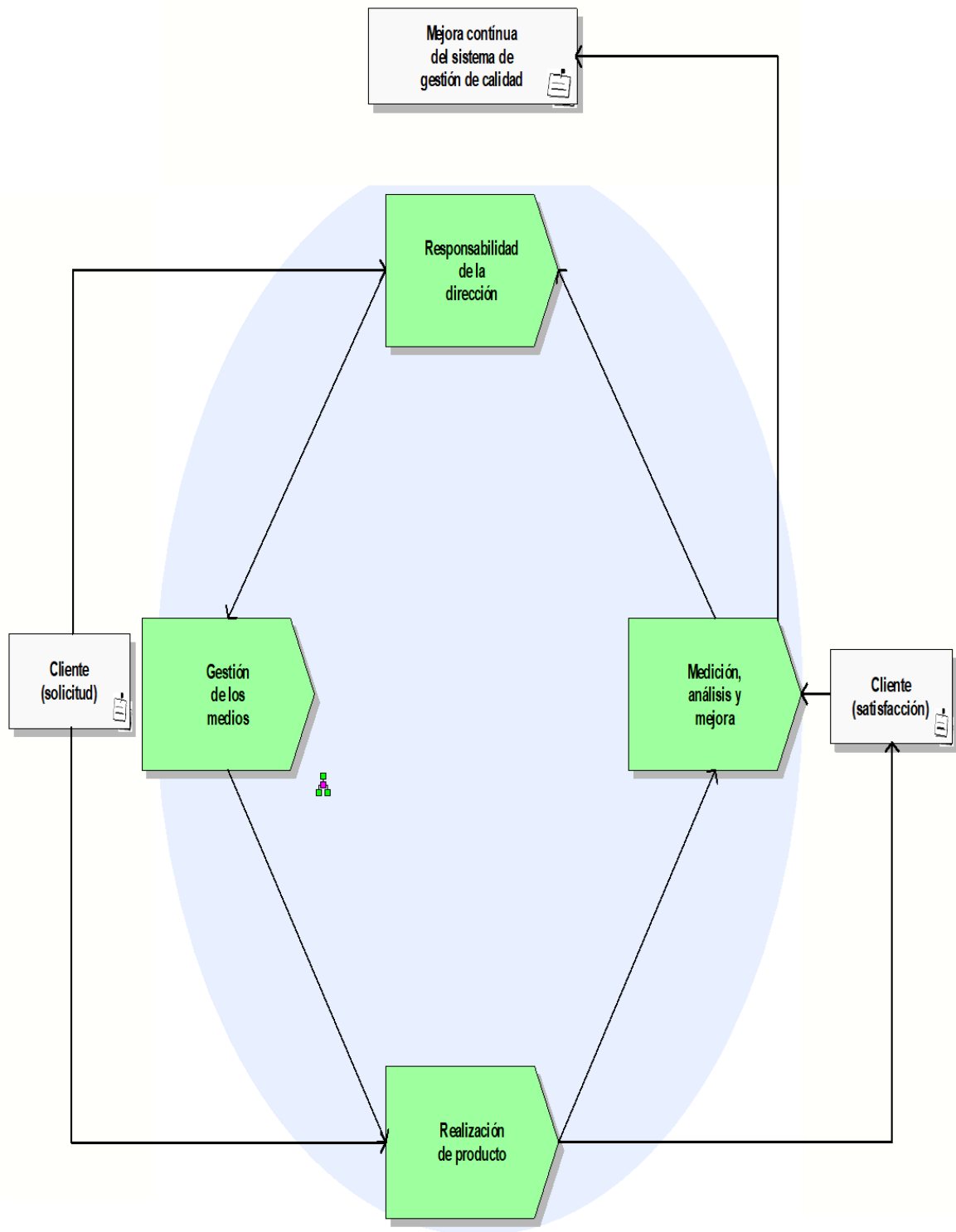
El éxito de la implementación de un sistema de gestión de la seguridad de la información que dé resultados razonables radica en poder encarar el mismo basado en el concepto de reingeniería,

Basada en análisis de los procesos clave de la organización y análisis de los riesgos vinculados a los mismos.

En el siguiente cuadro se muestra un esquema de conceptos que abarca la reingeniería necesaria para lograr la implementación de un sistema de gestión de la seguridad de la información.

La reingeniería que actualmente es más aplicada en el ámbito organizacional es la orientada a los procesos de negocio, es decir entender cuales son los procesos clave de la gestión y determinar el nivel de activos, amenazas sobre los activos, riesgos y salvaguardas que deben aplicarse en los procesos. (RB 8 – Planes de contingencia).

El modelo para analizar, documentar y mejorar los procesos de negocio se basan en el Esquema de la ISO 9000 (RB 7), Modelo Plan-Do-Check-Act, de la mejora continua de los procesos. El siguiente está tomado del modelo de la norma mencionada y que se aplica a todos los sistemas de gestión:



En este esquema se aplican los conceptos de reingeniería que se establecen en el siguiente esquema de aplicación:

Reingeniería



Se requiere:

Apoyo de la Alta Dirección y Gerencia

RRHH con conocimientos y experiencia

RRHH capacitados para el día a día

Recursos Económicos

Tiempo

¿Por donde empezar?

El fundamento de una buena seguridad reside en conocer la sensibilidad y/o criticidad de los activos que se desean proteger; para ello es necesario efectuar:

– Clasificación de la información.

– Gestión de riesgos.

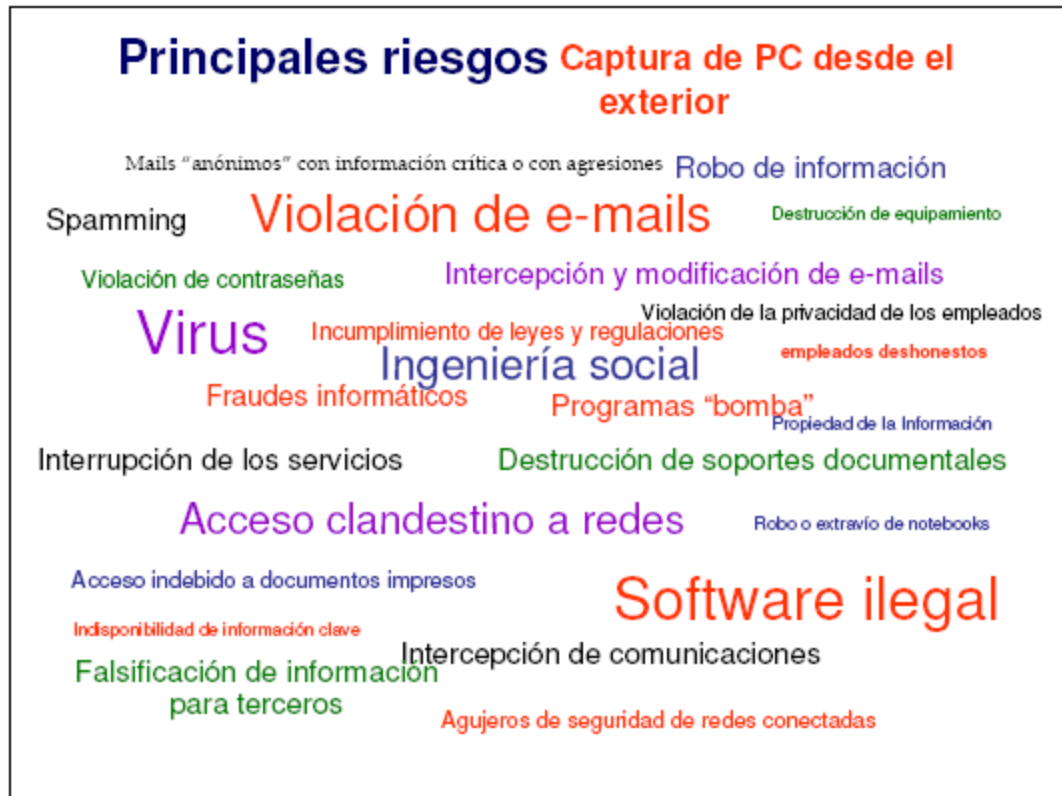
Clasificación de información:

Niveles de valoración de la información (confidencial, privado, público).

Activos físicos y lógicos.

Ejemplos; Códigos de tarjetas y cuentas de clientes, historia clínica médica, presupuestos y proyectos, ERP, información de pagos (proveedores y clientes).

A continuación, en el cuadro que sigue, se muestran los principales riesgos a que se ve sometida una organización en materia de seguridad de la información.



Se puede estar preparado para que el riesgo, ocurra lo menos posible:

Sin grandes inversiones en software

Sin mucha estructura de personal

Tan solo:

Ordenando la Gestión de Seguridad y parametrizando la seguridad propia de los sistemas. Utilizando herramientas licenciadas y libres en la Web

Ejemplos de **amenazas** a la información:

Empleados

Baja conciencia de la importancia en cuestiones de seguridad

Crecimiento en redes y computación distribuida

Crecimiento en complejidad y falta de eficiencia en las herramientas de detección de intrusos y virus

Correo electrónico

Fuego, inundación,

RECURSOS Y METODOLOGÍAS DISPONIBLES PARA CONTRARRESTAR LAS AMENAZAS:

Normas (ISO, IEEE, ITU, CMM, COSO, COBIT, ITIL y otras.

Herramientas: Magerit...)

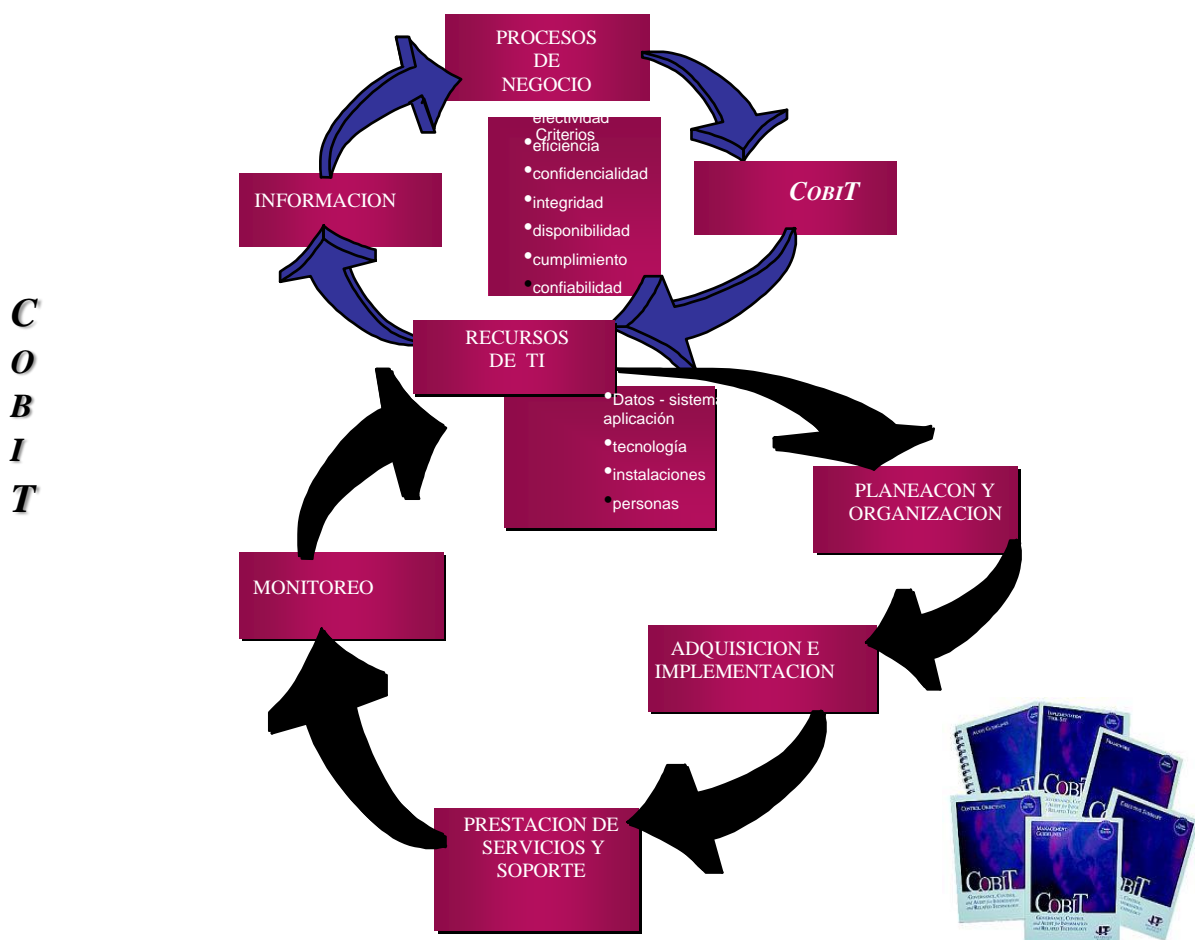
Productos (PKI, SSL, VPN, cortafuegos, IDS,...)

Soluciones de software (gestión, operación y el control).

Servicios de seguridad.

Los siguientes gráficos muestran la estructura de COBIT (RB 17) e ITIL, biblioteca de mejores prácticas para la gestión de la información de TI.

Mejores Prácticas: COBIT

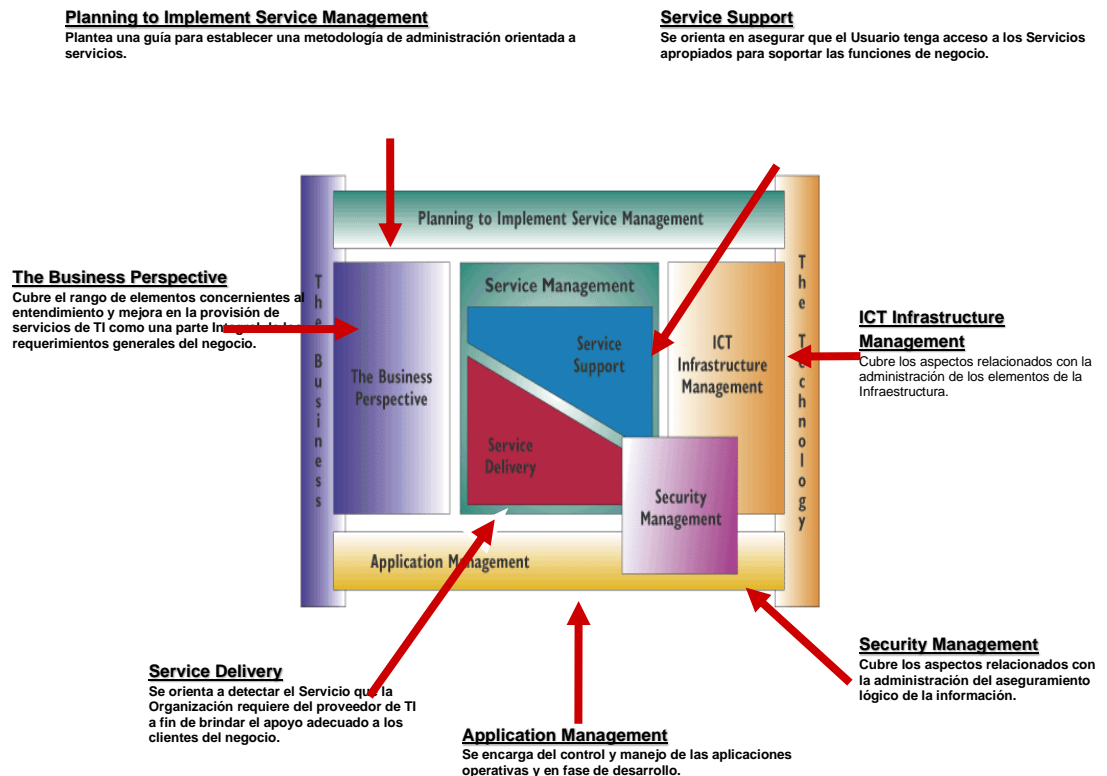


Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

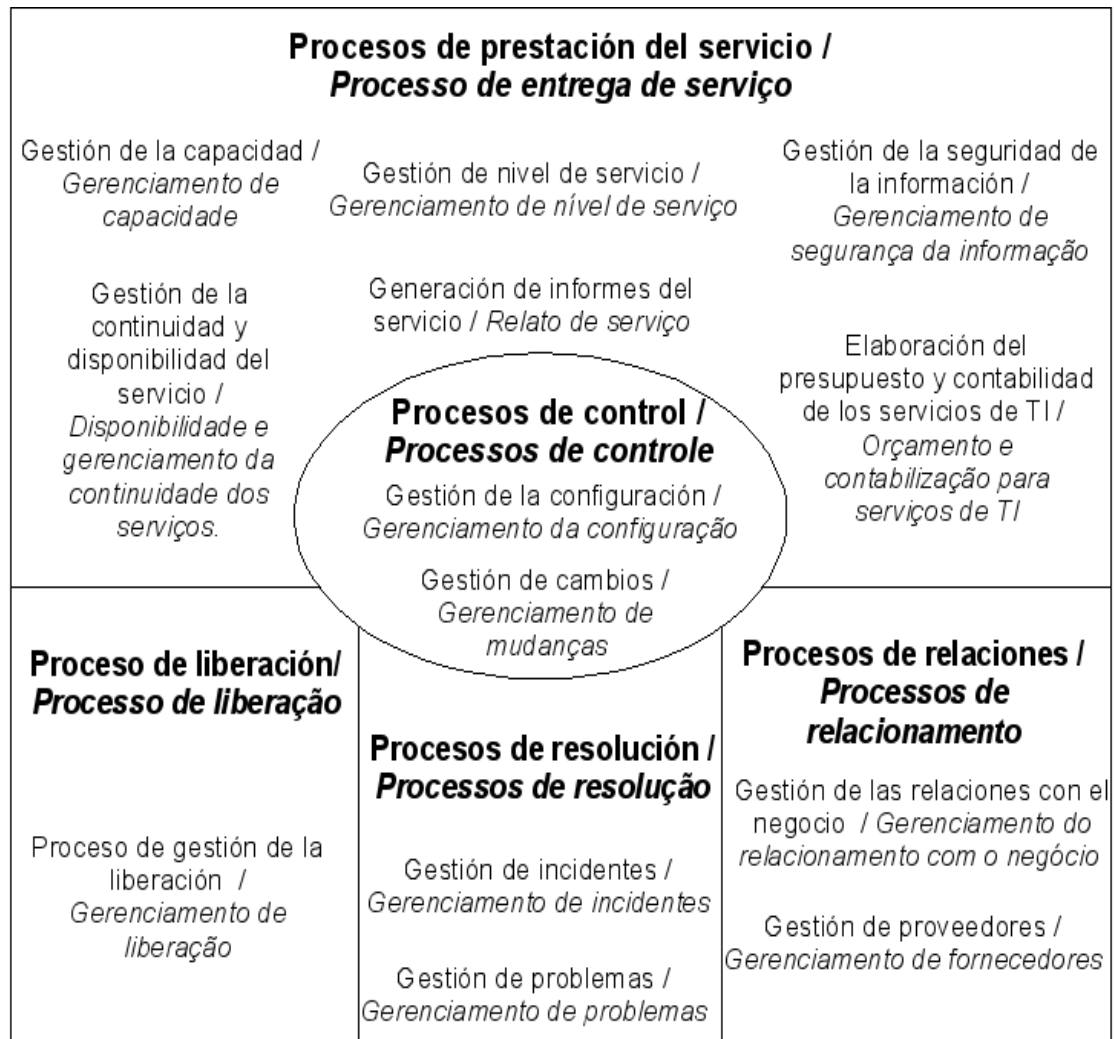
ITIL – Biblioteca de mejores prácticas para gestionar La tecnología de la información.

Que es ITIL?



La norma ISO / IEC 20000-1 (RB 18), que certifica la calidad del servicio de Tecnología de la información e incluye gestión de riesgos y la norma ISO / IEC 20000-2 que propone las mejores prácticas para los servicios de TI, brindan un marco de certificación a la implementación de ITIL.

El gráfico siguiente describe la funcionalidad del sistema de gestión de servicios de TI, tomado de la norma Mercosur ISO/IEC 20000-1:



VULNERABILIDADES

Constituyen las debilidades que presenta la organización frente a los riesgos o amenazas que presentan los activos de la información y los procesos clave, las que pueden ser Internas /Externas.

Principales *vulnerabilidades*

Puntos de accesos remotos sin debida protección.

Control inadecuado de acceso a routers.

Cuentas de usuarios con privilegios excesivos.

Aplicaciones.

Falta de políticas de seguridad.

Excesivos mecanismos de control de acceso.

Falta de formación y educación en seguridad.

Fuga de información por SNMP, SMTP, NETBIOS, DNS

Capacidades inadecuadas o inexistentes de login, monitoreo y reacción ante incidentes.

Deficiente administración de los accesos.

Mantener servicios activos en forma inadecuada.

Estructuras inadecuadas (perimetral),

Consecuencias

Robo: dinero, información empresarial relevante, propiedad intelectual, recursos, etc.

Pérdida de productividad; Corrupción de datos, horas extraordinarias, fallas de equipos,..

Pérdidas indirectas; Daños de imagen, pérdida de "confianza",..

Exposición legal; incumplimiento de contrato, de compromisos de confidencialidad, ilegalidad de actividades a través de los Sistemas

Tendencia

Globalización de mercados e institucional.

La infraestructura Internet, millones de dispositivos non-stop...y el crecimiento explosivo.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Delimitación confusa en los b2b, c2b...

La competitividad y los plazos de lanzamiento e innovación de productos y servicios.

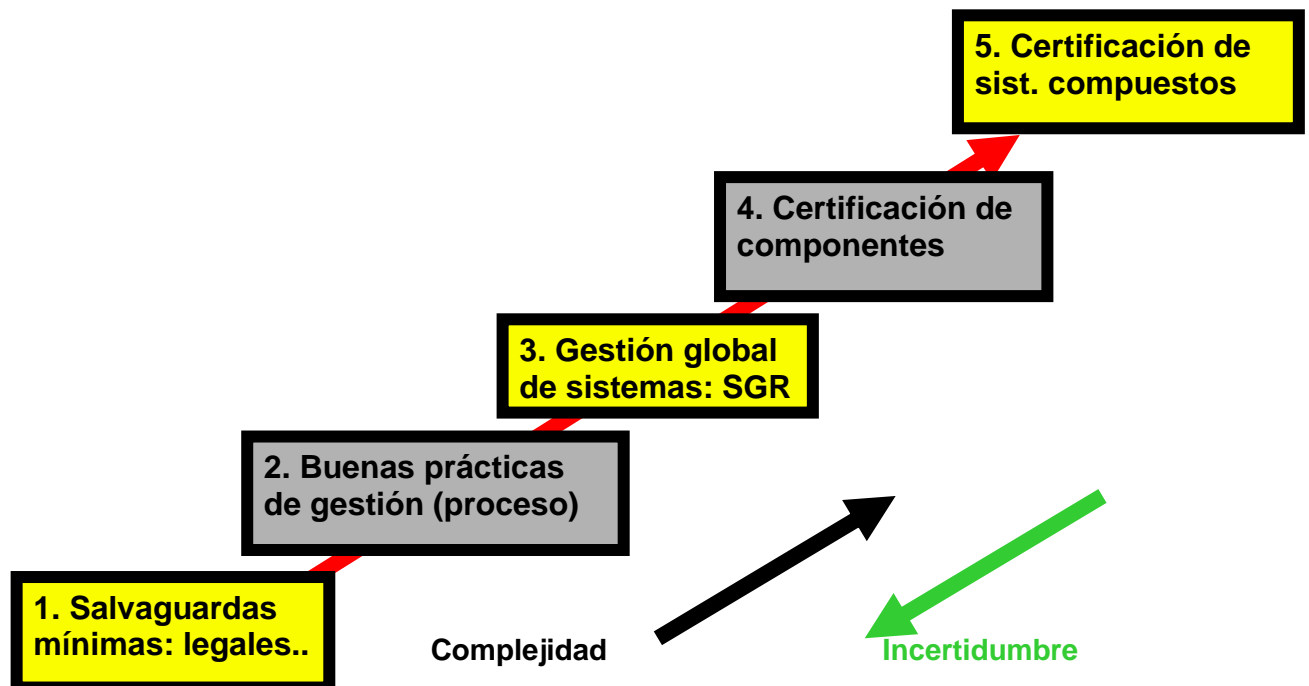
La infraestructura informática (propietario/libre)

DESCRIPCIÓN DE SOLUCIONES DE GESTIÓN DE RIESGOS Y PLANES BASADO EN EL MODELO DE ANÁLISIS DE PROCESOS.

Analizando los niveles de madurez de la gestión de la seguridad de la información, el nivel II establece la necesidad de gestionar la misma en base a procesos, tal como lo describe el siguiente cuadro:

MODELO DE MADUREZ DE LA SEGURIDAD

Las entidades pueden organizar su estrategia y política de seguridad en forma de 'escalones' para mejorar su nivel progresivamente



Estableciendo un sistema de gestión de planes de contingencia y riesgos en base a estudiar los procesos clave de la organización y determinando procesos de gestión de la seguridad, se logra un nivel II de madurez, luego, integrando los sistemas de análisis de procesos para determinar activos de la información, estudiando los

riesgos que presentan estos activos y luego de establecer las salvaguardas, monitorear la aplicación de controles y el estado de cobertura de los riesgos, se puede alcanzar un nivel III.

La base del diseño presentado es la realización del análisis de riesgos y definición de salvaguardas para los procesos clave de la organización esto es, analizar los procesos de gestión estableciendo aquellos denominados claves que permiten la operación normal del flujo de trabajo organizacional.

La propuesta de la tesis es encontrar los riesgos de los activos de información mediante un proyecto basado en el análisis de los procesos de negocio claves De la organización, considerando proceso el diagrama siguiente:

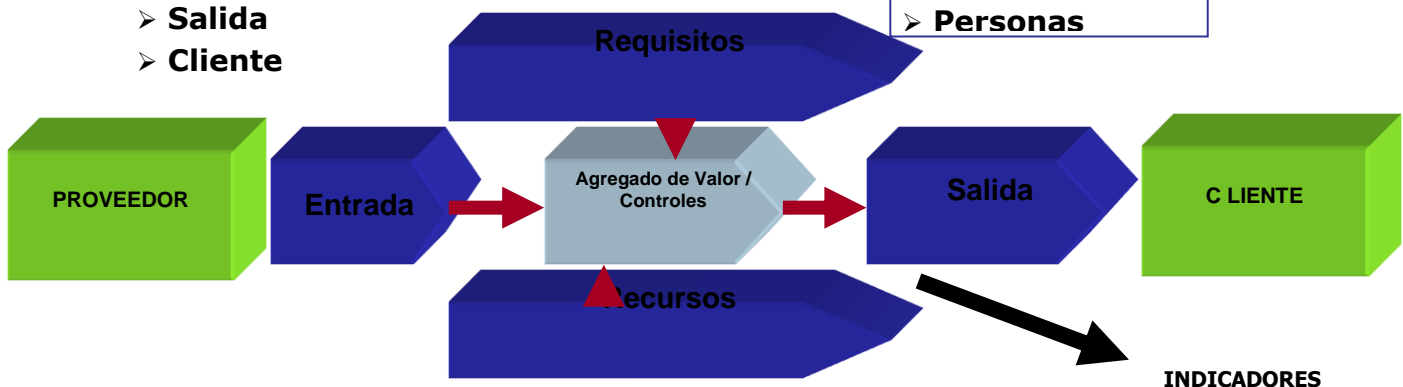
MODELO DE PROCESOS:

Elementos:

- **Proveedor**
- **Entrada**
- **Requisitos**
 - **Actividades o tareas que agregan**
- **Salida**
- **Cliente**

Recursos:

- **Materiales**
- **Herramientas**
- **know-how**
- **Personas**



Los procesos muestran la red de actividades a través de toda la organización, generalmente tienen un dueño o responsable, se diferencian de los procedimientos según lo que se muestra a continuación:

Diferencia entre Procedimiento y Proceso

Procedimiento

Se orientan por operaciones y/o por la norma.
 Se documentan en instrucciones de procedimiento

Proceso

Se orientan por la generación de valor
 Se documentan en descripciones de procesos

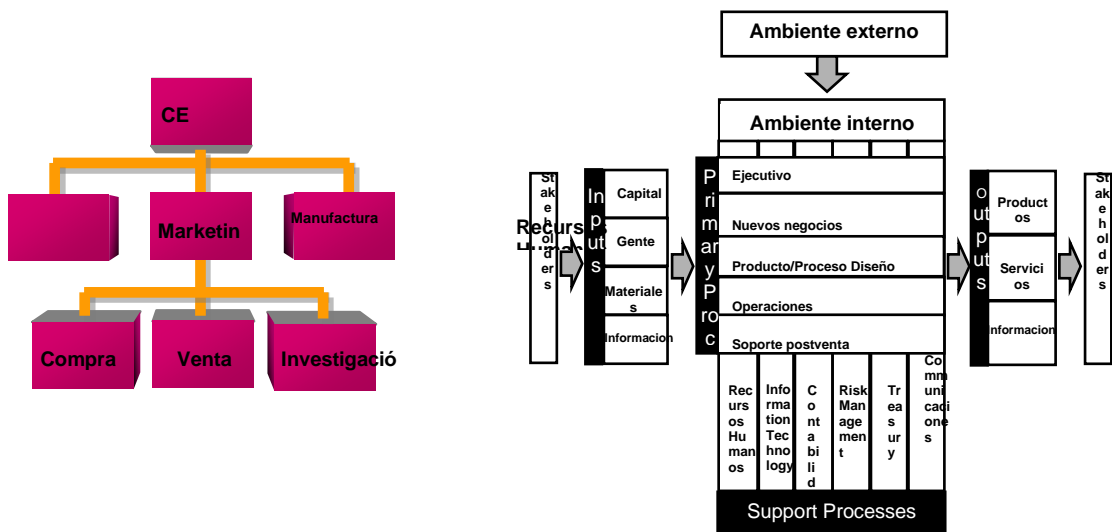
Contenidos:

- Objeto/ Campo de aplicación
- Responsabilidades
- Ejecutores
- Instalaciones
- Desarrollo (Event. Flujoograma)
- Documentación
- Registros

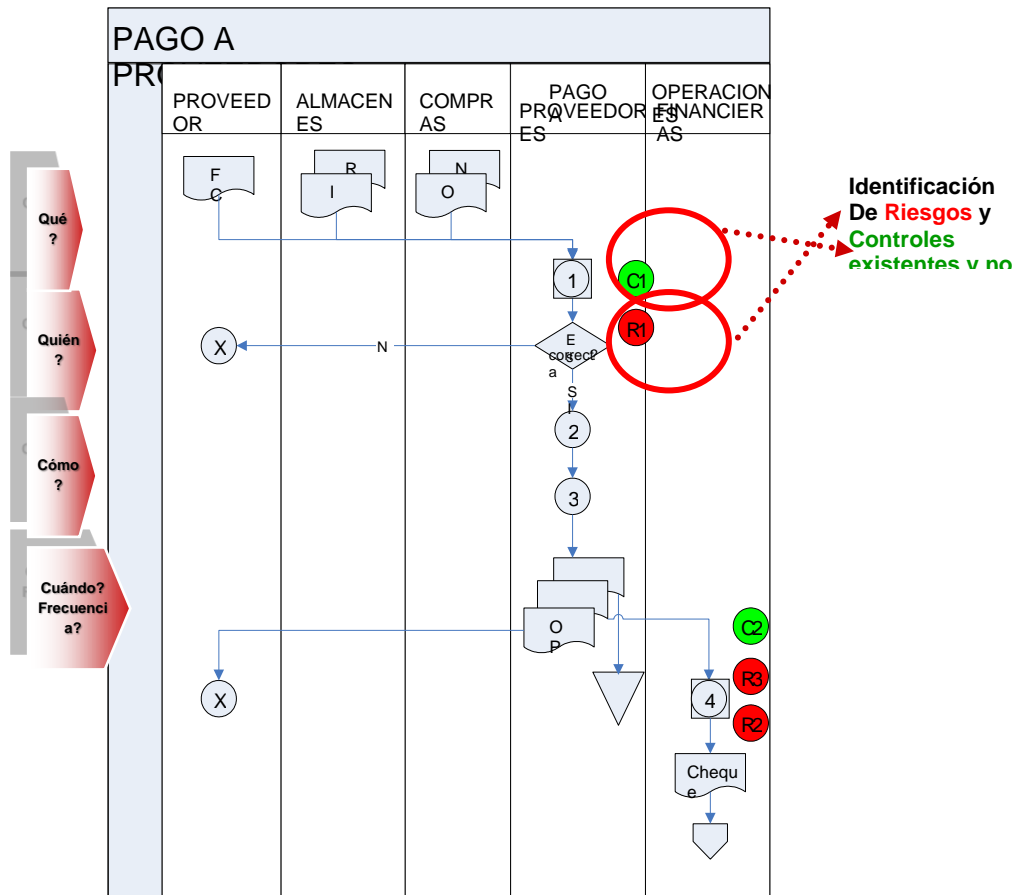
Contenidos:

- Descripción del desarrollo
- Dueño del proceso
- Cliente del proceso
- Proveedor del proceso
- Objetivos del proceso
- Indicadores
 - Cuantitativos /cualitativos
- Marco de condiciones
- Acciones de mejora

Vistas de función y proceso



Ejemplo de proceso:



Para aplicar las ayudas que brindan estos sistemas Web es necesario contar un el auxilio de una herramienta de modelización de procesos que facilite la identificación de niveles de abstracción y permita asignar responsables a las funciones y actividades dentro de un proceso para designar los denominados dueños de proceso, dueños de función y dueños de riesgos.

Un ejemplo de tales herramientas es la plataforma ARIS TOOLSET, de IDS Scheer AG (RB 9).

Otro posible método de modelización de procesos consiste en utilizar alguna herramienta para modelar Diagramas de actividad en el lenguaje UML, como por ejemplo JUDE Community (RB 14) o Enterprise Architect.

Por otro lado, cada función dentro de un modelo de proceso, tiene asociados activos de la información (archivos, bases de datos, transacciones, aplicaciones de software) que también deberán tener designados los dueños de esos activos.

Las funciones y actividades de los procesos deben tener identificados los riesgos para determinar cuales son los controles que debe aplicar y gestionar el dueño del proceso.

Los siguientes son ejemplos de procesos modelizados con ARIS TOOLSET en el proyecto de gestión de riesgos y auditorias de controles realizado durante 2004, 2005 y 2006 por el autor de la Tesis, para la empresa Siemens en Latinoamérica.

En dicho proyecto, se aplicó la metodología planteada en la tesis mediante la definición de los procesos clave, el establecimiento de un Framework de modelización de procesos, con indicación de los riesgos en los mismos, determinando los controles a implementar y la utilización de un sistema de auditoria para la verificación de la realización de controles en los procesos que incluyen riesgos.

Se relavaron los procesos de la organización, se determinaron los denominados críticos, se modelaron y se incluyeron objetos de control sobre las funciones que presentaban riesgos, luego se realizó una verificación de consistencia de los procesos modelados y documentados de común acuerdo con los usuarios y responsables de los sistemas estudiados.

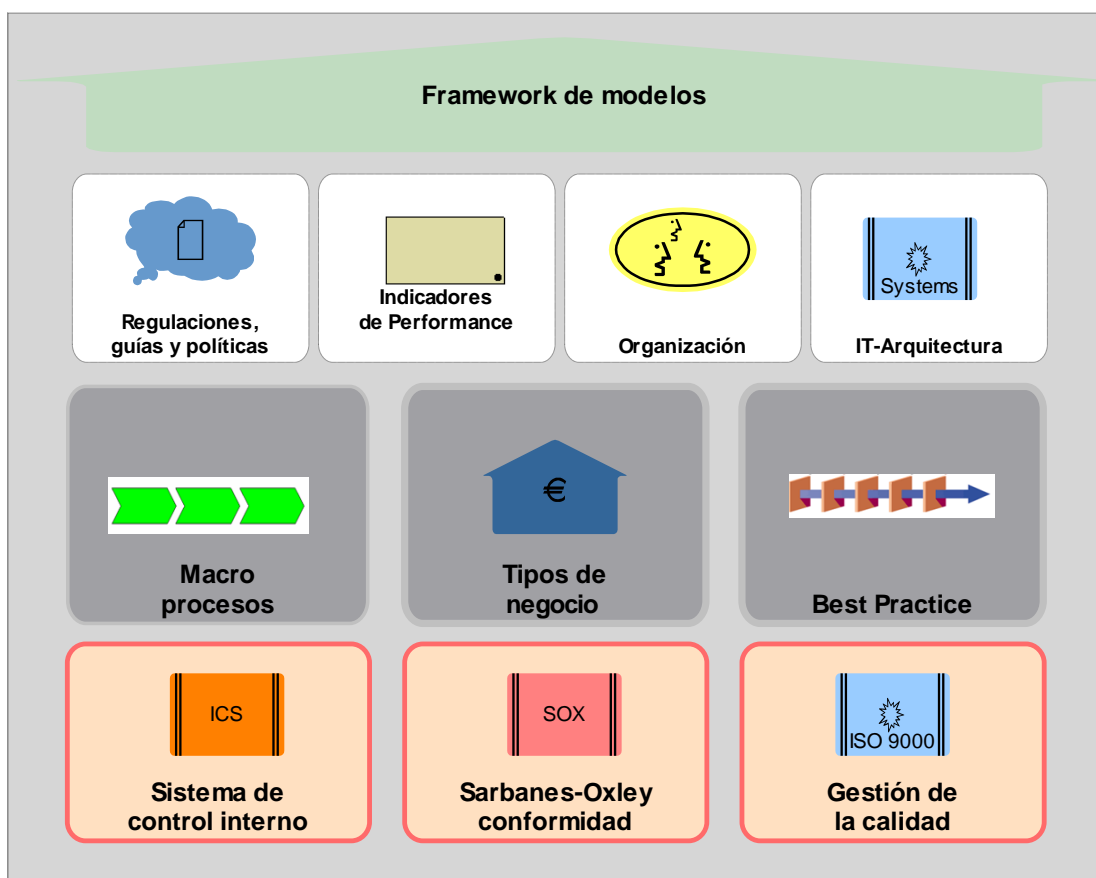
A continuación, se describen los principales conceptos utilizados en el sistema implementado:

Normas de modelización de procesos – ejemplos utilizando ARIS TOOLSET como software de modelización

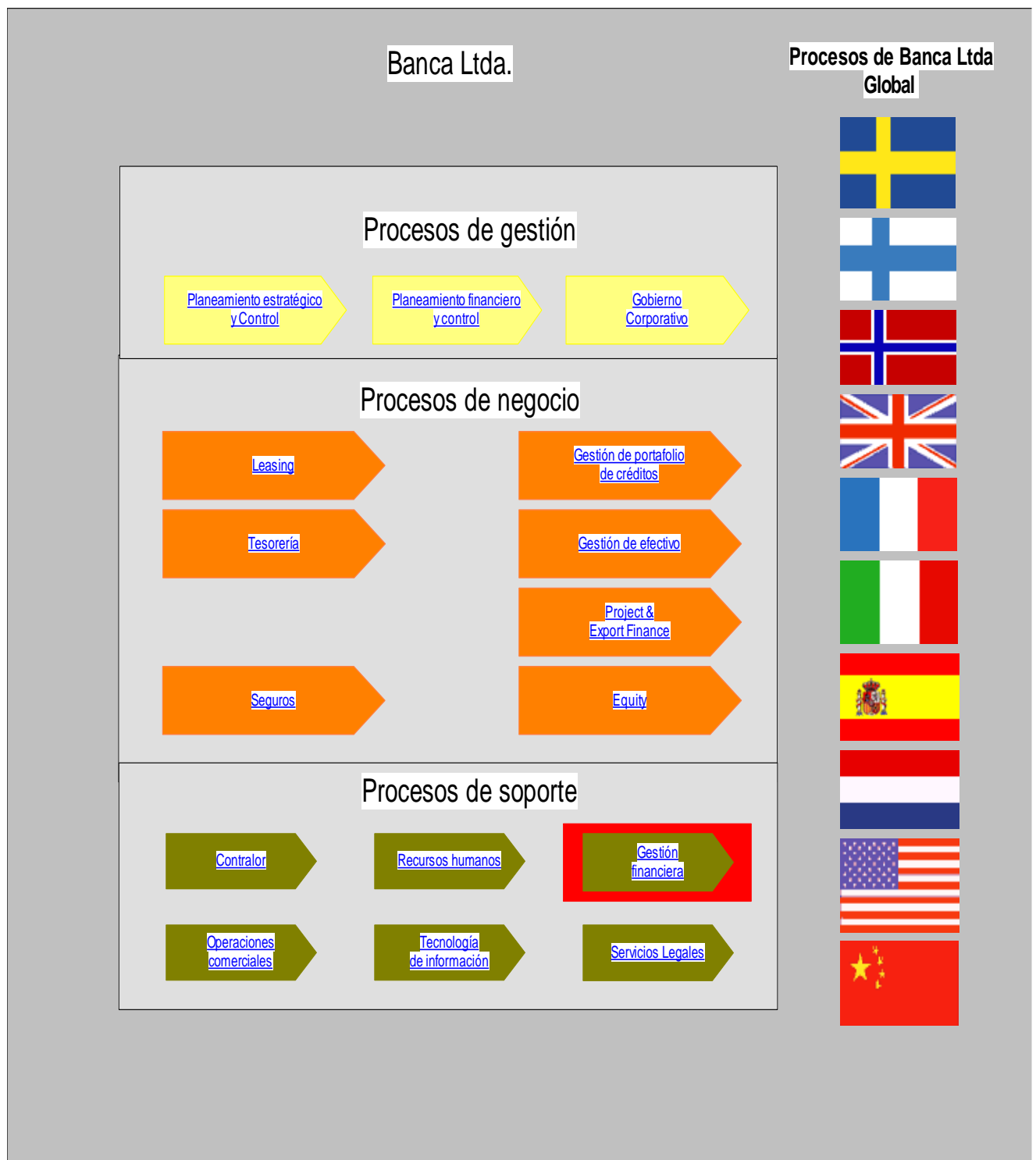
Los objetos que se presentan denominados SOX-control son los que se modelan para indicar que existe definido un control ante un eventual riesgo.

Ejemplo de niveles de procesos claves en la organización

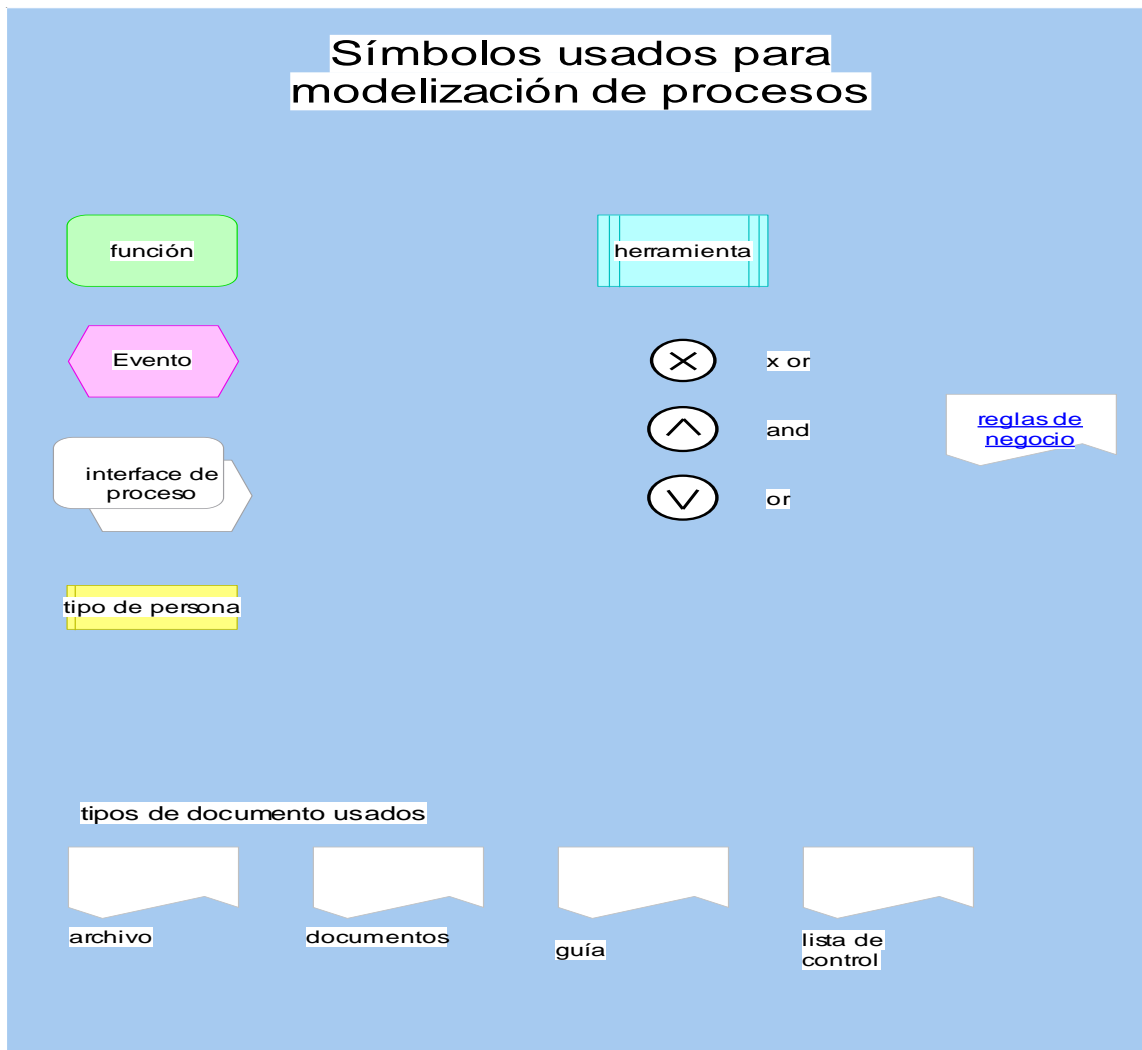
Framework ejemplo de modelización de procesos



Ejemplo de aplicación del Framework

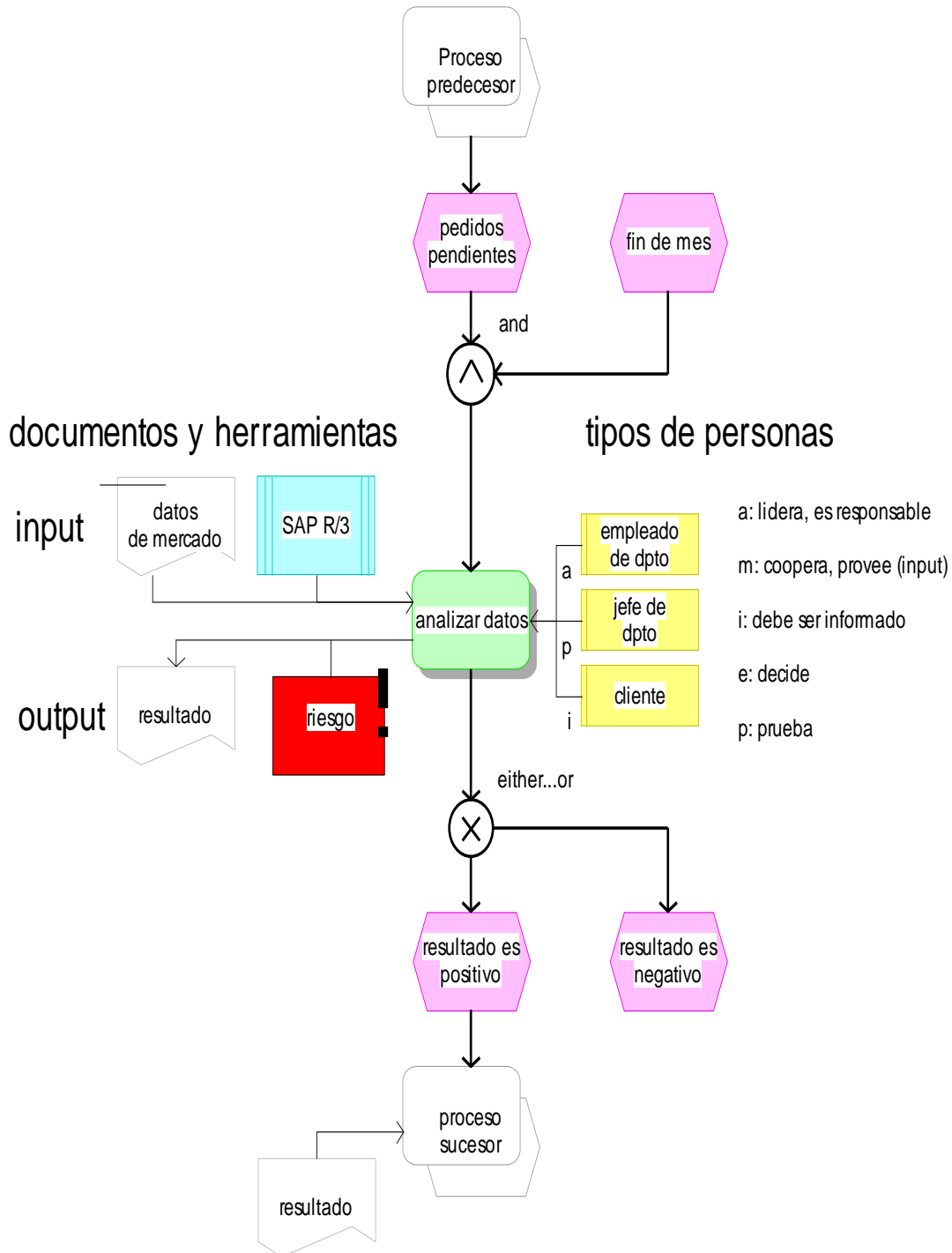


Reglas de modelización de procesos

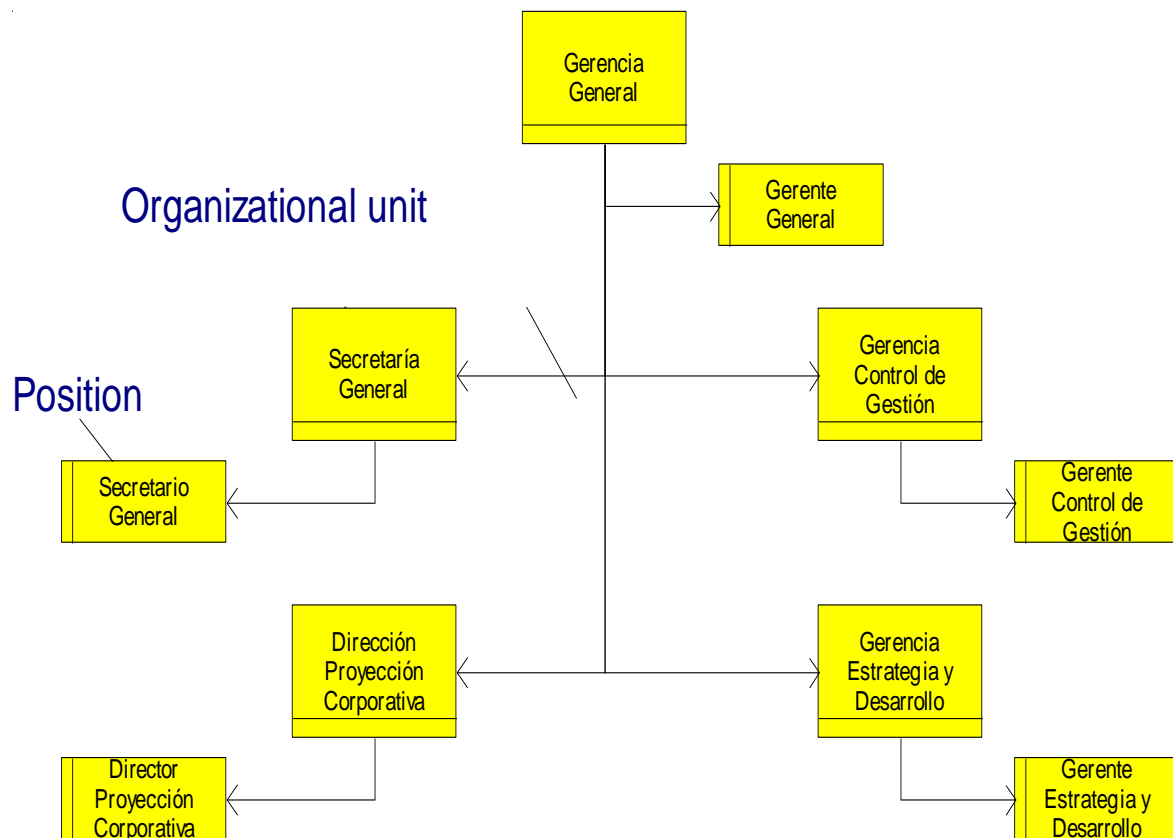


Ejemplo de modelo de proceso

Flujo de proceso

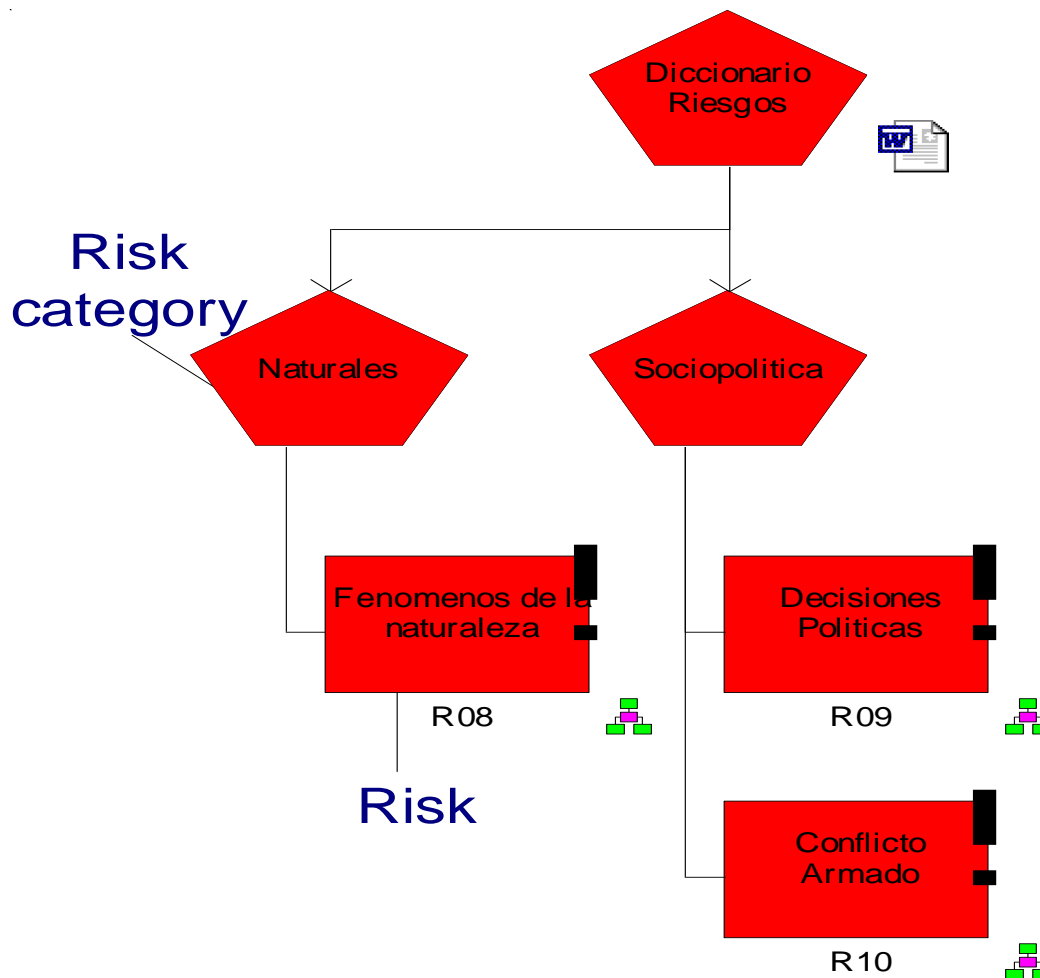


Estructura de gestión de auditorías de proceso de gestión de controles

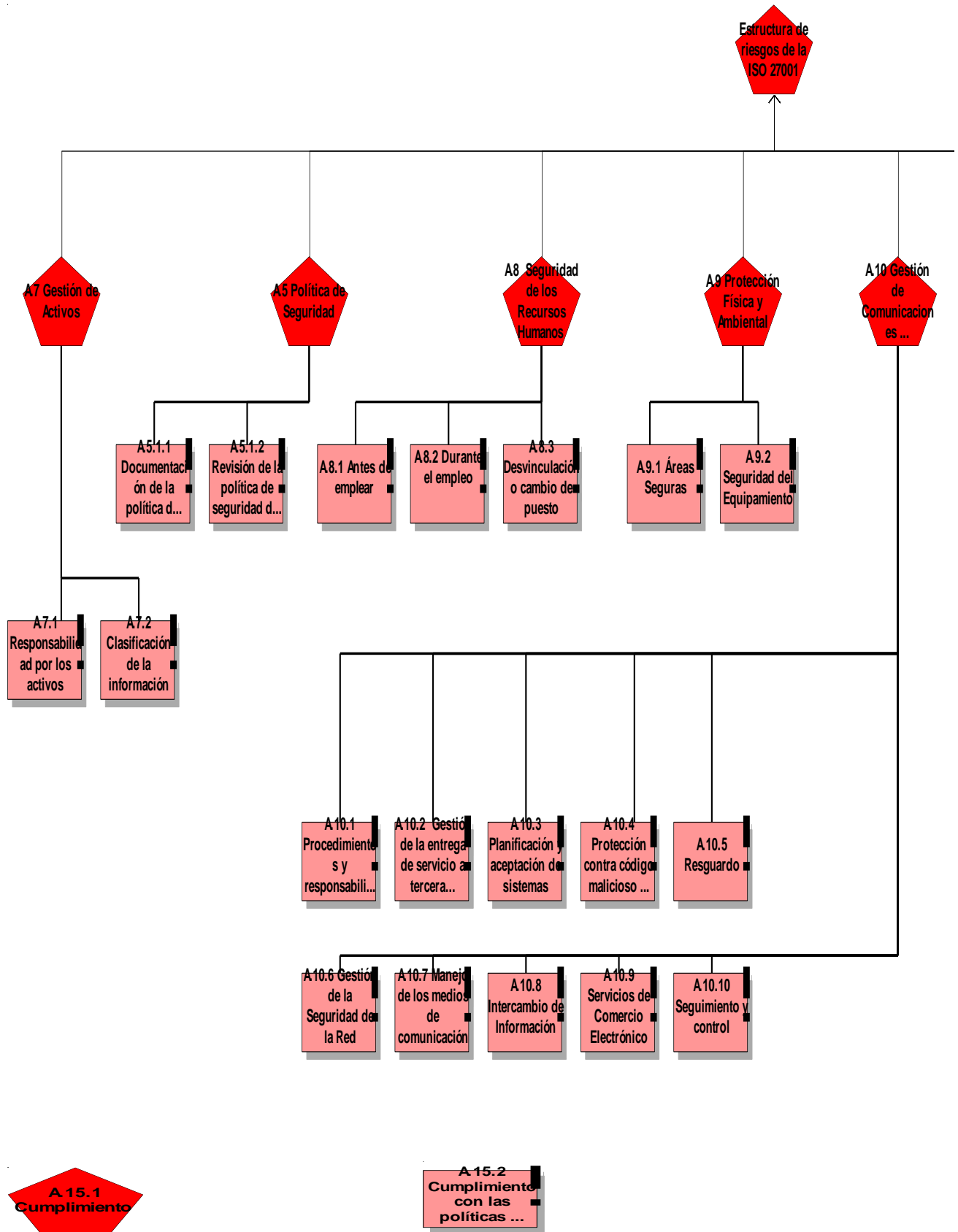


Ejemplos de modelos de procesos realizados en ARIS TOOLSET, en el proyecto de implementación del sistema de auditorías de controles de riesgos en Siemens durante los años 2004 / 2005, para cumplimentar la Ley Sarbanes-Oxley.

Ej.: SOX Riesgos y Controles

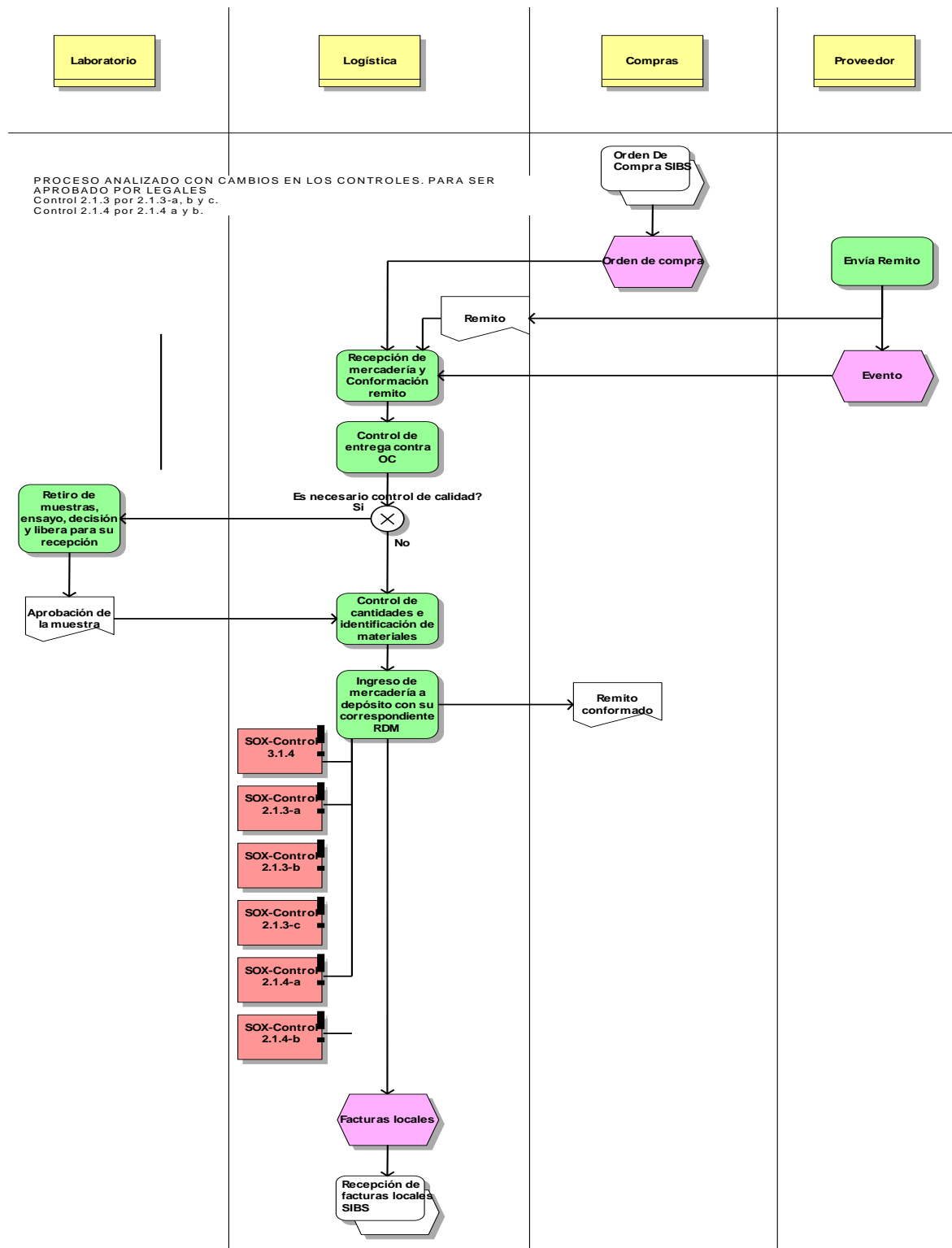


Se detalla a continuación un árbol parcial de categorías de riesgos basados en ISO 27001:

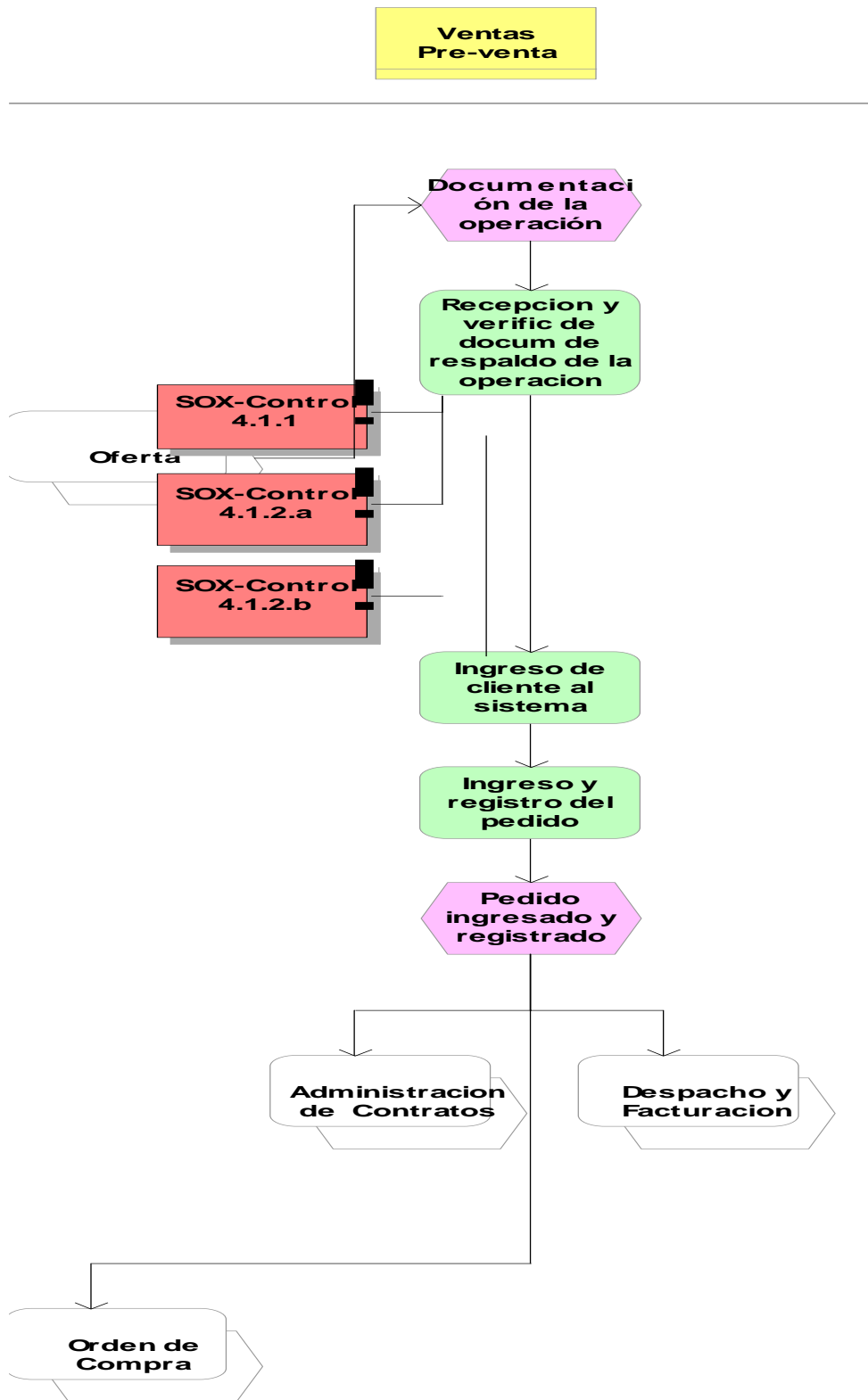


Categoría de riesgo **Riesgo**

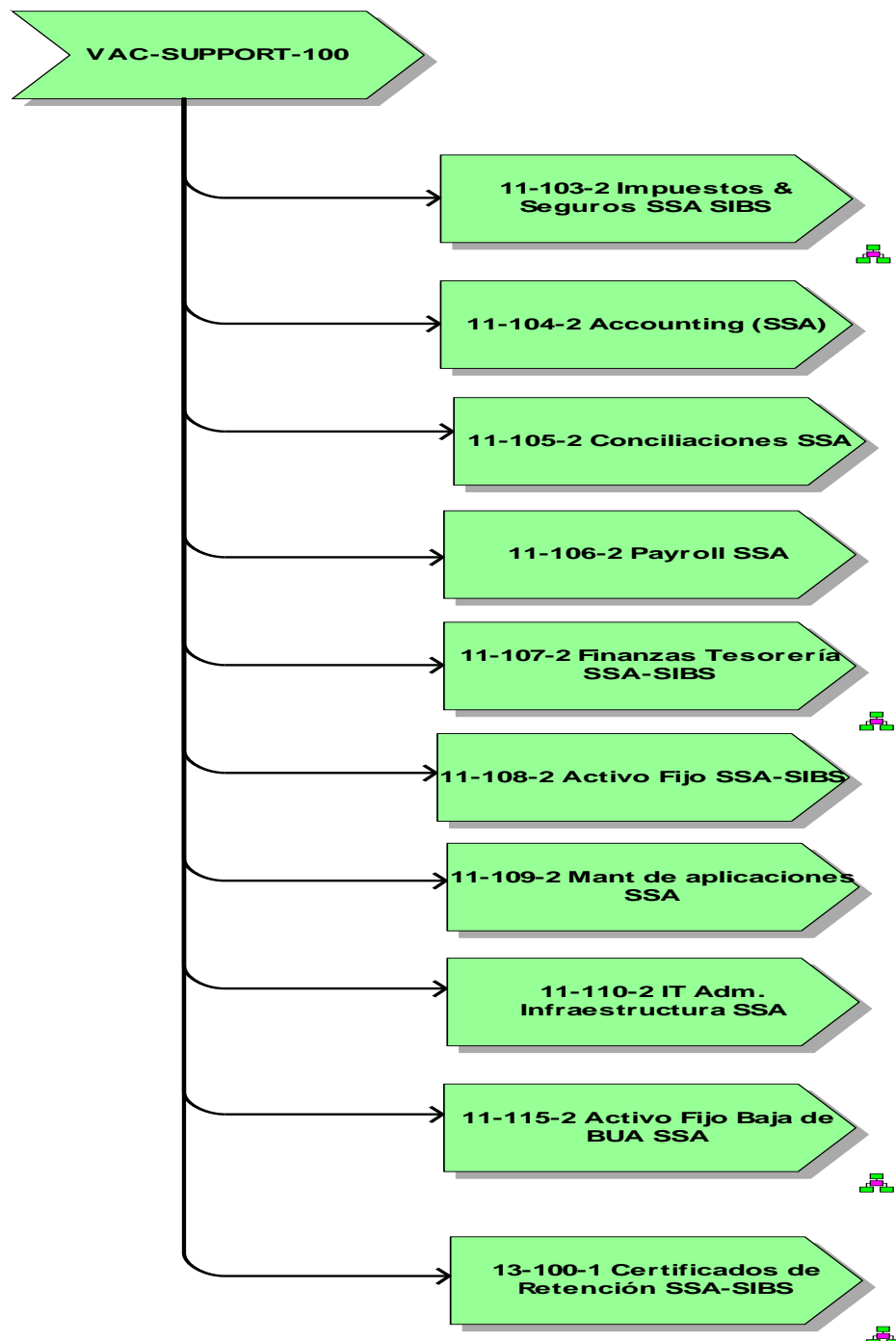
Proceso 13-106-1- PROVEEDORES - Recepción de Mercadería SIBS



Proceso 8-108-2- DELIVERY-PRODUCTOS Y SERVICIOS-Ingreso de Pedido (SSA)

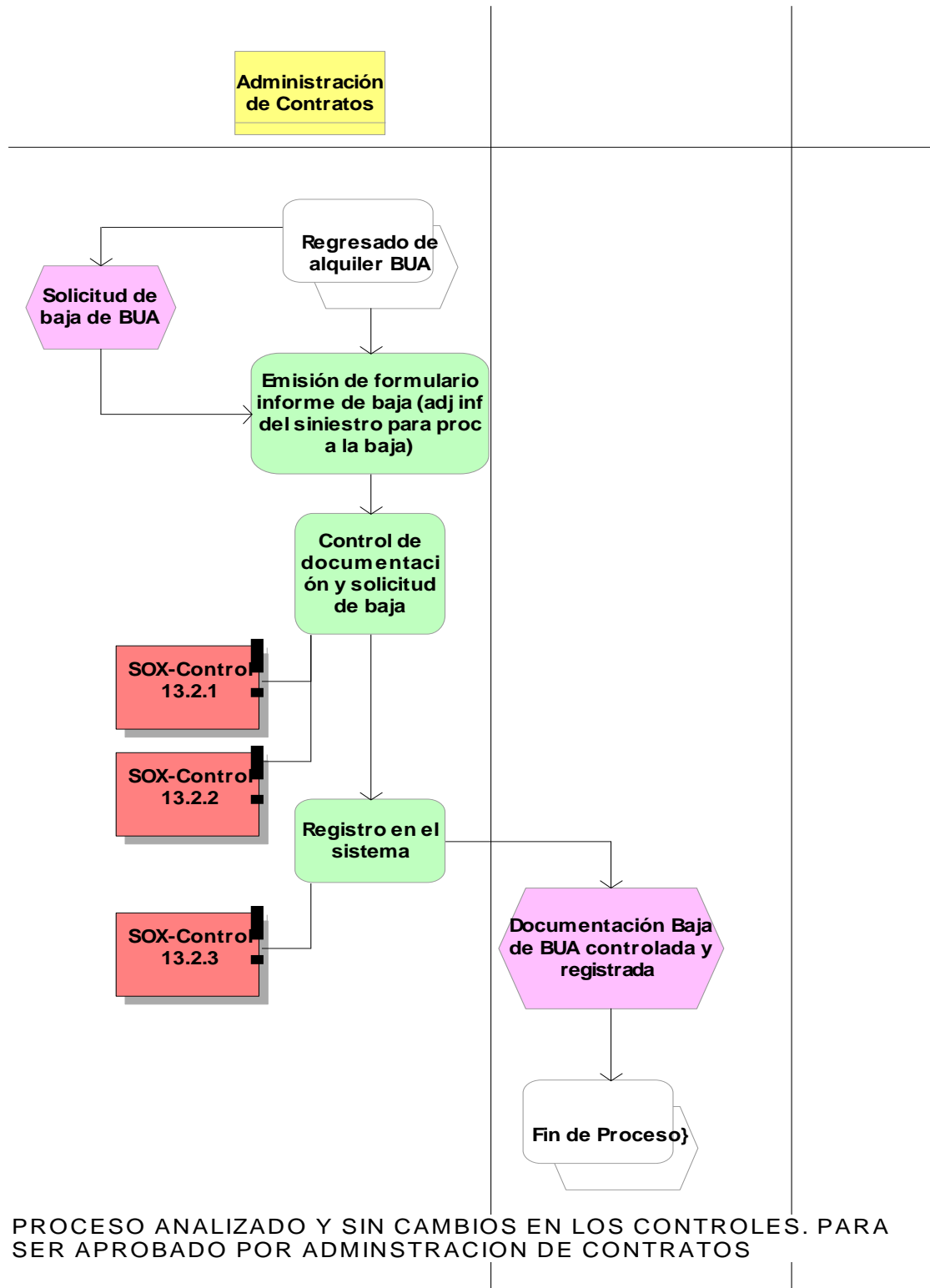


Modelo de cadena de valor con procesos de nivel inferior

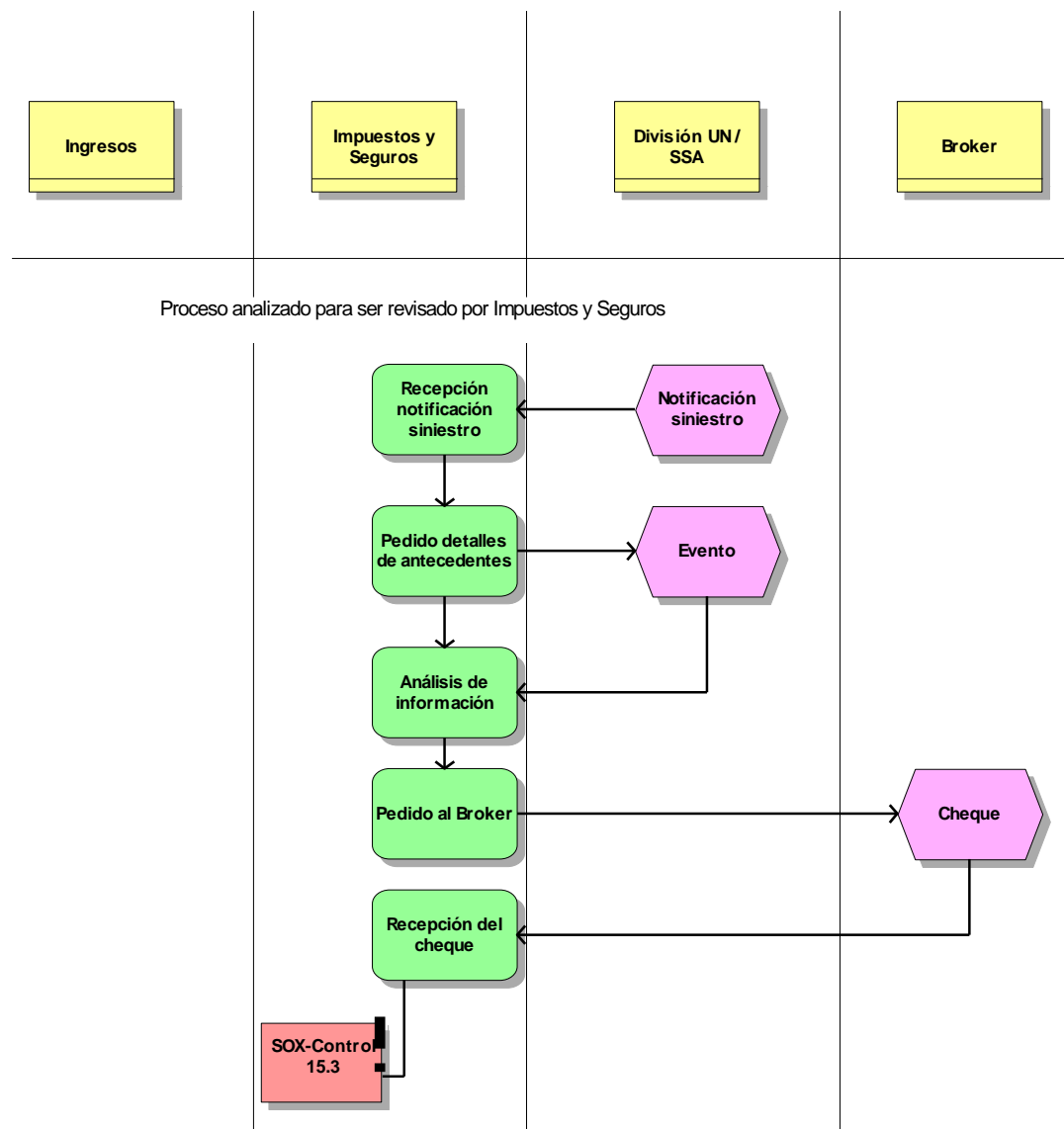


El símbolo de tres funciones significa que haciendo doble clic en el mismo se abrirá un modelo de detalle del macro proceso planteado.

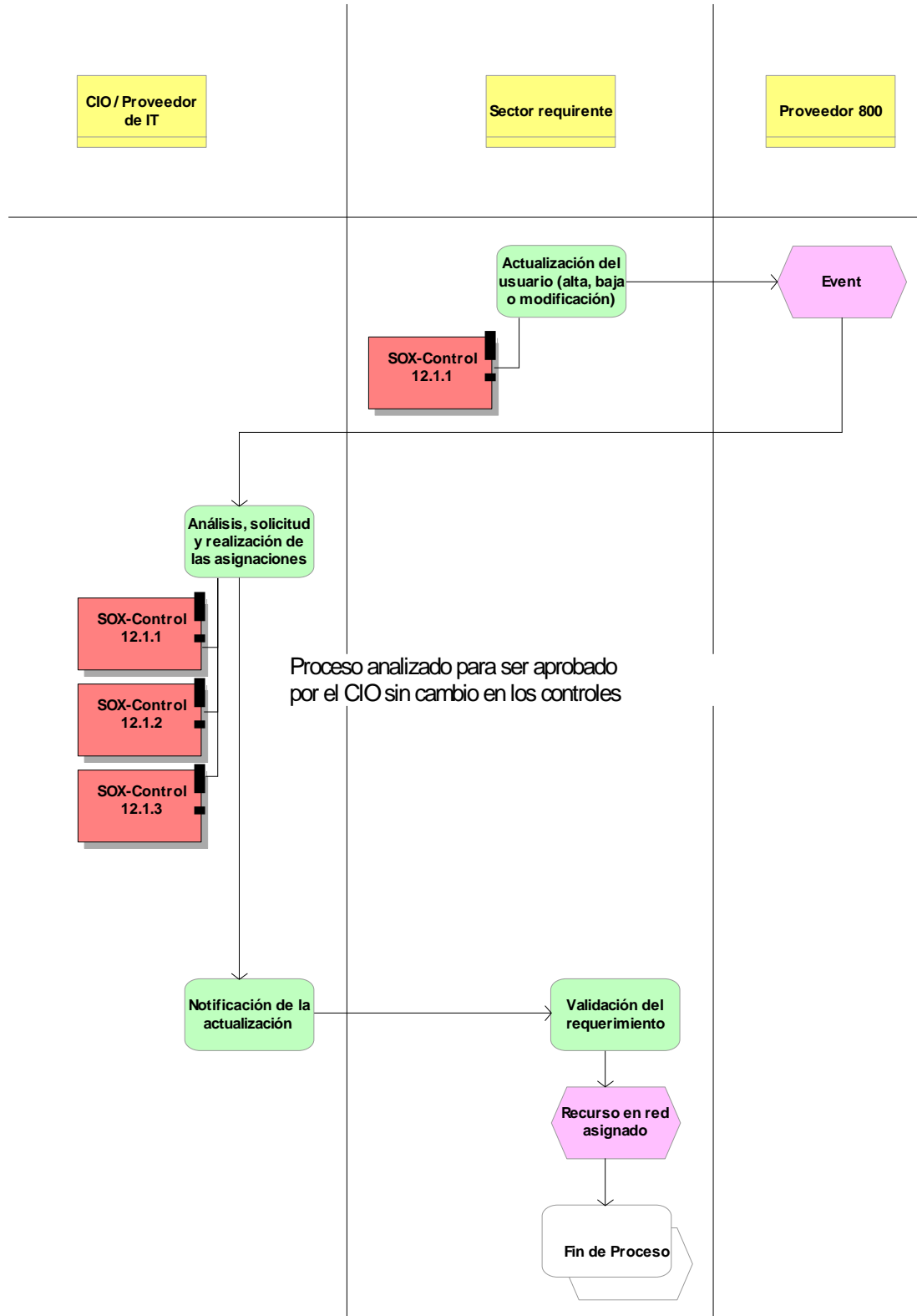
Proceso de detalle activo fijo baja de activo - BUA SSA



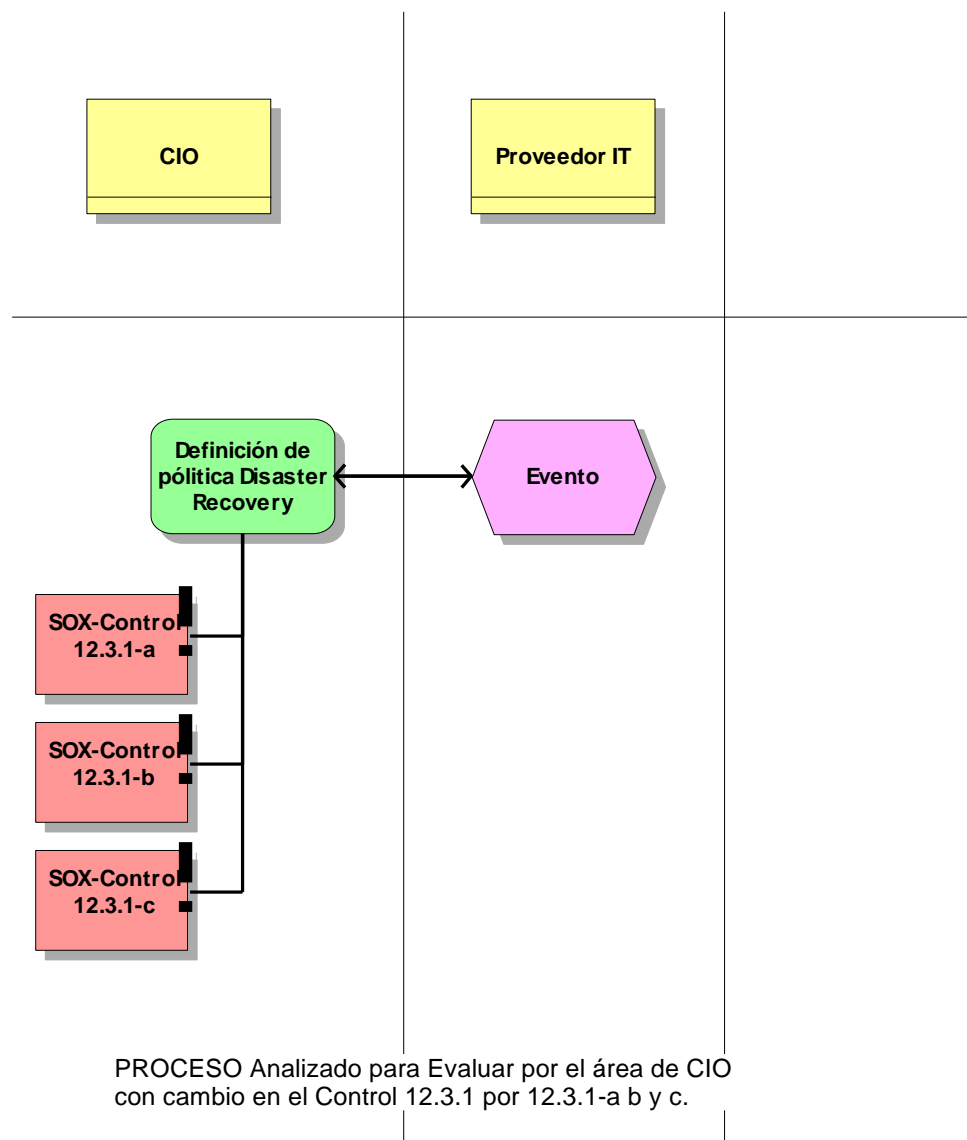
Proceso de detalle impuestos y seguros SSA SIBS



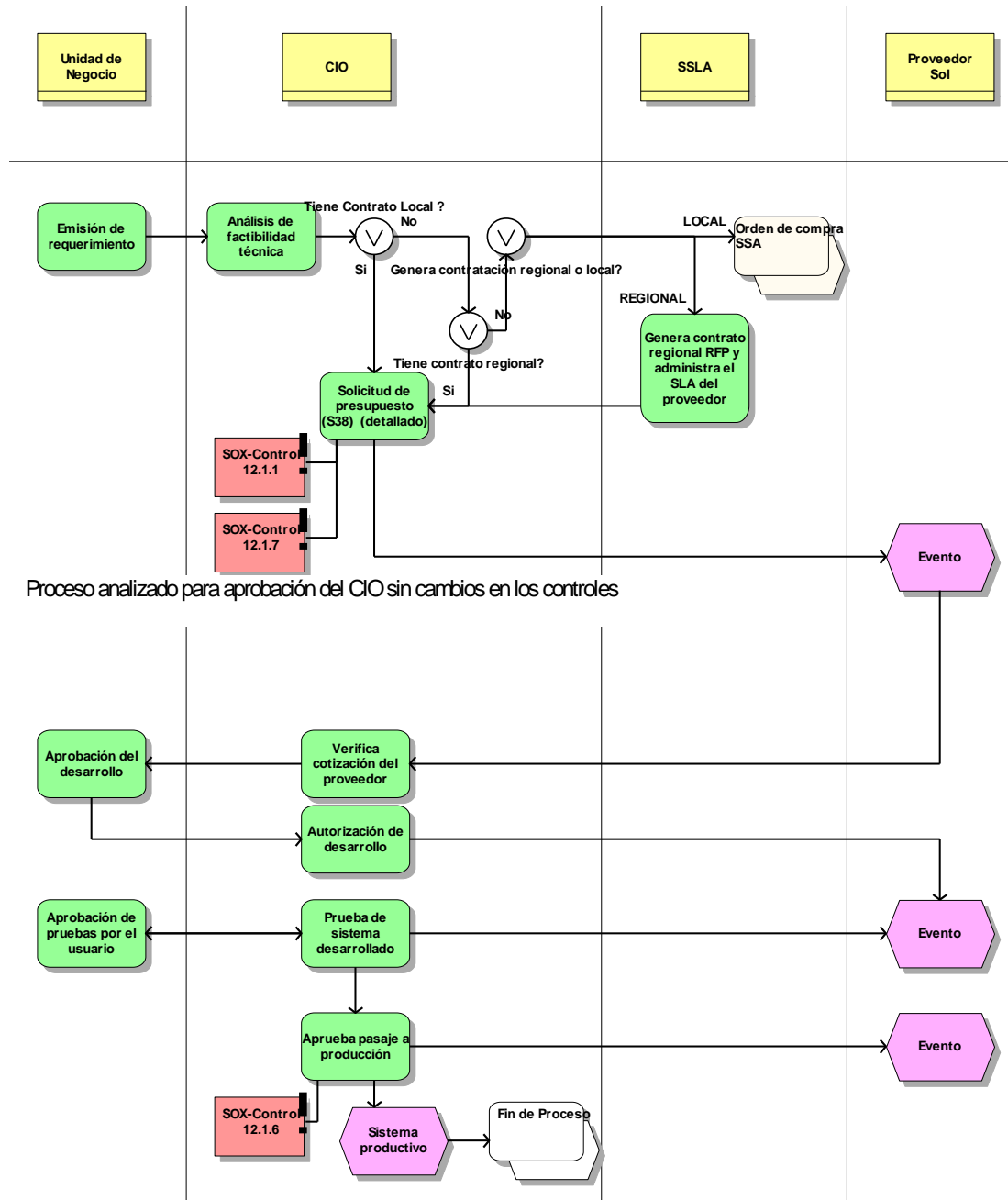
Procesos IT 11-110-2 PROCESOS DE SOPORTE - IT - Creación y asignación de recursos en red (SSA)



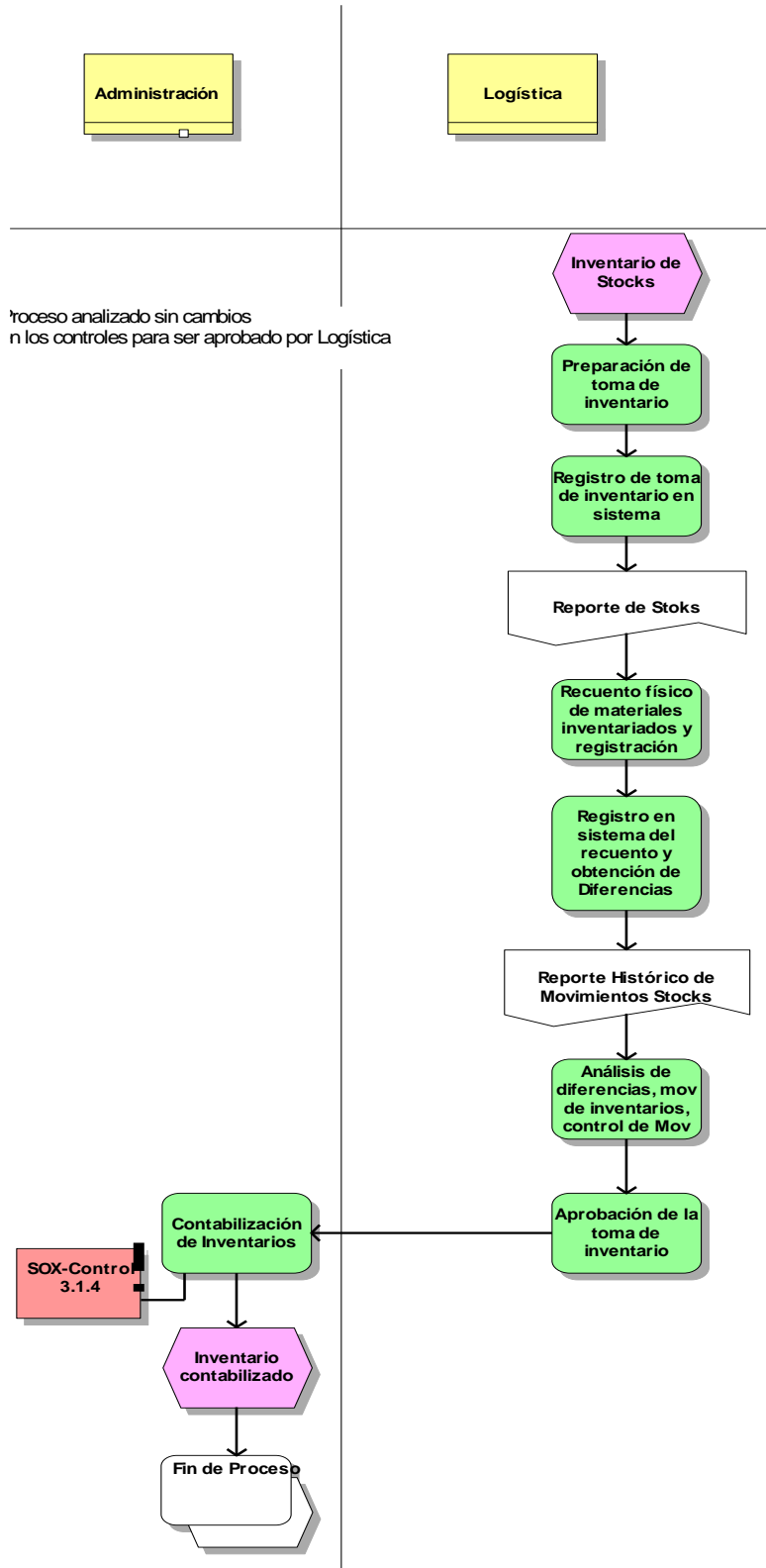
11-110-2-PROCESOS DE SOPORTE - IT - Contingency & Disaster Recovery (SSA)



11-109-2-PROCESOS DE SOPORTE - IT - Atención de requerimientos UN (SSA)

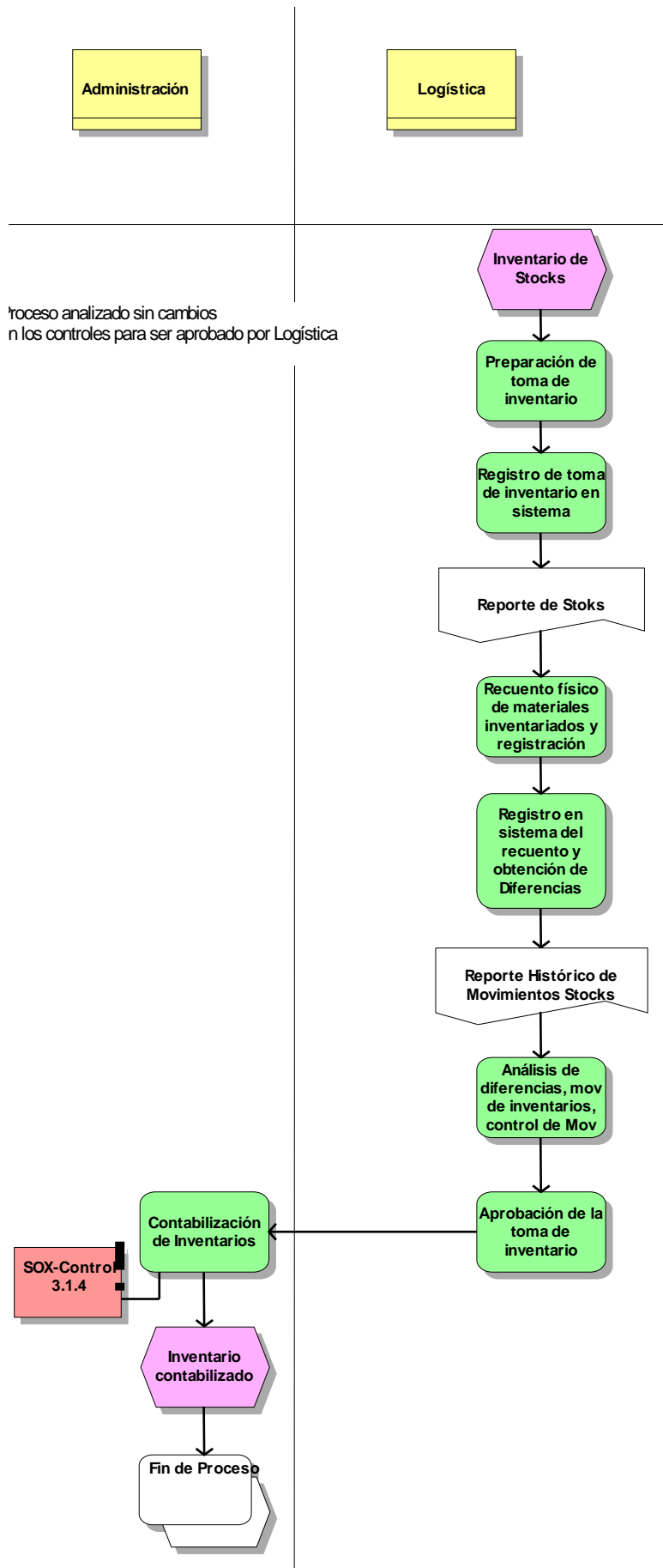


Proceso 13-105-1-A&D-SCM-SOURCE - MAKE - Costeo de inventarios (SIBS)

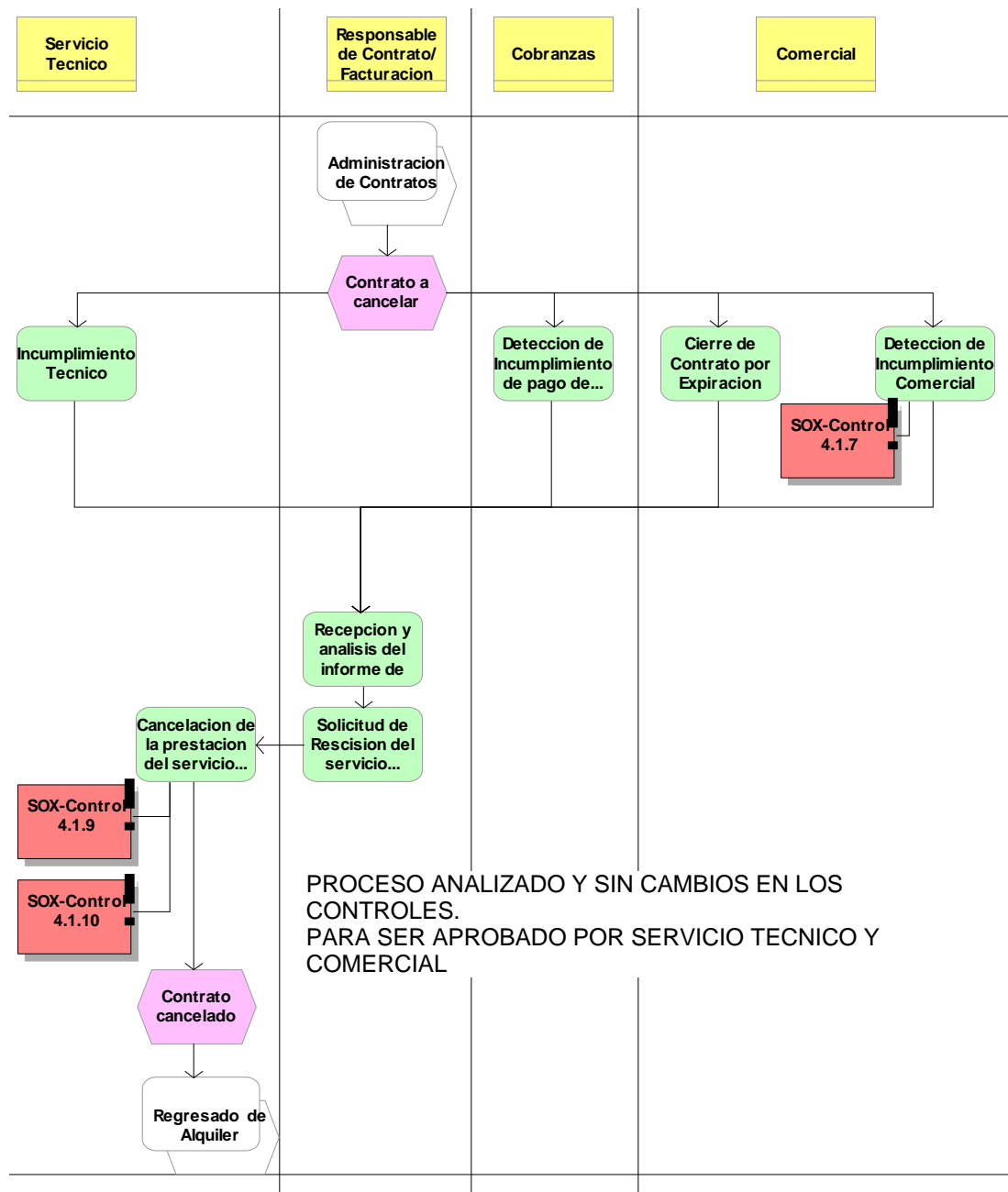


Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

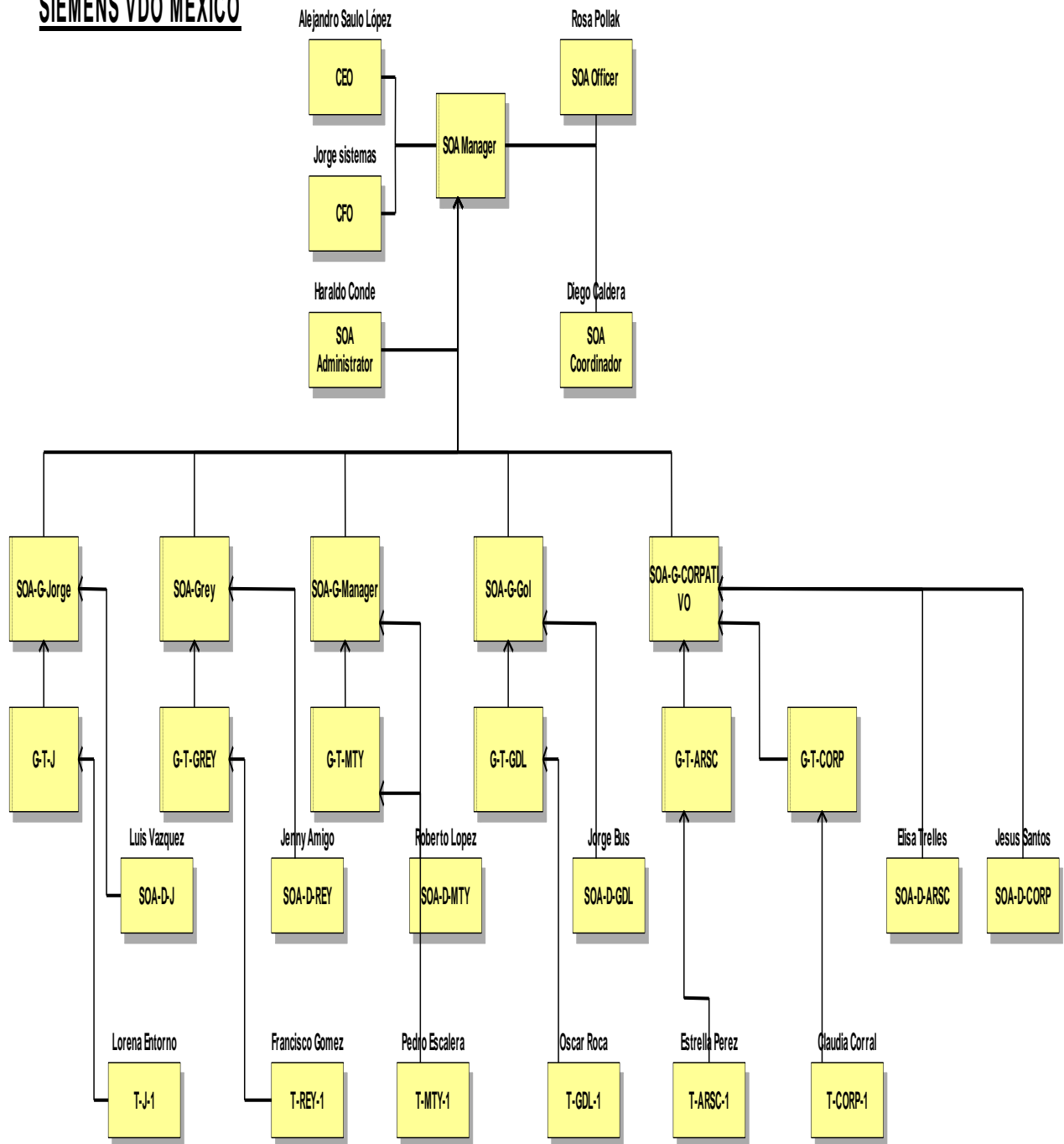


Proceso 8-108-2-DELIVERY PRODUCTOS Y SERVICIOS-Rescisión/ Cierre de Contrato (SSA)-COL



Estructura orgánica del grupo de testers que realizan la auditoria de controles:

ESTRUCTURA DE TEST DE SIEMENS VDO MEXICO



Como se describe en los modelos presentados, cada proceso incluye funciones algunas de las cuales presentan riesgos los que deben tener vinculados procedimientos de control para mitigar, evitar o convivir con el riesgo.

El proyecto incluyó una reingeniería por procesos para determinar los procesos clave y aquellos que deberían ser modelados y documentados por tener actividades o funciones bajo riesgo.

Además se implementó un sistema que utilizan los auditores que verificaron el cumplimiento de los procedimientos de control establecidos por el sistema de gestión de riesgos, dejando almacenada su intervención y evidencias.

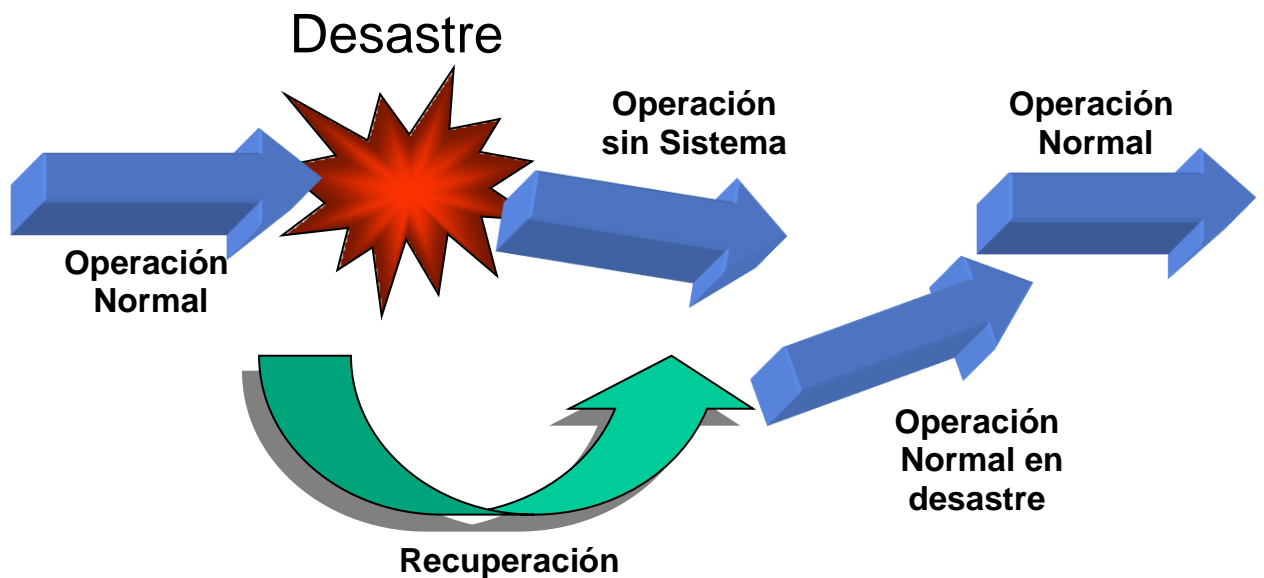
Este sistema del ejemplo de gestión de auditorías de controles es parte del sistema de gestión de riesgos y contingencias de la empresa Siemens a nivel corporativo, implementado en toda la Región Sur por el autor, como Consultor de la empresa IDS Scheer AG, realizando el estudio y capacitación del personal de Siemens de Latinoamérica para la implementación del sistema de gestión de riesgos por procesos y auditoría de controles y fue realizado por el autor de esta tesis, durante los años 2004, 2005 y 2006.

En el capítulo V de la presente tesis, se detalla el Help del sistema con la funcionalidad disponible en la aplicación, necesaria para gestionar controles de soporte a las auditorías de tercera parte de verificación de que los controles implementados para atacar los riesgos son efectivamente realizados.

PLAN DE CONTINGENCIAS

Un Plan de contingencias debe brindar los elementos necesarios para que de ocurrir un desastre la continuidad de la gestión esté garantizada, tal como se muestra a continuación:

Pasos a seguir ante un desastre



En la actualidad existen diversos enfoques metodológicos para abordar proyectos de Planes de contingencia y gestión de riesgos, sin embargo hay tres que se destacan del resto, estos son:

- La **Guía para elaborar Planes de contingencia del NIST, National Institute of Standards and Technology**, del Departamento de Comercio de los Estados Unidos (RB 10).

- **Magerit**, Metodología de análisis y gestión de riesgos de los sistemas de información del Ministerio de administración Pública de España (RB 11).

- La **norma ISO 27001**, requisitos de los sistemas de gestión de la seguridad de la información (RB 12).

Aquí presentamos brevemente estos enfoques de manera sucinta y a modo de luego establecer las ventajas de la metodología por procesos planteada en esta tesis.

El NIST, National Institute of Standards and Technology, del Departamento de Comercio de los Estados Unidos, publicados en Diciembre de 2001, desarrolló una serie de recomendaciones para elaborar la Guía para Planes de Contingencia (RB 10), para Tecnología de Sistemas de Información, en su resumen ejecutivo establece:

La Guía de Planificación de Contingencia para la Tecnología de la Información (TI) de sistemas, proporciona instrucciones, recomendaciones y consideraciones del gobierno de TI para la planificación de la contingencia. La planificación de contingencia se refiere a las medidas para la recuperación de los servicios de emergencia o después de una interrupción del sistema de gestión. Las medidas podrán incluir el traslado de los sistemas de TI y las operaciones a un sitio alternativo, la recuperación de las funciones de TI utilizando el equipo alterno, o el cumplimiento de funciones de TI utilizando métodos manuales. La información presentada en este documento trata de siete tipos de plataforma:

Desktops and portable systems

- Web sites
- Servers
- Local area networks
- Wide area networks
- Distributed systems
- Mainframe systems.

El documento define las siguientes siete etapas de proceso contingencia que una agencia puede aplicar para desarrollar y mantener un programa viable de planificación de contingencia para sus sistemas informáticos. Estos siete pasos se han diseñado para ser integrados en cada etapa del ciclo de vida del desarrollo del sistema.

Elaborar la política de planes de contingencia. Un departamento o área oficial de políticas, proporciona la autoridad y la orientación necesaria para desarrollar un efectivo plan de contingencia.

Realizar el análisis del impacto sobre la gestión de negocio (BIA). La BIA ayuda a identificar y dar prioridad a los sistemas y componentes de TI críticos. Identificar los controles preventivos. Medidas adoptadas para reducir los efectos de las perturbaciones del sistema puede aumentar la disponibilidad del sistema y reducir los costos de la contingencia durante el ciclo de vida.

Elaborar estrategias de recuperación. Basamento de las estrategias de recuperación para garantizar que el sistema puede recuperarse con rapidez y eficacia a raíz de una interrupción.

Desarrollar el plan de contingencia. El plan debe contener una guía detallada y los procedimientos para la restauración de un sistema dañado.

Plan de pruebas y capacitación del personal. En la Planificación de pruebas del plan se identifican las brechas, mientras que la formación del personal se prepara para la activación del plan de recuperación; mejorar el plan de actividades, tanto la eficacia y la gestión global de la preparación.

Mantener el plan. El plan debe ser un documento vivo que se actualiza periódicamente para permanecer al día con mejoras en el sistema.

El documento presenta un formato modelo para el desarrollo de un plan de contingencia de TI. El formato define tres fases que rigen las medidas a ser adoptadas a raíz de una interrupción del sistema.

La fase de Notificación / Activación describe el proceso de notificación al personal a cargo de la recuperación y la realización de una evaluación de los daños. En la fase de recuperación se analizan las medidas adoptadas por la recuperación de equipos y del personal de TI para restaurar las operaciones en un sitio alternativo o la utilización de las capacidades de contingencia. En la fase final, la reconstitución de la operación, se esbozan las medidas adoptadas para devolver el sistema a condiciones normales de funcionamiento.

Si un sistema no puede ser recuperado en el sitio original, en la mayoría de los casos debe ser reubicado en un sitio alternativo para el procesamiento temporal. En la guía de planificación se analizan los distintos tipos de sitios y alternativos con sus respectivas capacidades. Estos sitios son alternativos de la siguiente manera:

- Sitios fríos
- Sitios móviles
- Sitios cálidos
- Sitios calientes
- Sitios reflejados.

El documento del NIST, ofrece recomendaciones específicas de la planificación de contingencia para las siete plataformas de TI. No obstante, varias estrategias o técnicas que nos son comunes a todos los sistemas de TI. Algunas estrategias de contingencia común incluyen las siguientes:

Almacenamiento externo. El Sistema de información debe estar respaldado con regularidad y se almacena afuera en un entorno protegido. En el documento se describen varias técnicas para realizar operaciones de copia de seguridad. Del Sistema operativo, aplicaciones, y datos de aplicación que deben estar respaldados como las bases de datos y sistemas críticos. Licencias de software, configuraciones del sistema, y otros documentos esenciales deben guardarse afuera con la copia de seguridad de datos.

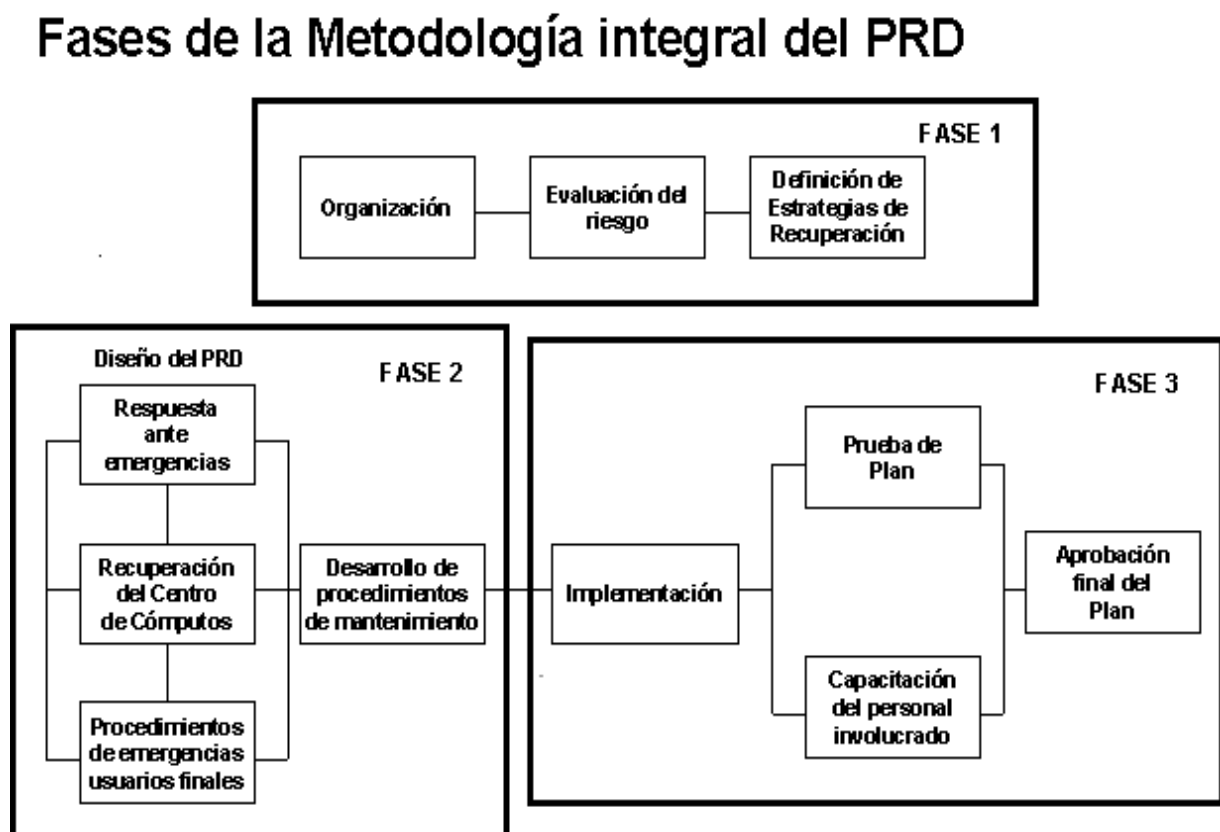
La interoperabilidad. Proporcionar plataformas y configuraciones estándar de sistemas de recuperación para ayudar a reducir los gastos asociados con la adquisición de equipo de sustitución.

Redundancia. El almacenamiento de datos redundantes, las vías de comunicaciones, fuentes de energía, los componentes del sistema para reducir la probabilidad de fallas del sistema. Los costos de la aplicación de capacidades redundantes deben ser sopesados frente a los riesgos de interrupción del sistema.

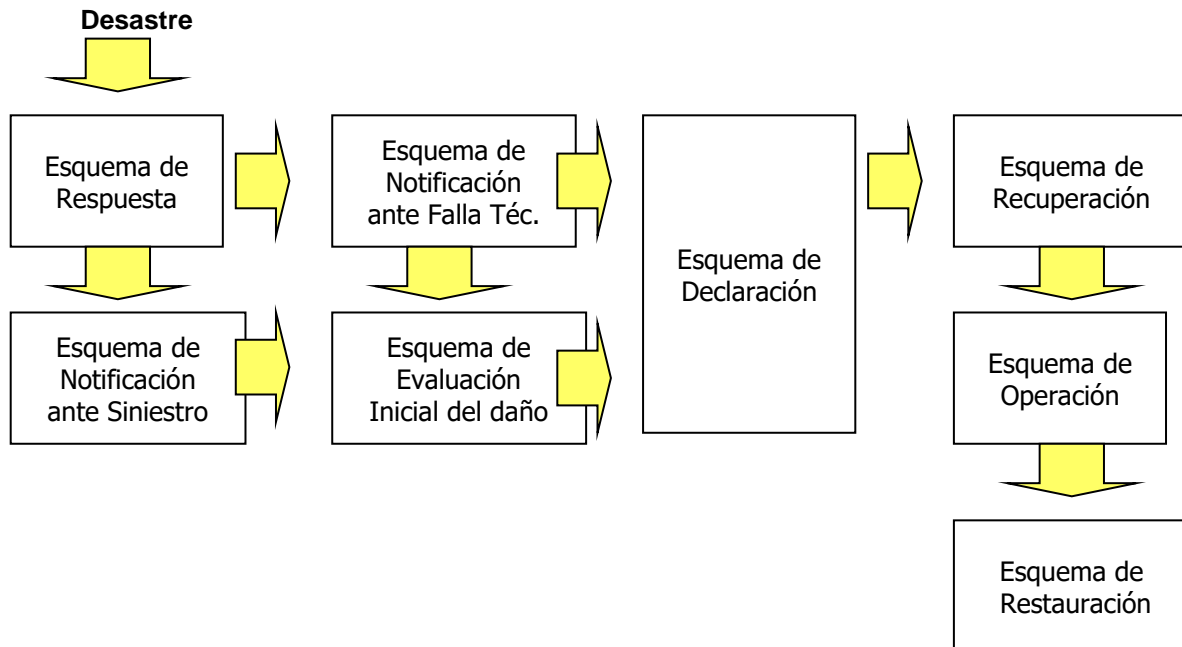
La coordinación con los controles de la seguridad. La planificación de contingencias no puede llevarse a cabo en un vacío. Las estrategias de contingencia deben coordinarse estrechamente con las técnicas existentes y las propuestas, de gestión y la seguridad operativa del sistema de control para reducir riesgos y garantizar capacidades y la viabilidad de la contingencia.

De esta guía en general se desprenden prácticamente todos los métodos para formular Planes de contingencia, además, cada Estado propone sus propios métodos para encarar esta cuestión.

La siguiente figura muestra el esquema adecuado que permite formular un adecuado plan de contingencia para recuperación ante desastres, obtenida de la presentación efectuada por el INDEC en la conferencia sobre Desastres Informáticos el 17 y 18 de junio de 1998, en Buenos Aires, Argentina:



Componentes del Plan de Contingencias



Como queda planteado en la presentación del NIST, la base de los planes de contingencia son los recursos de proceso de la información, es decir hardware y software, sin embargo la debilidad es que si uno analiza en detalle cualquier organización, mucha de la información de gestión y decisión no esta totalmente informatizada y la pérdida entonces no esta controlada.

MAGERIT Versión 2, propone una metodología de análisis y gestión de riesgos de los sistemas de información.

En su capítulo 2, establece los siguientes conceptos sobre la gestión de riesgos:

Se resumen a continuación algunos conceptos centrales de la metodología:

Análisis de Riesgos (establece conceptos sobre análisis de riesgos)

Paso 1: Activos (determinación de los activos de información a ser analizados)

Paso 2: Amenazas (que ponen en peligro los activos de la información)

Paso 3: Determinación del impacto (en caso de producirse la situación de amenaza)

Paso 4: Determinación del riesgo (que produce la amenaza)

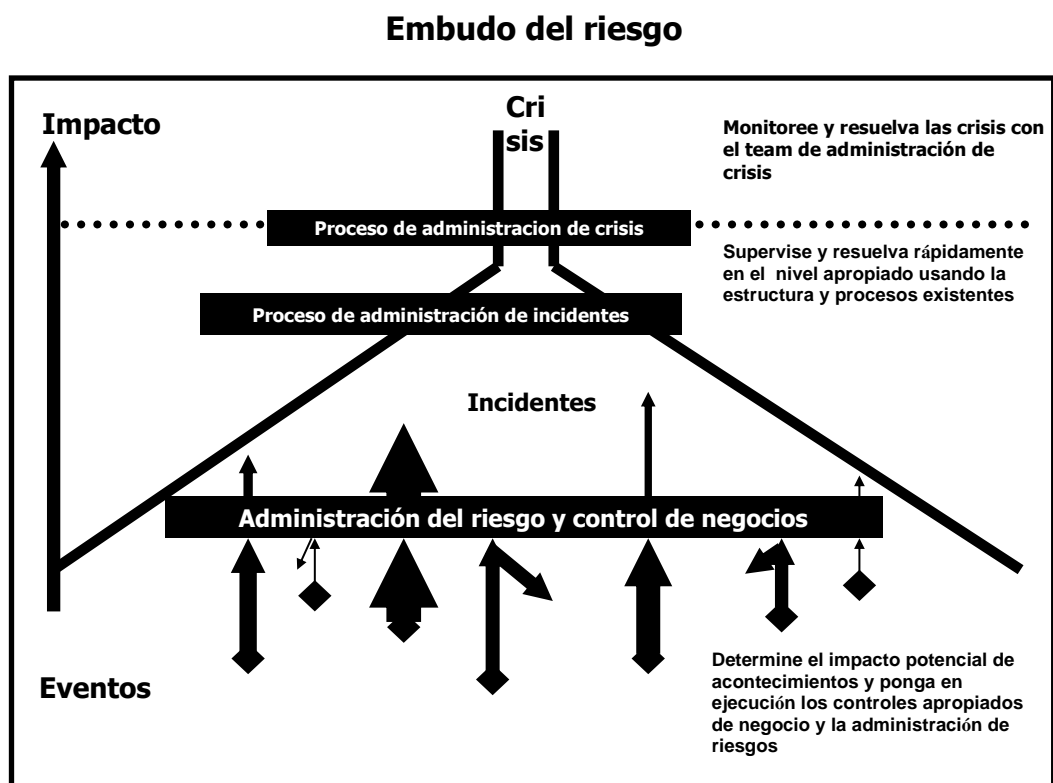
Paso 5: Salvaguardas (establecimiento de contramedidas para mitigar o eliminar el riesgo de ocurrencia de la amenaza)

Revisión del paso 3: impacto residual (que se estudia si no se disponen de medidas y salvaguardas)

Revisión del paso 4: riesgo residual (que permanece al no tener totalmente cubierto el riesgo)

Gestión de Riesgos

Se debe analizar el riesgo de cada activo, en la siguiente figura se establece el denominado:



La interpretación de los valores de impacto y riesgo residuales asumidos.

Selección de salvaguardas:

Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

1. establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa
2. establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
3. establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer
4. desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas
5. desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto

Pérdidas y ganancias

La actitud de la Dirección:

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias.

Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, etc...). Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección

Si el impacto y/o el riesgo están por encima de lo aceptable, se puede:

1. eliminar el activo; suena muy fuerte, pero a veces hay activos que, simplemente, no vale la pena mantener
2. introducir nuevas salvaguardas o mejorar la eficacia de las presentes

Revisión del paso 1: revisar los nuevos activos incorporados por las salvaguardas.

De lo expuesto se deduce que el principio rector de la metodología es establecer los Activos de la información, realizando una detección y registrando un inventario de los mismos.

Esto presenta un problema desde el punto de vista de la denominada información no controlable por no estar ubicada en dispositivos físicos y tangibles.

Es el caso de los Recursos humanos, que utilizan medios como celulares, teléfonos, anotadores, agendas de uso personal que generalmente guardan información valiosa y crítica pero no son pasibles de ser inventariadas de la misma manera que el boca a boca tampoco puede ser inventariado.

CAPITULO III

PLANTEAMIENTO DEL PROBLEMA

CAPITULO III - PLANTEAMIENTO DEL PROBLEMA

PROBLEMAS PARA IMPLEMENTAR PLANES DE CONTINGENCIA Y GESTIÓN DE RIESGOS

En este contexto una serie de conceptos son utilizados para mitigar las amenazas sobre los activos de la información, es la denominada Gestión de Riesgos, cuyo objetivo principal es determinar el máximo nivel permitido de riesgos que se está dispuesto a tolerar, así como la definición de controles pertinentes para proteger los recursos de las vulnerabilidades existentes.

Es una construcción propia que permita lograr niveles de protección previniendo la ocurrencia de amenazas.

Es un proceso dinámico para asegurar integridad, disponibilidad y confidencialidad de la información.

SE ESTABLECE LA EVALUACIÓN DE RIESGOS DE LA SEGURIDAD

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos de ella.

El gasto en los controles es necesario compararlo con el probable perjuicio que resulte de fallas en la seguridad las técnicas de evaluación de riesgos se pueden aplicar a toda la organización, o solamente a partes de ella, como también a los sistemas de información individuales, componentes específicos de un sistema o servicios, cuando sea práctico, realista y útil.

La evaluación del riesgo es la consideración sistemática de:

- El probable perjuicio al negocio que resulte de una falla en la seguridad, tomando en cuenta las consecuencias potenciales de una pérdida de confidencialidad, integridad o disponibilidad

- La probabilidad realista de que tal falla ocurra, en vista de las amenazas y vulnerabilidades efectivas, y los controles actualmente implementados

Las revisiones se deberían realizar en diferentes niveles de profundidad, dependiendo de los resultados de las evaluaciones previas y de los cambios de niveles de riesgo que la dirección está preparada para aceptar.

Las evaluaciones de riesgo, a menudo se realizan primero a alto nivel, como una forma de priorizar los recursos en áreas de alto riesgo, y luego en un nivel más detallado, para abordar riesgos específicos.

La siguiente lista muestra los conceptos y modelos de gestión del análisis de riesgos y de administración de riesgos:

- OCTAVE
- NIST
- AS/NZS 4360
- ITIL
- CRAMM
- MAGERIT
- ISO/IEC 27005 (Por publicarse en 2008)

CUANTITATIVO VS. CUALITATIVO

- El análisis de riesgos cualitativo utiliza diferentes escenarios de posibilidades de riesgo y clasifica la seriedad de las amenazas y la sensibilidad de los activos. Esta basado en juicios, intuición y experiencia, en vez de números y valores financieros.

Cuantitativo

Beneficios

- Los riesgos son priorizados por impacto financiero; los activos son priorizados por valores financieros.
- Los resultados facilitan la administración de riesgos por su retorno en inversión en seguridad (ROSI).

- Los resultados pueden ser expresados en terminología específicamente administrativa (valores monetarios y probabilidad expresada en términos de porcentajes específicos).

- Se tiende a incrementar la precisión conforme pasa el tiempo mientras la organización crea un registro histórico de los datos, mientras gana experiencia.

Cualitativo

Beneficios

- Es más fácil alcanzar consensos.
- No es necesario cuantificar la frecuencia de las amenazas.
- No es necesario determinar el valor financiero de los activos.
- Es más fácil involucrar a personas que no son expertos en seguridad o en el uso de Sistemas de Información.
- Permite la visión y entendimiento de la clasificación de riesgos.

Cuantitativo

Desventajas

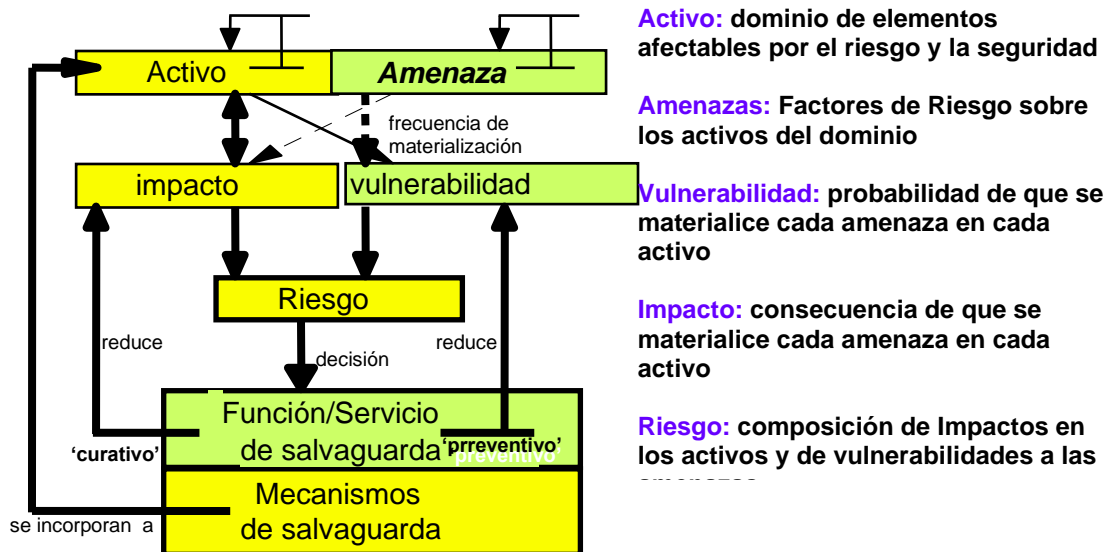
- Los valores de impacto asignados a los riesgos están basados en opiniones subjetivas de los participantes.
- El proceso para alcanzar resultados creíbles y consensos consume mucho tiempo.
- Los cálculos pueden ser muy complejos y consumir mucho tiempo.
- Los resultados solo son presentados en términos monetarios y pueden ser difíciles de interpretar por personas no técnicas.
- El proceso requiere de experiencia, por lo que la guía de los participantes puede que no sea sencilla.

Cualitativo

Desventajas

- No hay suficiente diferenciación entre riesgos importantes.
- Difícil de justificar inversiones en la implementación de controles debido a que no hay bases para el análisis costo-beneficio.
- Los resultados dependes de la calidad del equipo de administración de riesgos conformado.

Un ejemplo trivial de gestión de riesgos



- **Activo:** Es cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección.
- **Amenazas:** Cualquier circunstancia o evento con el potencial para causar daño al activo al explotar sus vulnerabilidades. Las amenazas se componen de agentes (entidad que al actuar explota la vulnerabilidades de un activo) y eventos (situación en que el agente de la amenaza causa un daño a un activo).
- **Vulnerabilidades:** Una vulnerabilidad es una debilidad inherente a un activo. Por sí misma no es causante de daño, simplemente es una condición o conjunto de condiciones que incrementan la probabilidad de que el evento de una amenaza se materialice. La falta de control también es considerada como una vulnerabilidad.
- **Impacto:** Es el grado de daño causado por la materialización de un evento de Amenaza.

Activo



Casa de madera

Vulnerabilidad



Estructura con riesgo al fuego

Agentes



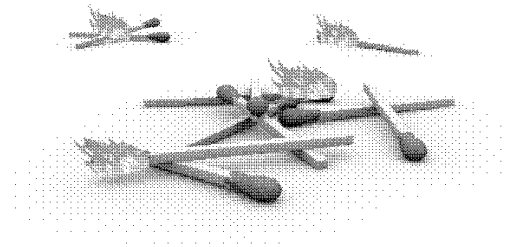
Evento

Fuego



Impacto

Incendio

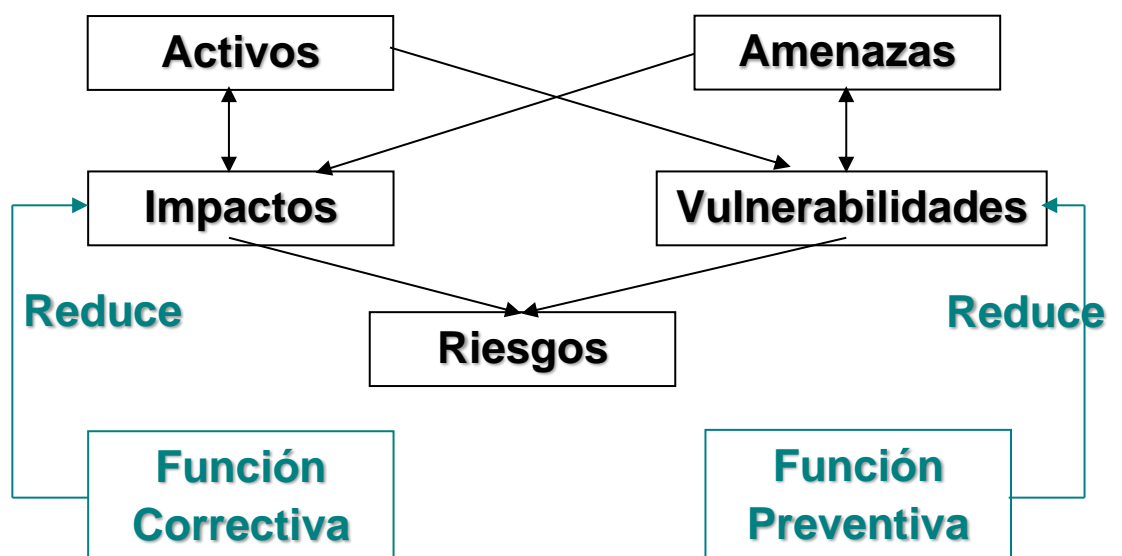


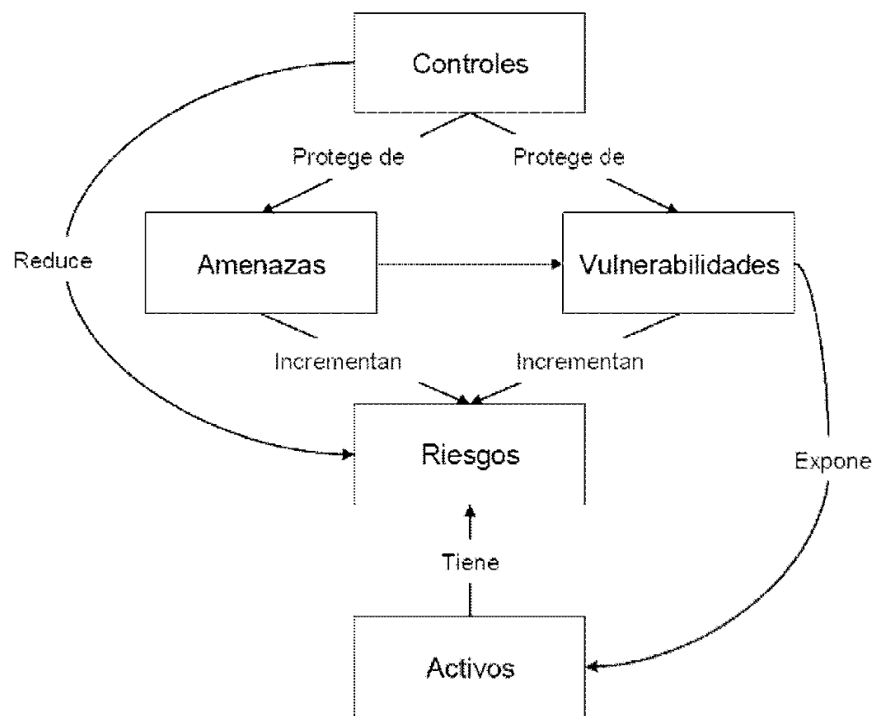
IMPACTO

Destrucción

Modelo:

Análisis de Riesgos – Modelo de Gestión





Un ejemplo de establecimiento de plan de contingencias (RB 13):

Identificación de información y activos

Identificar proceso.

Identificar actividades involucradas en el proceso.

Identificar activos involucrados en la ejecución de las actividades.

Identificación de información y activos

Proceso: Nómina.

Actividades: Calcular nómina, aplicar descuentos, aplicar bonos, imprimir cheques, etc.

Activos (cheques):

Tesorero, información de pagos, cheques, PC Tesorero, Excel, impresora, cheques impresos.

Política de Seguridad

“Conjunto de Normas y Procedimientos documentados y comunicados, que tienen por objetivo minimizar los riesgos de la seguridad de la información mas probables”

La Política de Seguridad Involucra:

Responsabilidad de la Dirección

Establecimiento de procedimientos de control

Uso de métodos, técnicas y herramientas

Cumplimiento de Tareas por parte de personas

Se muestra la política de seguridad de la información establecida en el estado argentino, basada en la ISO 17799 (RB 16):

Modelo de política de gestión de la seguridad en tres niveles



Definición de Plan de contingencias:

“Conjunto de Normas y Procedimientos documentados y comunicados, cuyo objetivo es recuperar operatividad mínima en un lapso adecuado a la misión del sistema afectado, ante emergencias generadas por los riesgos informáticos”

El Plan de Contingencias Involucra:

Uso de herramientas

Cumplimiento de responsabilidades de las personas

Documentación de procedimientos de control y actividades de contingencia para mitigar o afrontar los riesgos que se transforman en cese de actividades de gestión.

Esta metodología de diseño, elaboración e implementación de planes de contingencia es en la práctica la más utilizada, generalmente se producen manuales de contingencia luego de haber implementado el plan, los mismos tienden a quedar rápidamente en desuso debido a la imposibilidad de realizar una prueba de contingencia integral o parcial de los procesos incluidos para no afectar la productividad de la empresa.

Por ello, la hipótesis de la tesis encarada es la de desarrollar un sistema informático de soporte a los proyectos y sistemas de gestión de planes de contingencia de tal manera de utilizar los recursos actuales como Internet y conectividad con dispositivos móviles que facilitarían tanto el desarrollo de plan como la implementación efectiva del mismo.

La experiencia del autor de la tesis indica que generalmente los planes de contingencia son elaborados cuando ocurre alguna falla o evento que pone en riesgo el negocio y la operación normal de la organización con la potencial pérdida que esto acarrea. Ante estas situaciones imprevistas, la alta Dirección tiene tendencia a contratar un experto quien lleva a cargo la redacción del manual del plan de contingencias de la compañía, generalmente en un plazo perentorio y con no mucho apoyo del resto de la organización.

El manual tiene una característica estática, representa una fotografía de los procesos y responsables de la gestión de la organización en un momento de la operación de la misma.

Cabe destacar que la gestión de una organización hoy es dinámica con cambios continuos producidos en su entorno de negocios y su medio ambiente socio económico, con lo cual cualquier fotografía tiende a quedar obsoleta en poco tiempo.

Reiniciar el proyecto de actualización del plan de contingencias resulta entonces una tarea sumamente costosa ya que se trata de revisar todas y cada una de las potenciales fallas y riesgos que presenta la organización en cada momento, siendo que el resultado puede ser no producir cambios.

Ejemplos de planes de contingencia inconclusos se presentan en numerosas organizaciones que comienzan el proyecto con gran ímpetu y luego discontinúan o espacian la actividad del mismo motivados por problemas y situaciones cotidianas que demandan mayor atención a los responsables de realizar el mismo.

CAPITULO IV – SOLUCIÓN

DISEÑO Y ESPECIFICACIÓN DE UNA SOLUCIÓN PARA ELABORAR PLANES DE CONTINGENCIA Y GESTIÓN DE RIESGOS BASADOS EN ANÁLISIS DE PROCESOS CRÍTICOS Y SISTEMAS WEB SERVICES.

La solución que se presenta en esta tesis de Maestría, consiste en un conjunto de productos de software, denominados Web Services, navegables, que tienen los siguientes objetivos:

Que la Dirección y alta gerencia de una organización disponga de una ayuda en intranet o Internet a los Gerentes de proyectos que tienen a su cargo llevar adelante la implementación de la gestión de riesgos y elaborar los planes de contingencia de las organizaciones.

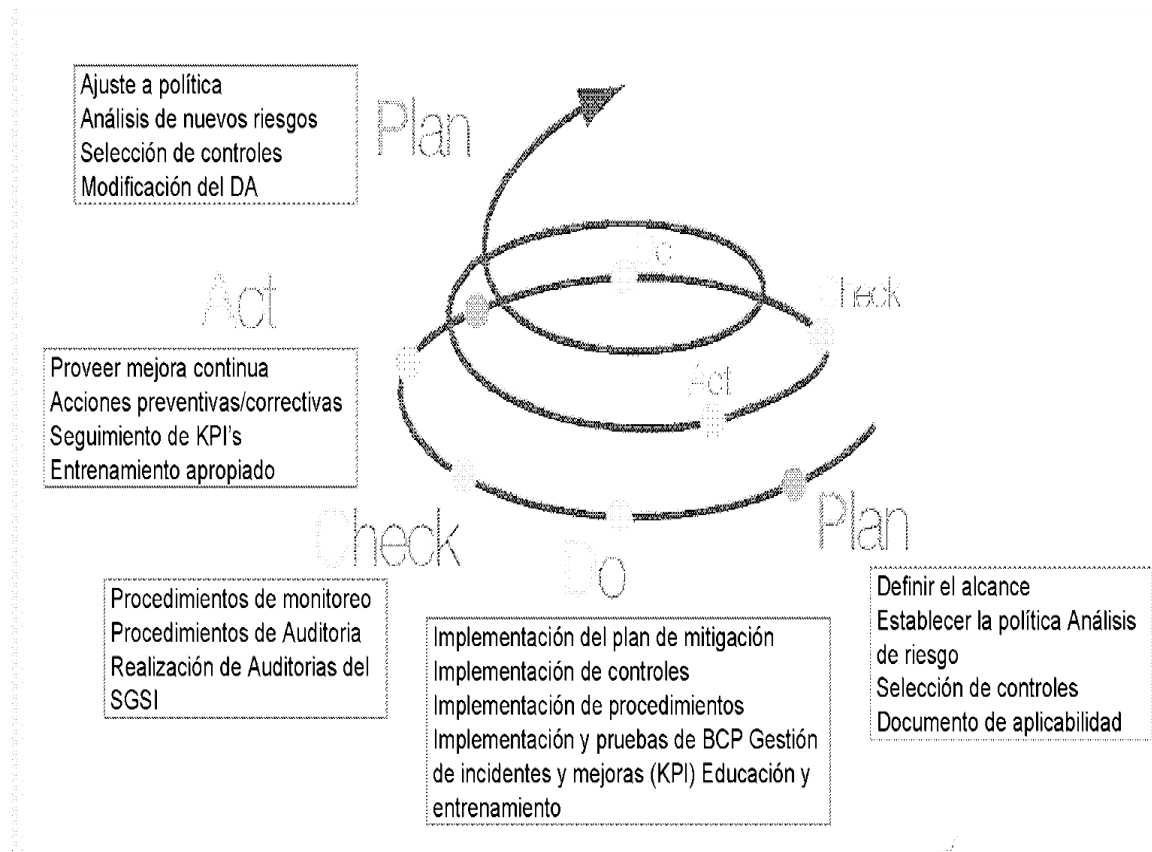
La ayuda consiste en brindar una metodología prescriptiva, es decir por fases, divididas en actividades y estas en tareas, con ayudas de plantillas, métodos, técnicas y herramientas necesarias para la realización y documentación del sistema a implementar.

La estructura del proyecto se basa en la realización de la reingeniería de procesos de negocio de la organización para determinar los procesos críticos en cuanto a los riesgos, económicos, financieros, de información, de infraestructura y todo aquel que afecte la continuidad del negocio.

Uno de los objetivos fundamentales de los sistemas diseñados es que la organización pueda implementar el modelo Plan – Do – Check – Act, tal como se fue planteado al inicio en el capítulo I, aplicado a los sistemas de gestión de la seguridad de la información:

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello



El denominado **Asistente para la gestión de riesgos**, basado en el análisis de los procesos críticos de la organización, tiene las siguientes fases principales:



[Asistente de la Gestión de riesgos](#)



[Política de riesgos](#)



[Análisis de Procesos](#)



[Análisis de riesgos](#)



[Concepto de objetivo](#)



[Reporte de riesgos](#)



[Control de riesgos](#)

Este sistema propone una Solución para la implementación del sistema de gestión de Riesgos en la organización adoptante y como consecuencia es la base fundamental para la estructuración del Plan de contingencias de la misma.







El Asistente del proceso de riesgos lo ayudará a planificar y diseñar su sistema de gestión de riesgos. Lo guiará y acelerará su proyecto mediante la ayuda de elementos predefinidos, y provee respuestas a las más importantes cuestiones con un método prescriptivo y procedural, que describe las fases, paquetes de trabajo y actividades individuales de un proyecto de gerenciamiento de riesgos y establecimiento de un Plan de contingencias. El Asistente posee además listas de control, listas de preguntas y otras herramientas para documentar las actividades que se desarrollen durante el proyecto.










El asistente del proceso de riesgos vincula los procesos de negocio con los elementos de riesgos relevantes para los mismos.

El manual de convenciones de modelización ayudará a customizar y modelar los procesos mediante los modelos de proceso mas adecuados.

El eventual Administrador o Gerente de riesgos, podrá generar un **portal** de la gestión de los riesgos y sus salvaguardas establecidas, y además, publicarlo en la intranet de la compañía.

La fase de establecimiento de la Política de riesgos incluye las siguientes actividades

-  Política de riesgos
-  Workshops de inicio del proyecto
-  Preparación del Workshops de inicio del proyecto
-  Realización del Workshops de inicio del proyecto
-  Seguimiento posterior a la realización del Workshops
-  Definición de la Política de Riesgos














-  Definición de términos y categorías de riesgos
-  Selección de instrumentos para establecer las salvaguardas
-  Definición de unidades de análisis
-  Definición de estrategias de acción
-  Documentación de la Política de riesgos
-  Creación de un Plan de Proyecto borrador
-  Desarrollo de un Plan de proyecto borrador
-  Actualización del Plan de Proyecto borrador
-  Revisión de la Política de Riesgos

El asistente de Proceso de riesgos provee soporte efectivo para el proceso de establecimiento de la Política de riesgos, usando las siguientes herramientas:

- Espécimen: Agenda del taller de apertura
- Ejemplos: factores críticos de éxito
- Formulario: minutas para documentar reuniones
- Ejemplo: definición de términos de riesgos
- Ejemplos: instrumentos para identificación de riesgos
- Formulario: estrategias de acción y definición de salvaguardas
- Ejemplo: política de riesgo documentada
- Espécimen: Plan de proyecto borrador
- Ejemplo: Instrucciones para usar el plan de proyecto borrador
- Formulario: minutas de proyecto
- Formulario: revisión de política de riesgos

La siguiente Fase corresponde a la realización del análisis de los procesos de negocio, para determinar aquéllos que son críticos e incluyen riesgos sobre activos de información y por lo tanto los que deben tener incluidos procedimientos de control de tal manera de mitigar o eliminar el riesgo.

Estos procesos críticos serán, mediante estos procedimientos de control, los que tengan incluidas actividades inherentes a planes de contingencia para lograr la continuidad del negocio, en caso de que se presenten situaciones que generen riesgos a la continuidad de la actividad organizacional.

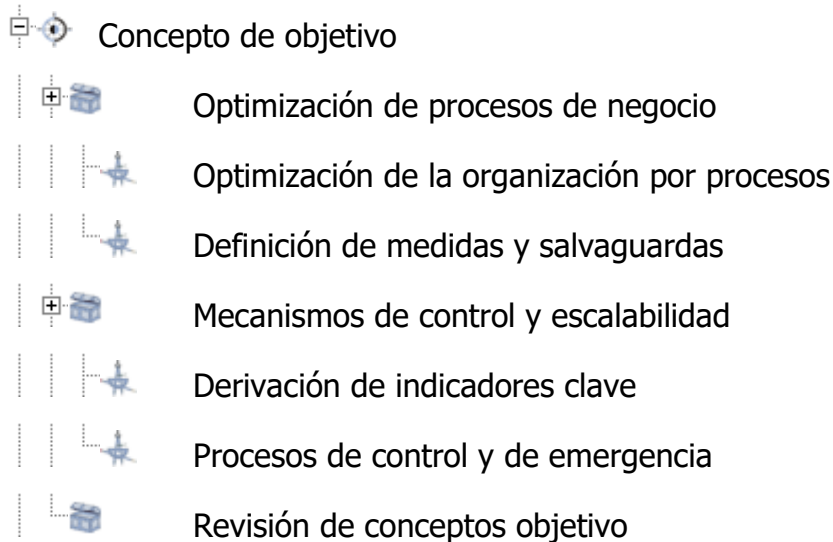
-  **Análisis de Procesos de negocio**
-  Workshops de Convenciones para modelar los procesos
-  Selección de métodos de modelización de procesos
-  Definición de niveles de modelización (global o detallado)
-  Definición de convenciones gráficas
-  Representación de la estructura organizacional
-  Desarrollo de las cartas estructuradas organizacionales
-  Documentación de las responsabilidades del personal
-  **Análisis de Procesos de Negocio**
-  Preparación del análisis de procesos de negocio
-  Workshops de análisis de Procesos
-  Documentación de los procesos analizados
-  Revisión del análisis de procesos efectuado

El asistente del proceso de riesgos proporciona una ayuda eficaz, para este proceso de análisis, brindando el uso de las herramientas siguientes:

- Lista de modelos importantes y relevantes (p.ej. cadena de valor agregado)
- Ejemplo de niveles de modelización
- Espécimen: Manual de convenciones para modelar
- Espécimen: estructura organizacional tipo
- Espécimen: concepto de rol
- Formulario: Identificación de procesos de negocio
- Ejemplo: Modelización de procesos

- Check list: Revisión de análisis de procesos

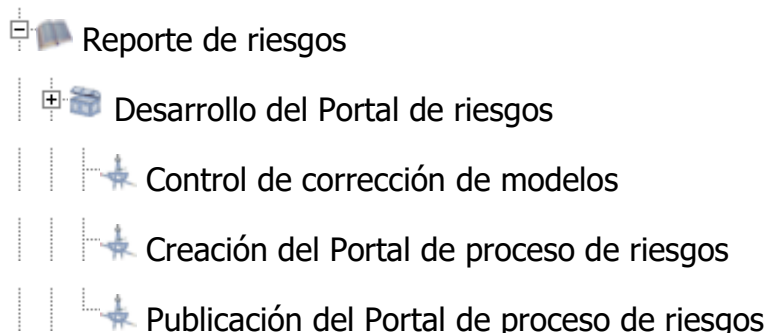
Luego se continúa con la siguiente fase, en la que se establecen las medidas y salvaguardas necesarias para cubrir los riesgos:



El Asistente del proceso de riesgos proporciona la ayuda eficaz para esta fase, incluyendo las herramientas siguientes:

- Ejemplo de un proceso de contingencia en caso de fuego
- Check list: revisión del concepto objetivo

Luego en la siguiente fase se establece el denominado portal de riesgos, es decir un sistema en la intranet de la compañía que facilite el monitoreo y control de la situación de los riesgos y las medidas de control establecidas:




 Revisión de reportes de riesgos

El Asistente del proceso de riesgos proporciona una ayuda eficaz para la implementación del portal, incluyendo las herramientas siguientes:

- Ejemplo: Portal de Procesos de Riesgos
- Check list: Reporte de Riesgos


La fase final, es la que permite establecer el subsistema de control de riesgos:


 Control de riesgos

 Definir medidas de control y salvaguardas

 Promoción del reconocimiento de riesgos por el personal

 Control Inmediato

 Desarrollo continuo (evolución y mejora continua)

 Revisión del control de riesgos

El asistente del proceso de riesgos provee soporte efectivo en esto, incluyendo las siguientes herramientas:

- Formulario: Necesidades de entrenamiento
- Check list: Registro de Control de los riesgos
- Check list: Revisión de control de riesgos

Todas y cada una de las actividades a realizar por el equipo de proyecto están diseñadas en base la modelo:

I-P-O

Es decir **Input – Process – Output**

Que facilita atacar los niveles de gran complejidad como son los que presenta establecer un Plan de contingencias y de gestión de riesgos,

Mediante las denominadas

Precondiciones: es decir que es lo que sirve de entrada al proceso a desarrollarse cuando se lleva a cabo la actividad, que elementos son necesarios disponer, documentos, modelos y definiciones previas.

Procedimiento: es decir la lista detallada de tareas a realizar paso a paso por el equipo de proyecto, desarrollada de manera exhaustiva.

Resultados (Post condiciones): es decir que debe producir el proceso a través de la aplicación del procedimiento establecido para la realización de tareas, generalmente esta salida servirá de entrada a las precondiciones de las siguientes actividades, en la misma fase o en otras del proyecto.

A modo de ejemplo se desarrolla la actividad de Revisión del control del Riesgo, donde se muestra la estructura y los denominados facilitadores que son las herramientas que brinda el asistente para la realización de tareas del proyecto.

Revisión del control del Riesgo

Objetivo:

La revisión del control de riesgos asegura que todos los pasos de esta fase han sido implementados

Precondición

- Los paquetes de trabajo de la fase de control de riesgos han sido completados.

Procedimiento

- Invitar la Superioridad representativa y el staff involucrado en las fases individuales a una reunión de revisión.
- Dibujar un resumen (overview) de los paquetes de trabajo completados.
- Los miembros relevantes del staff realizan la presentación de los resultados y el status de sus paquetes de trabajo respectivos.
- Comprender los resultados de los pasos individuales en una discusión de grupo.
- Discutir y documentar acciones de mejora.
- Monitorear la conformidad con las acciones de mejora propuestas y revisar su efectividad.
- Entregar un reporte detallado a todos los participantes.

Resultado

La ejecución de los paquetes de trabajo individuales ha sido revisada y comprendida. Asimismo, se ha decidido monitorear las mejoras.

El sistema planteado que acompaña los proyectos orientados a reingeniería de procesos de negocio y permite implementar el sistema de gestión de riesgos, se acompaña y vincula con un sistema Web Services, es decir para utilizar mediante Internet o intranet, que incluye toda la información necesaria para la implementación del sistema de software que permita luego de instalado, realizar la efectiva gestión de riesgos y por ende la actualización continua de los planes de contingencia asociados.

Este es el denominado:

Sistema de gestión de planes de contingencia y riesgos (**SGR**), basado los principios de la OECD, que son la base de la implementación de un sistema de gestión de la seguridad de la información, prescripto en las normas ISO 27001 (conformidad a requisitos) e ISO 27002 (guías para la implementación de la seguridad de la información).

El diseño del sistema incluye los siguientes conceptos:

Elementos

- Bibliotecas
- Proyectos en curso
- Activos de la información (en el SGR)
- Dominios de seguridad de la información
- Salvaguardas (en el SGR)
- Perfiles de seguridad
- Niveles de valoración de los riesgos
- Niveles de madurez
- Niveles de criticidad

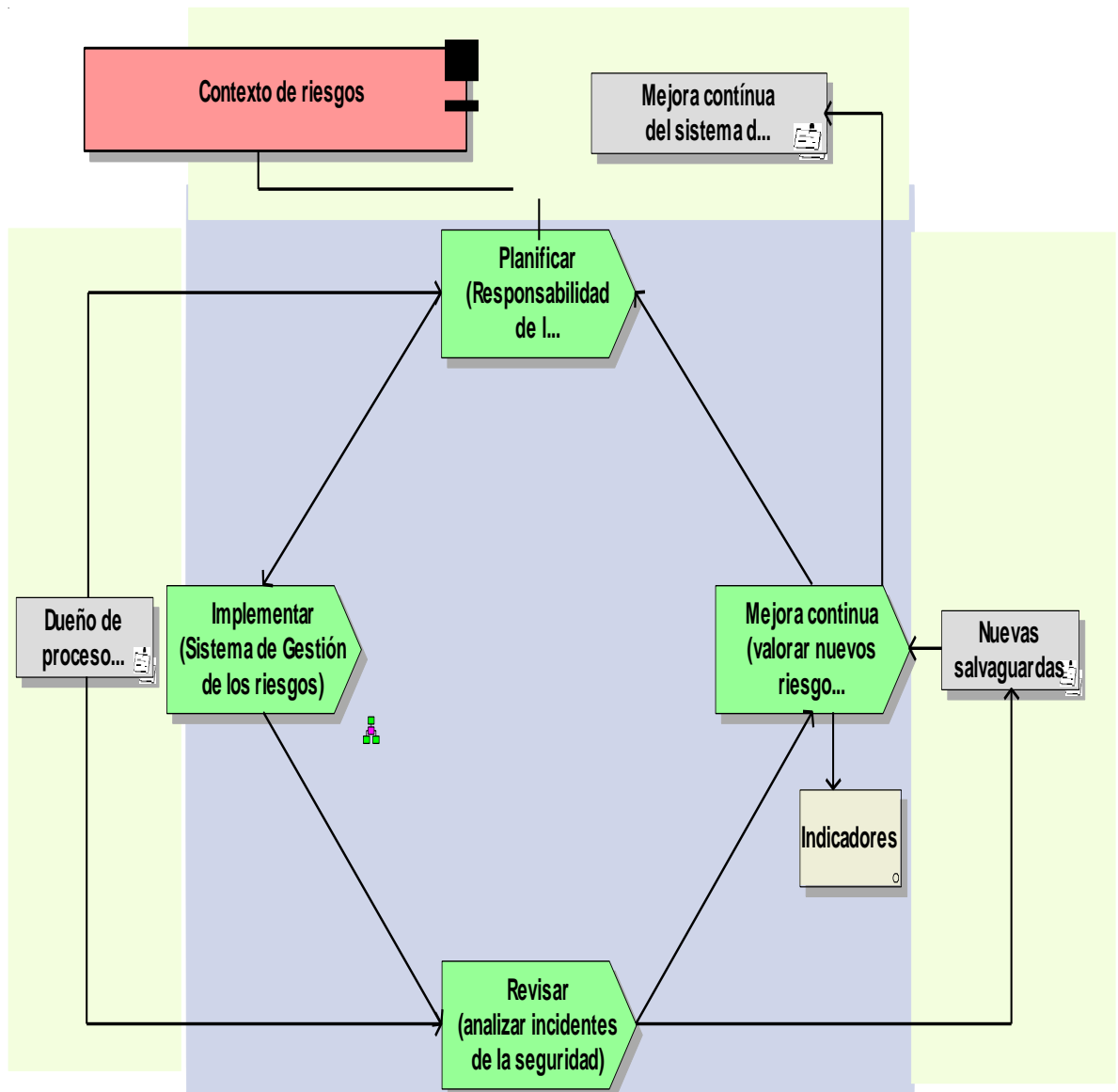
Las bibliotecas proporcionan:

- una colección de clases de activos
- una colección de dimensiones de seguridad
- una colección de niveles cualitativos
- una colección de amenazas
- una colección de salvaguardas
- amenazas típicas por clase de activo
- reconocimiento de la importancia relativa de las salvaguardas
- perfiles de seguridad
- perfiles de amenaza

Al referirnos a Proyectos, los mismos en general están embebidos en uno mayor o macro de alcance mayor cuyo objetivo principal es implantar un Sistema de Gestión de la Seguridad de la información (SGSI) en una organización, se da una guía de ayuda a las PYMES para la implementación de este sistema de Gestión de la Seguridad de la información ([plantilla para que las PYMES puedan llevar adelante sus proyectos de implantación de la gestión de la seguridad con menor costo](#))

El cuadro adjunto muestra el modelo Plan – Do – Check – Act presentado en la norma IRAM 17551 (RB 14) – Sistema de gestión de riesgos:

Modelo de un Sistema de Gestión de riesgos basado en Procesos



Cabe destacar que una vez determinado el riesgo y establecida la necesidad de implementar una salvaguarda, la misma pasa a formar parte de los denominados planes de contingencia, que permiten que la organización continúe operando aún bajo situaciones críticas, mediante la adecuada implementación de las mismas y una correcta asignación de responsables de ejecutar las salvaguardas y procedimientos establecidos en caso de contingencias.

Para subsanar en parte esta falencia de finalización y de actualización de los planes de contingencias, es que se presenta este conjunto de herramientas basados en servicios Web que facilitan la realización de los planes, la gestión de los riesgos y el control del estado del sistema de gestión, mediante tres funciones básicas:

- **diseño del sistema de gestión de planes de contingencia y gestión de riesgos**
- **estructura del proyecto de gestión de planes y riesgos**
- **sistema de control de estado de indicadores de riesgo**

Limitación:

No es el desarrollo completo de la solución sino el Framework de trabajo que facilita la realización de los proyectos de gestión de contingencias y riesgos, el diseño del sistema informático de gestión de riesgos y el diseño del sistema informático de gestión de contingencias.

La base del diseño presentado es la realización del análisis de riesgos y definición de salvaguardas para los procesos clave de la organización esto es, analizar los procesos de gestión estableciendo aquellos denominados claves que permiten la operación normal del flujo de trabajo organizacional.

Para aplicar las ayudas que brindan estos sistema Web es necesario contar un el auxilio de una herramienta de modelización de procesos que facilite la identificación

de niveles de abstracción y permita asignar responsables a las funciones y actividades dentro de un proceso para designar los denominados dueños de proceso, dueños de función y dueños de riesgos.

Un ejemplo de tales herramientas es la plataforma ARIS TOOLSET, de IDS Scheer AG (<http://www.idsscheer.com/international/en>)

Por otro lado, cada función tiene asociados activos de la información que también deberán tener designados sus dueños de activos.

Las funciones y actividades de los procesos deben tener identificados los riesgos para determinar cuales son los controles que debe aplicar el dueño del proceso.

El presente estudio brinda Métodos, técnicas y herramientas de software mediante la utilización de las nuevas tecnologías de la comunicación como Internet, para la organización que opera su gestión basada en una alta utilización de tecnología de la información (hardware, software, sistemas informáticos, comunicaciones y redes), es decir que posee un alto contenido de información útil en sus bases de datos y viajando a través de la red, al comunicarse on line con sus proveedores y clientes, y de esta manera pueda disponer de un conjunto de herramientas informáticas de soporte a dos temas clave, como son la gestión de la continuidad del negocio dentro del contexto del plan de contingencia de la organización y la gestión de riesgos, no solo de la Tecnología de la información sino de la gestión de los procesos clave de la organización.

Diseño del sistema de software

El diseño del software de soporte planteado, está planteado mediante el lenguaje UML con la utilización de los modelos de casos de uso y clases para dar la estructura básica de componentes que deberán ser desarrollados posteriormente, para disponer del sistema completo en funcionamiento.

En la presentación del método de gestión de planes de contingencia se menciona la palabra falla, la misma puede ser sinónimo de riesgo, es decir que deberá

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

estar incluido dentro de un sistema de gestión de planes de contingencia el inventario de riesgos potenciales, el análisis de riesgos y el establecimiento de iniciativas para mitigar aquéllos riesgos que pueden producir el cese de las actividades productivas de la organización.

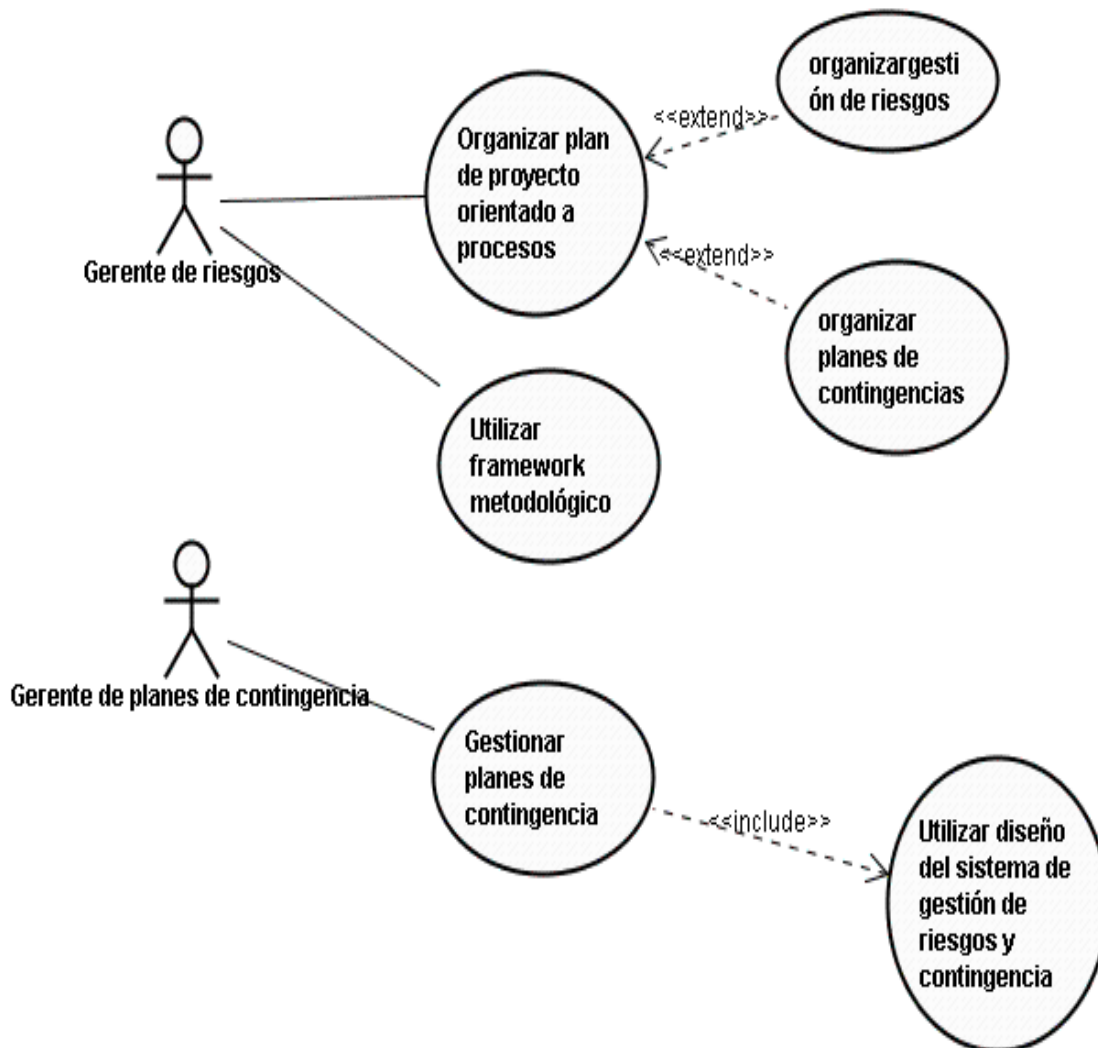
Utilizando la modelización orientada a Objetos del lenguaje UML y el software **JUDE** Community (<http://jude-users.com/en/>), a continuación se describen los principales modelos de diseño.

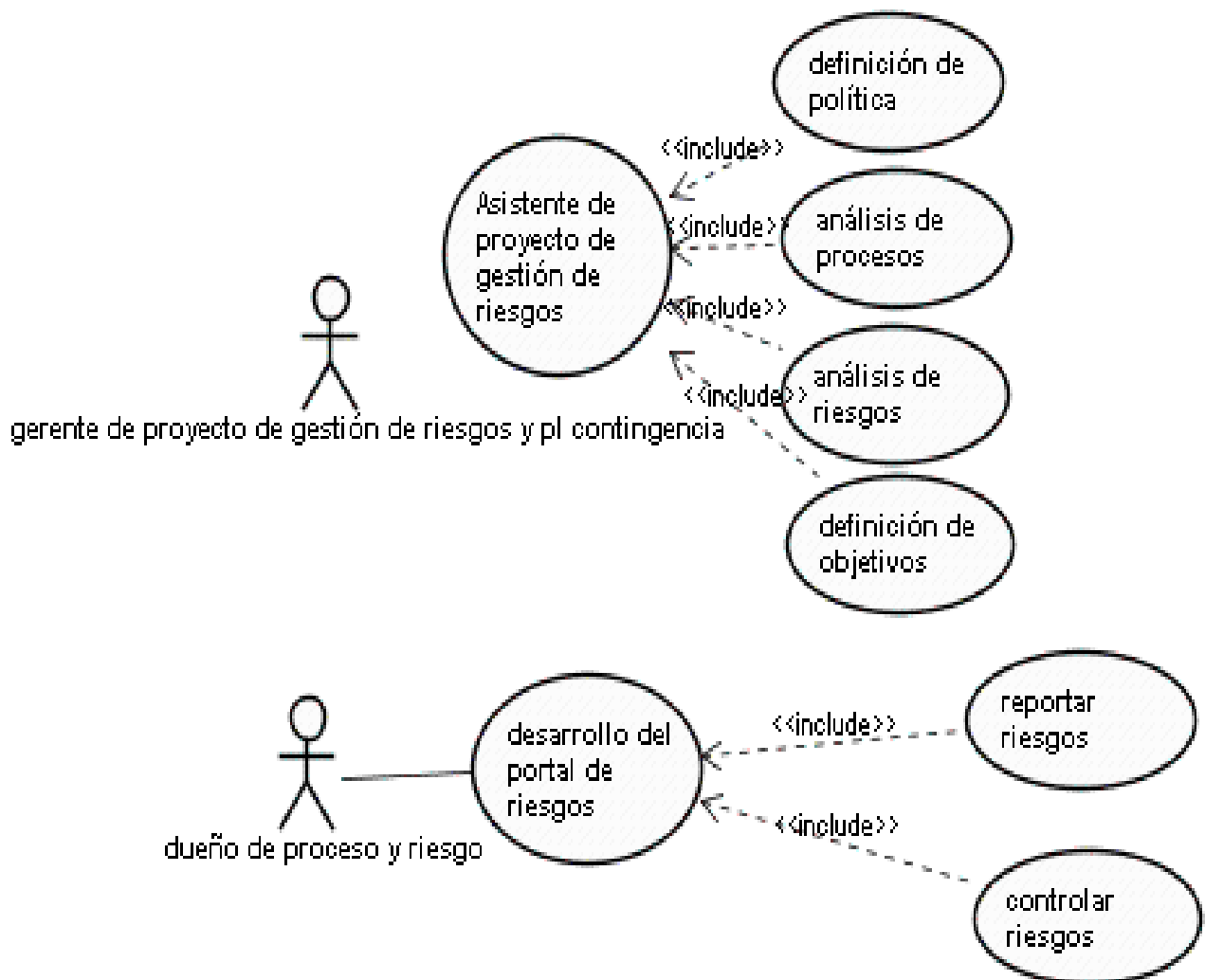
A continuación se muestran los diagramas del sistema general que integra los tres diseños de los sistemas propuestos.

Diseño del sistema de gestión de riesgos y planes de contingencia

Casos de uso de la gestión de riesgos y administración del portal de riesgos

El caso de uso describe la actividad con dos sistemas, el sistema de soporte a la elaboración de proyecto de gestión de planes y riesgos basado en análisis de procesos, mediante el uso del Framework metodológico planteado en esta tesis y el otro actor, gerente de planes de contingencia que usa para su gestión de planes de contingencia, los sistemas diseñados mediante el desarrollo de diseño de la presente tesis.



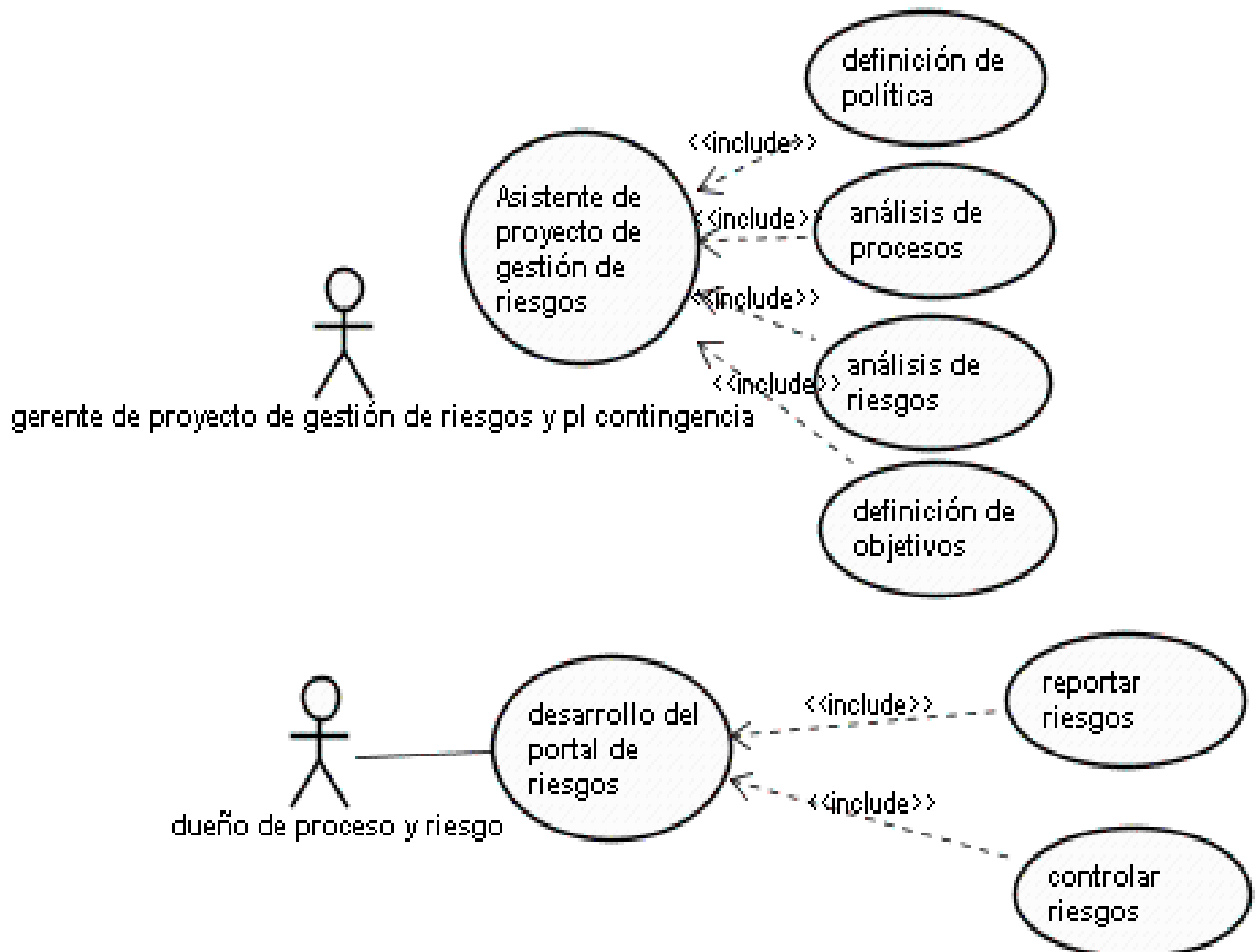


Este caso de uso presenta los dos actores principales, el gerente del proyecto de gestión de riesgos y planes de contingencia que utiliza el sistema de manera interactiva y que incluye las siguientes funciones: definición de la política, análisis de procesos, análisis de riesgos de los procesos y definición de objetivos de cobertura de los riesgos.

El otro actor es el dueño o responsable del proceso de riesgos quien accede interactivamente al sistema de portal del proceso de riesgos y utiliza dos funciones principales, controlar los riesgos y reportar riesgos (monitoreo y control de riesgos).

Diseño del sistema de gestión de riesgos y planes de contingencia

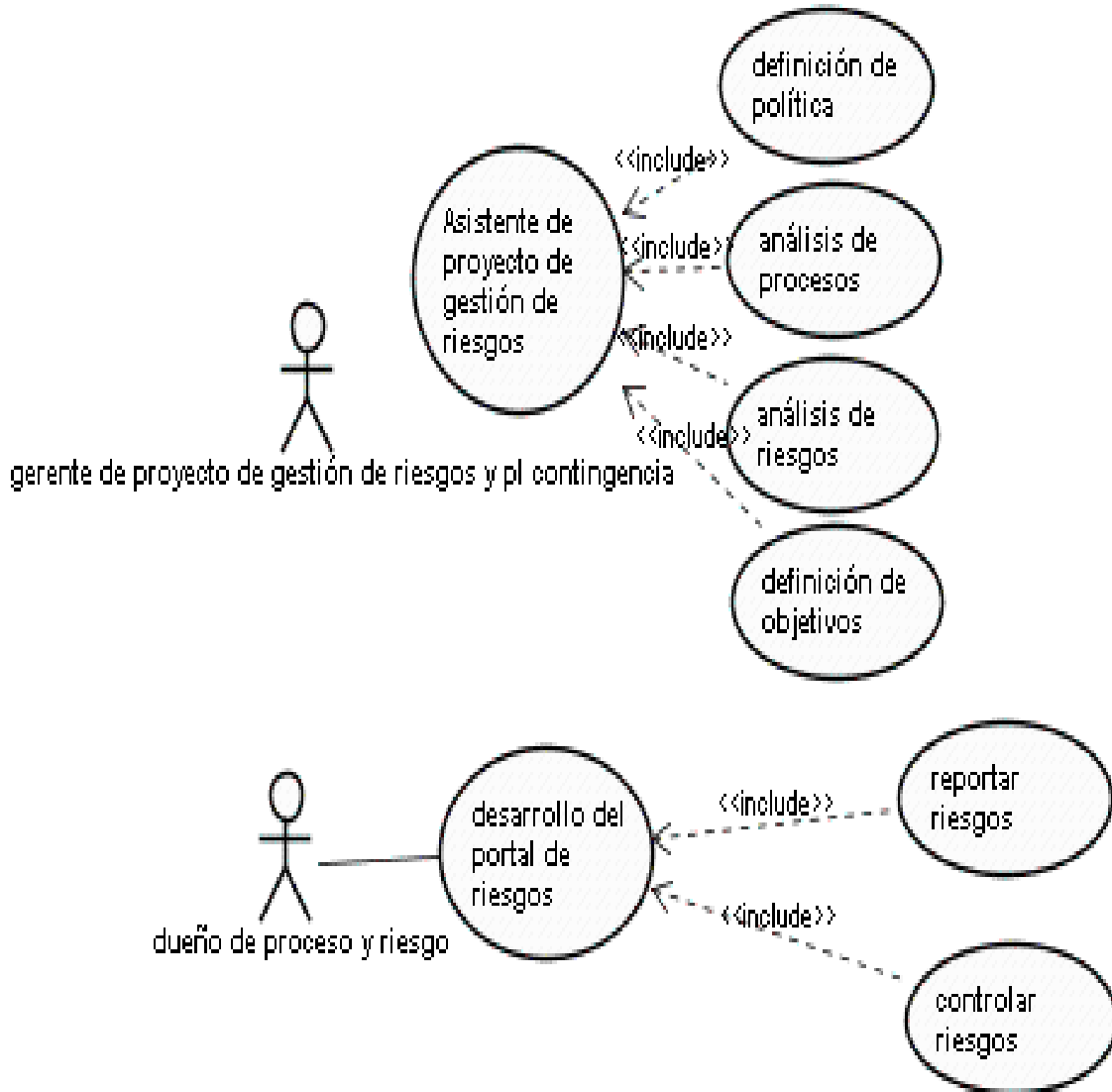
Caso de Uso: Consultar Metodología Magerit



Ambos actores para la realización de sus responsabilidades en distintos puntos del proyecto o de la gestión, deberán consultar algunos conceptos clave que están planteados en la metodología MAGERIT, esta consulta está implementada en los sistemas navegadores presentados en la tesis.

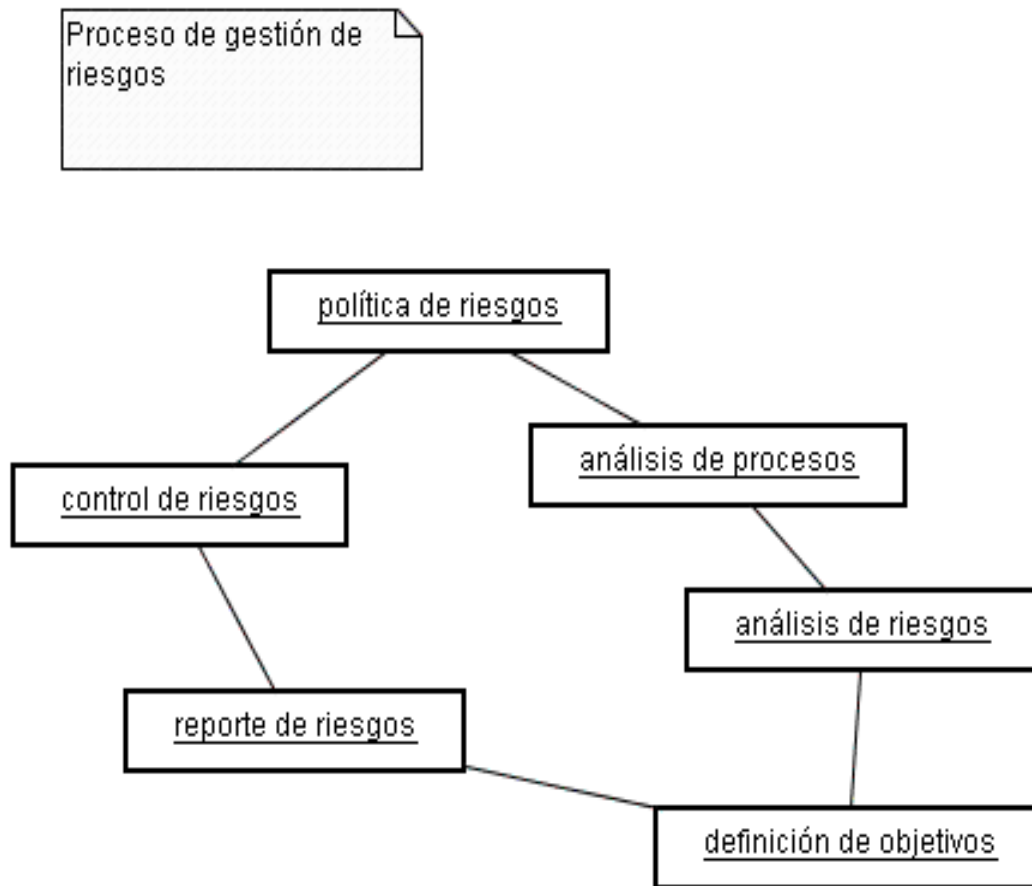
Diseño del sistema de gestión de riesgos y planes de contingencia

Caso de Uso: Administrar portal de proceso de riesgos



Diseño del sistema de gestión de riesgos y planes de contingencia

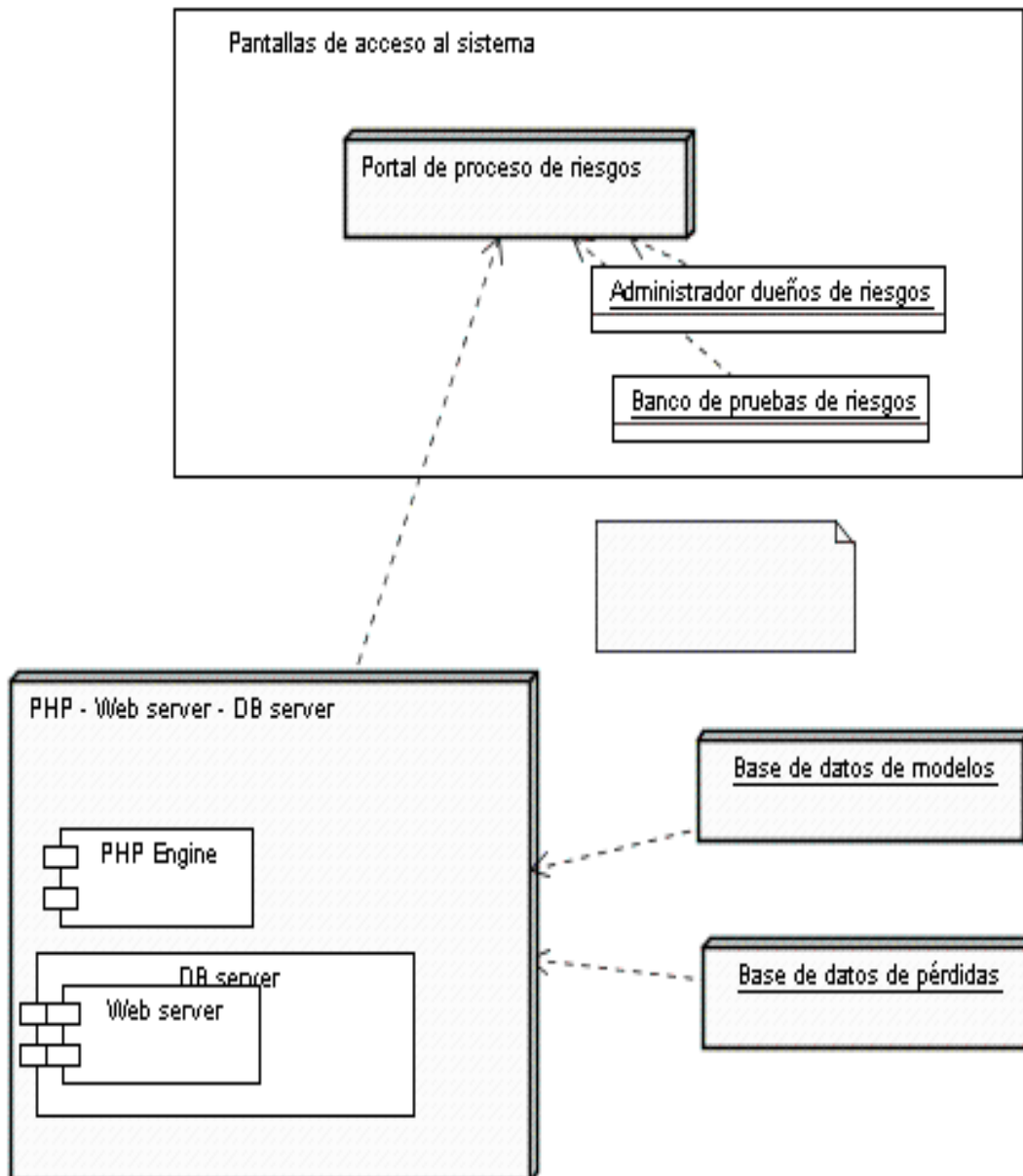
Diagrama de colaboración: Proceso de gestión de riesgos



El diagrama de colaboración entre objetos muestra las interacciones necesarias entre los componentes del sistema diseñado, de tal manera que se define la política de riesgos, para poder cumplir lo establecido en la misma, se realiza el denominado análisis de procesos clave del cual se deriva el análisis de riesgos lo que permite determinar el objetivo de cobertura a nivel objetivos de control de riesgos, luego se controlan y reportan estados de riesgos.

Diseño del sistema de gestión de riesgos y planes de contingencia

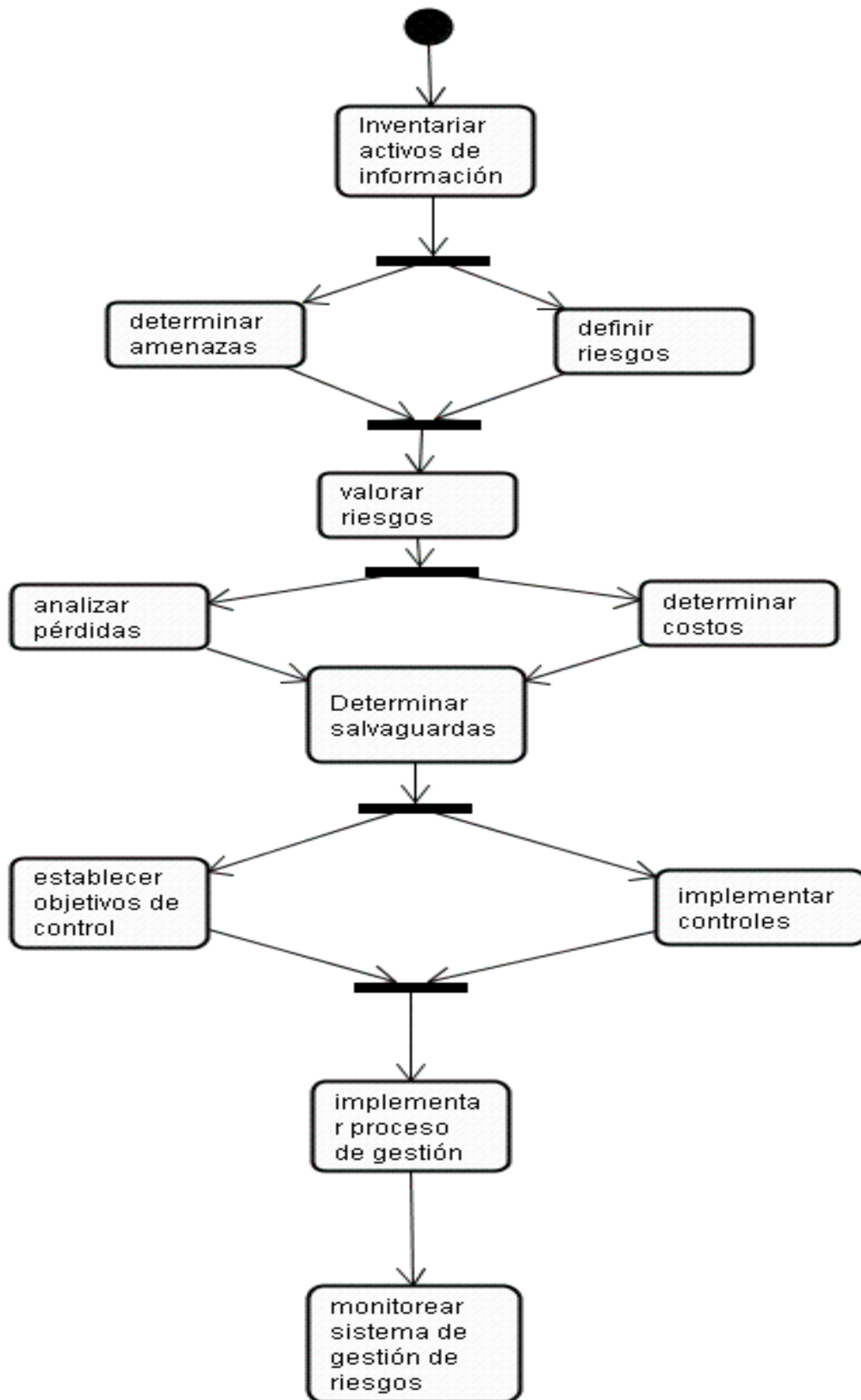
Diagrama de despliegue del portal de gestión de riesgos



Este diagrama presenta el modelo de servidor y clientes del sistema diseñado con las bases de datos necesarias para modelización y operación del sistema.

Los que continúan son los modelos y diagramas de cada uno de los tres diseños de sistemas propuestos en el presente trabajo.

Diseño del sistema de gestión de riesgos y planes de contingencia Diagrama de actividad del sistema de gestión de riesgos

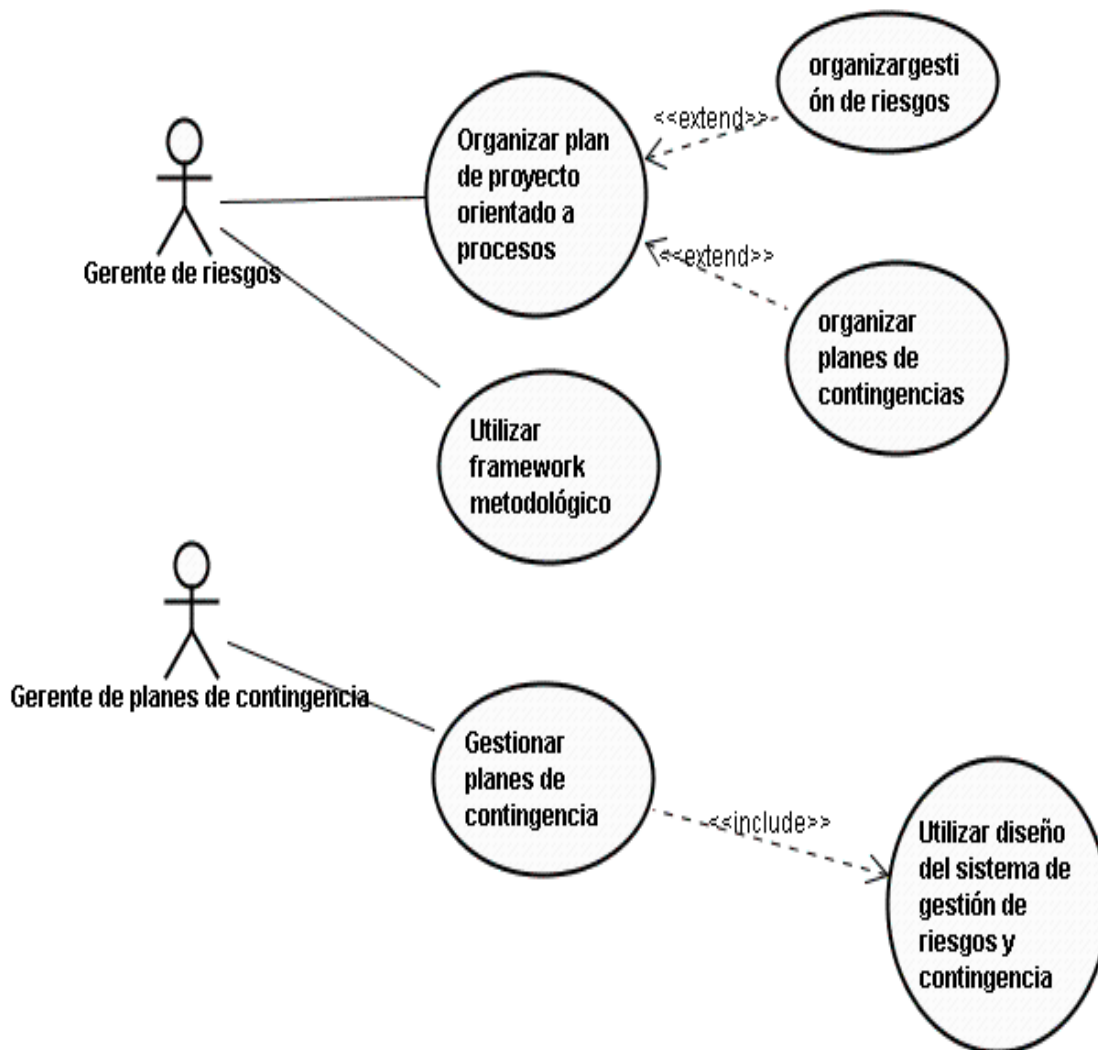


Diseño del sistema de gestión de riesgos y planes de contingencia

El proceso se gestiona mediante el siguiente sistema

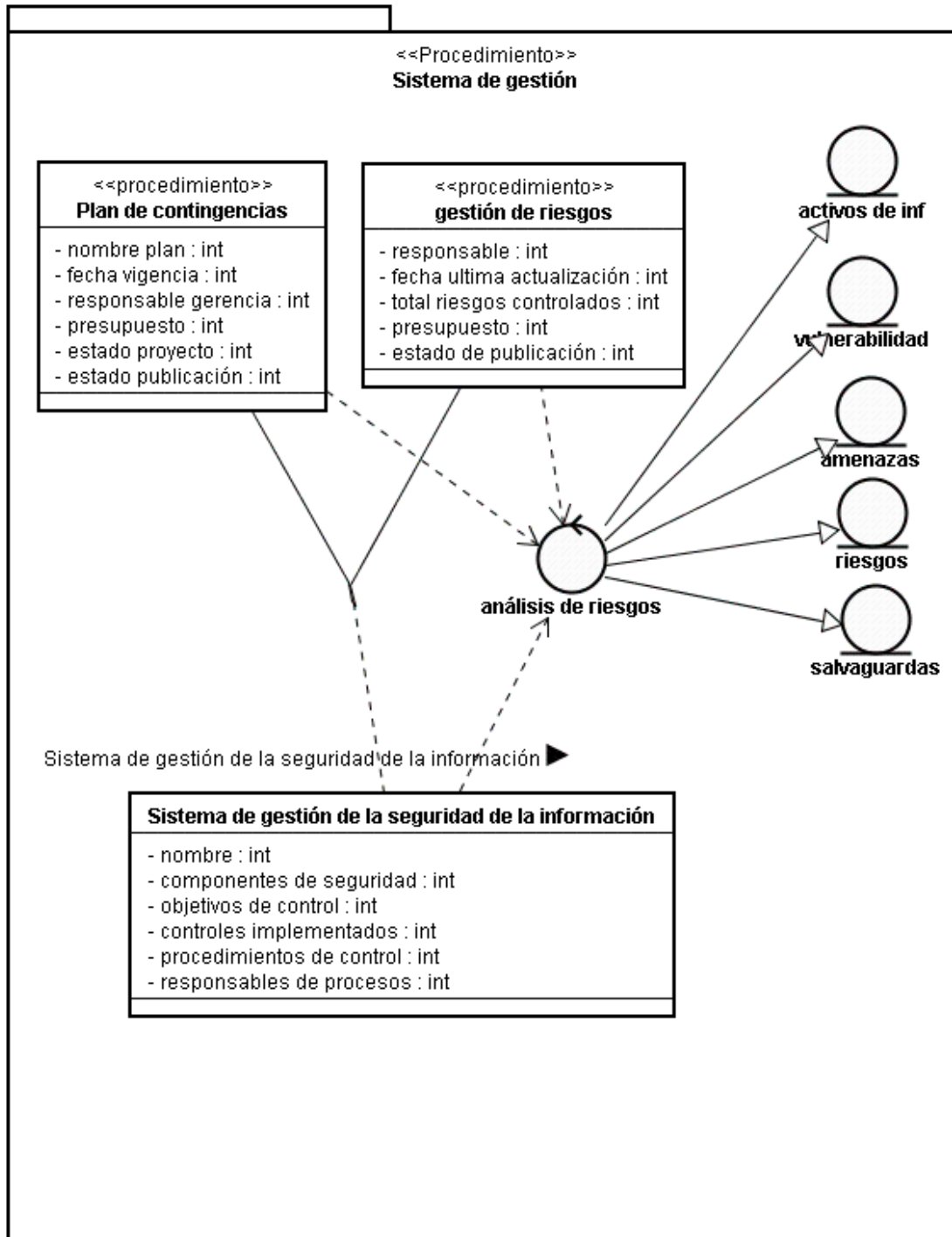
De soporte a la gestión de un proyecto de implementación de gestión de riesgos y contingencias.

Diagrama de casos de uso



Diseño del sistema de gestión de riesgos y planes de contingencia

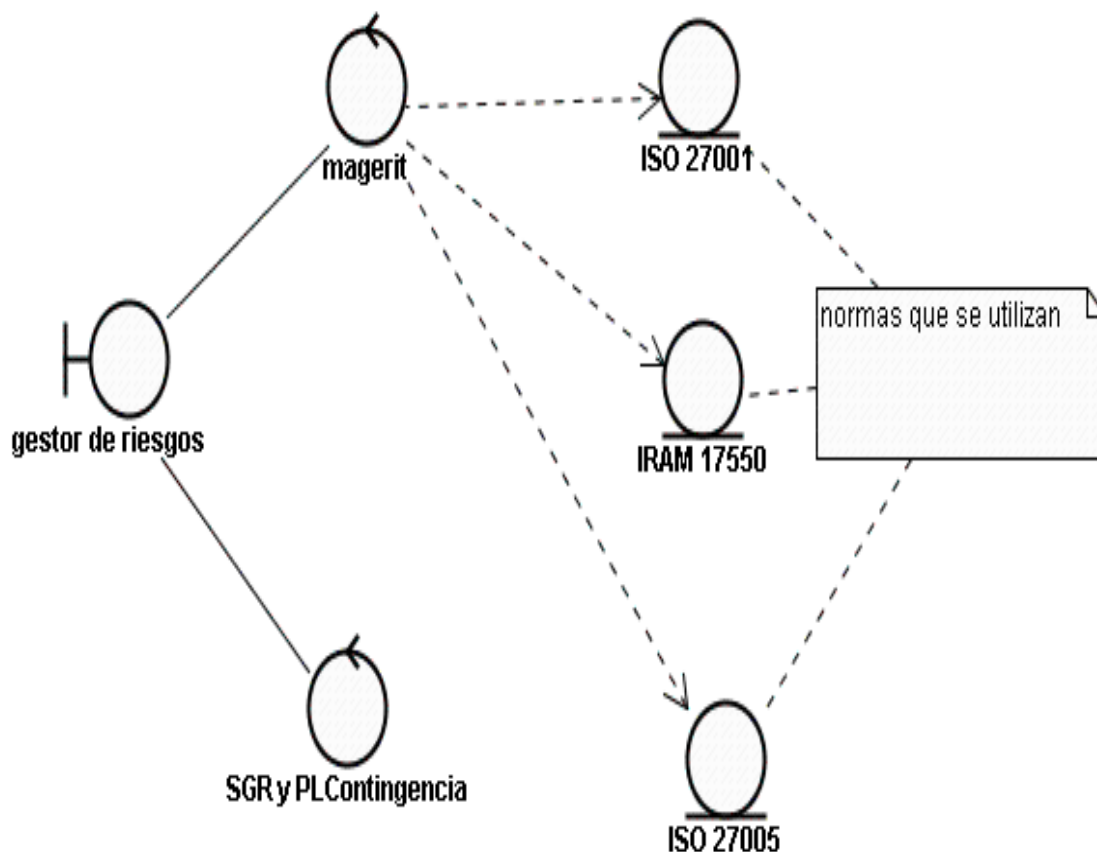
Diagrama de clases general



El diagrama de clases muestra las clases principales y los atributos necesarios para la ejecución del sistema. Muestra que un sistema de gestión de la seguridad de la información se compone de dos subsistemas, el de gestión de planes de contingencia y el de gestión del riesgo y que al análisis de riesgos analiza amenazas, vulnerabilidades de los activos o procesos, establece riesgos y determina salvaguardas (en general controles).

Diseño del sistema de gestión de riesgos y planes de contingencia

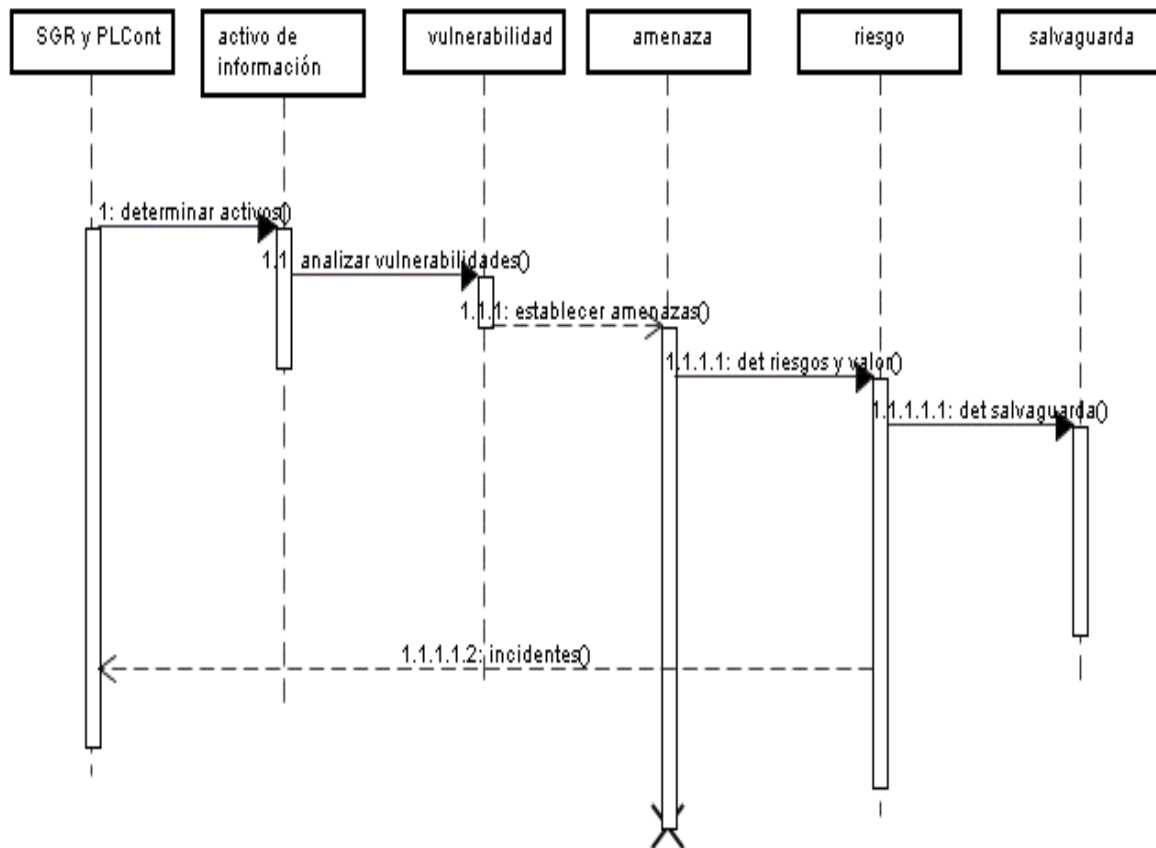
Modelo de negocio



El modelo de negocio muestra las principales clases representados por estereotipos de clases de interfase (gestor de riesgos), clases de control (magerit) y SGR y PLContingencia y clases de objetos (ISO 27001, IRAM 17550 e ISO 27005).

Diseño del sistema de gestión de riesgos y planes de contingencia

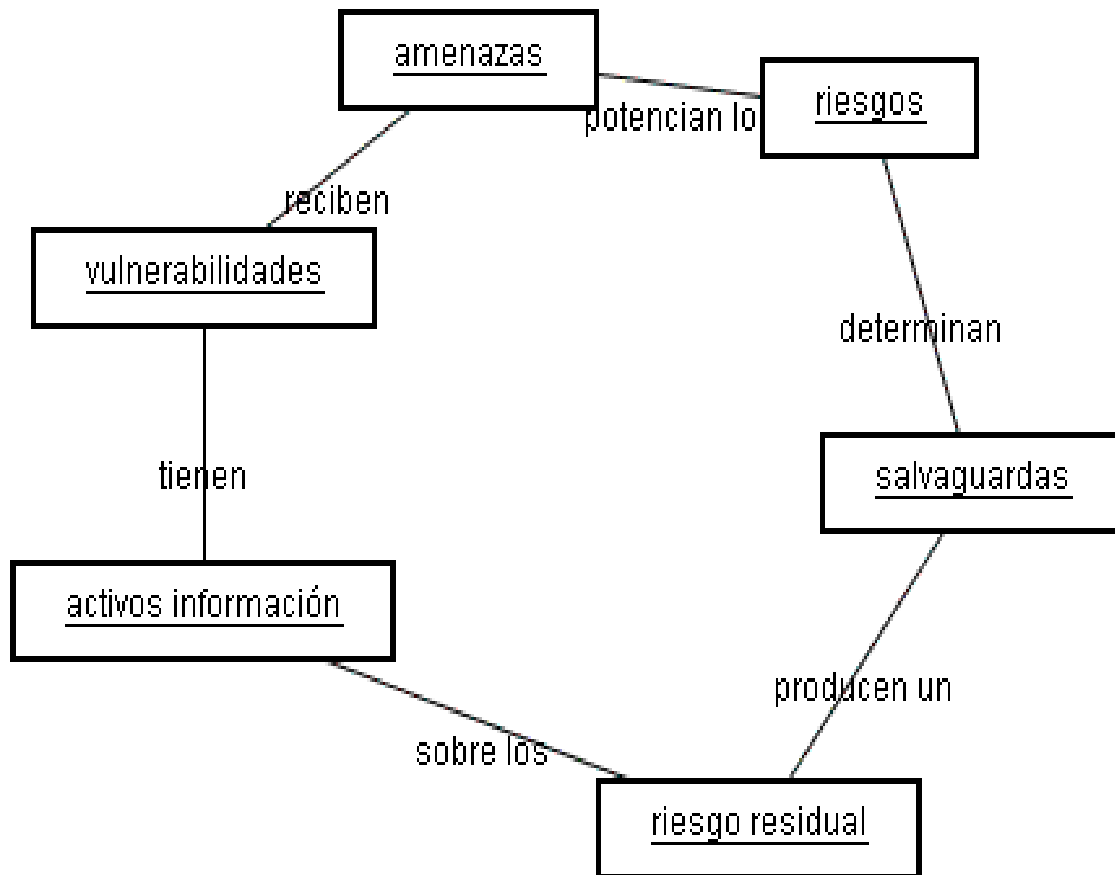
Diagrama de secuencias



Este diagrama de secuencia muestra la ejecución concreta al procesar para cada activo o proceso clave la determinación de vulnerabilidades, si estas determinan amenazas, si las mismas determinan riesgos y finalmente si se establecen salvaguardas.

Diseño del sistema de gestión de riesgos y planes de contingencia

Diagrama de colaboraciones



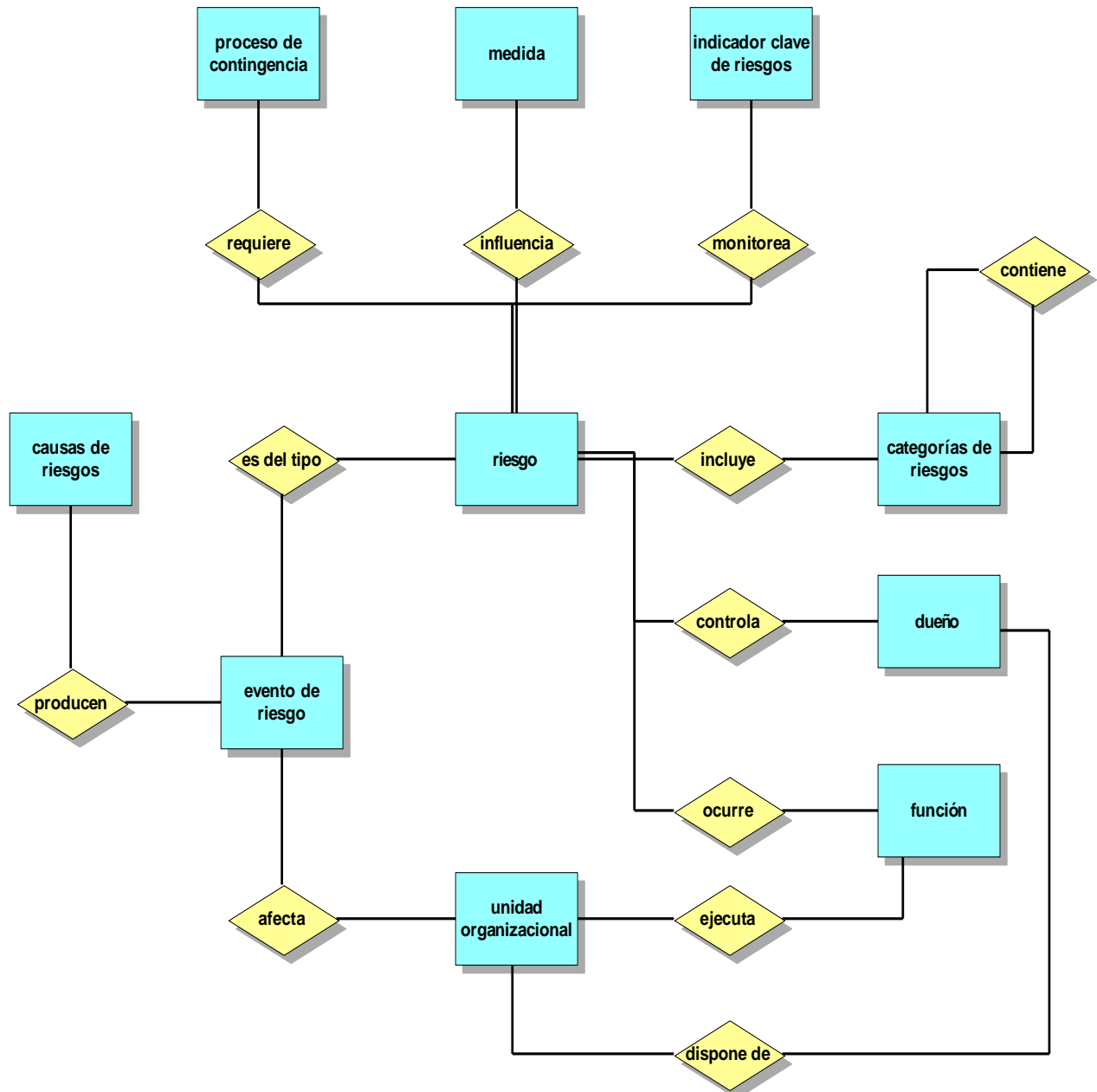
El diagrama de colaboraciones muestra la relación de mensajes entre los principales objetos de la aplicación.

Diseño del sistema de gestión de riesgos y planes de contingencia

El siguiente Diagrama de entidad y relación, permite modelar la base de datos de pérdidas que producen los riesgos en el sistema.

Diseño de la base de datos de pérdidas producidas por los riesgos

BASE DE DATOS DE PÉRDIDAS



El modelo básico que permite la gestión de riesgos es el Diagrama de controles de funciones de negocio:

Un Diagrama de controles de negocio representa los riesgos potenciales así como la gestión de riesgos de un proceso o de una función.

Definición: Un riesgo (Risk) representa el peligro potencial de un proceso que no alcanza el objetivo deseado del proceso.

Definición: La gestión o el control de riesgo (Control) representa una manera general de eliminar o mitigar un riesgo.

Definición: Una solución de riesgo significa implementar un control de riesgo respecto a un riesgo.

El diseño del Diagrama de controles de negocio corresponde a una matriz o tabla. La abscisa muestra los riesgos potenciales del proceso, y la ordenada muestra los posibles controles de riesgo. Soluciones de riesgo se insertan entonces como enlaces de un riesgo con control de riesgo. Adicionalmente pueden incluirse en el modelo unidades organizativas (en el sentido de exigencias del usuario) y documentos, que apoyan también la aplicación de una gestión de riesgo con respecto al riesgo.

Se utiliza al modelar los procesos y funciones en la metodología de reingeniería por procesos.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello







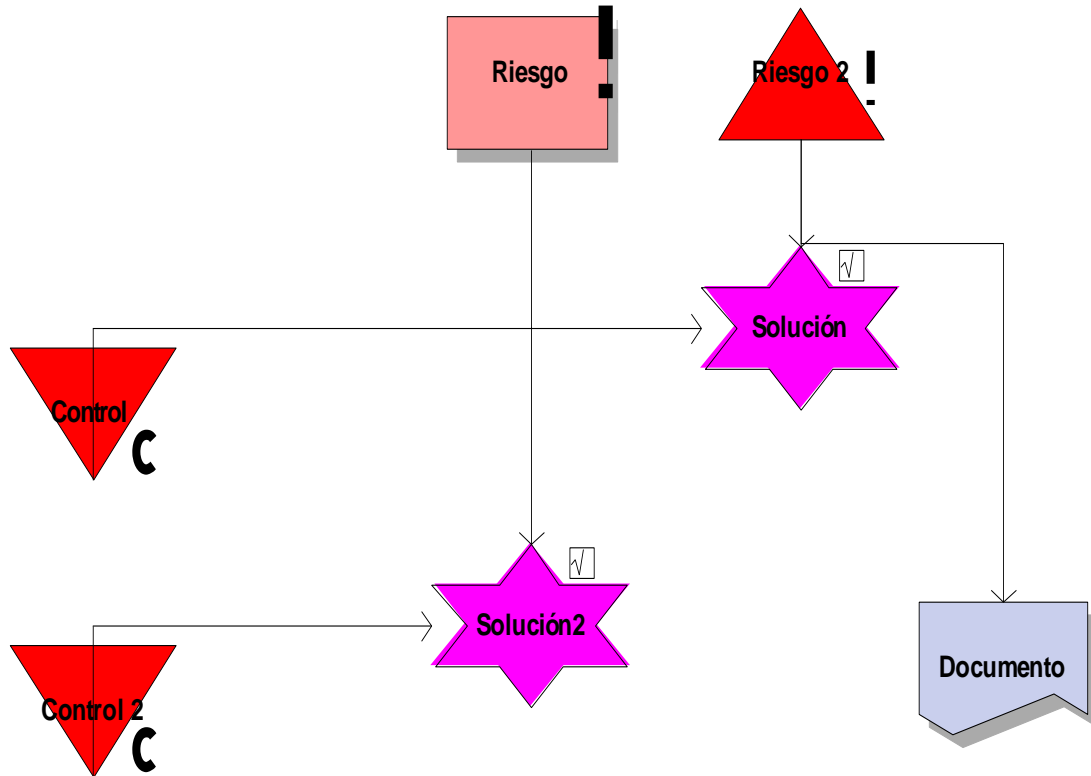
Símbolo(s)	Nombre de tipo de símbolo	Nombre de tipo de objeto
	Unidad organizativa	<u>Unidad organizativa</u>
	Documento	<u>Portador de información</u>
	Unidad organizativa	<u>Unidad organizativa</u>
	Risk	<u>Risk</u>
	Solution	<u>Solution</u>
	Controlador	<u>Controlador</u>

Diagrama de control de riesgos de funciones o procesos



Estos modelos presentados anteriormente, permiten diseñar las siguientes tres aplicaciones, que están implementadas como navegadores Web.

Diseño de un sistema de planes de contingencia y gestión de riesgos

El diseño es una guía para determinar la funcionalidad necesaria de un sistema de Planes de contingencia y gestión de riesgos, que Incluye la siguiente funcionalidad:

- SGR (que es el sistema)**
- Sobre la gestión de riesgos**
- Análisis cualitativo**
- Instalación**
- Elementos**
 - Bibliotecas**
 - Proyectos**
 - Activos (en el SGR)**
 - Dominios de seguridad**
 - Salvaguardas (en el SGR)**
 - Perfiles de seguridad**
 - Niveles de valoración**
 - Niveles de madurez**
 - Niveles de criticidad**
- Primera pantalla**
- Análisis y gestión de riesgos**
 - Datos del proyecto**
 - Análisis de Riesgos**
 - Evalúe las salvaguardas**
 - Evaluación del riesgo**
 - Informes**
 - Evalúe perfiles de seguridad**
- Magerit**
 - Análisis de Riesgos**
 - Tratamiento de los riesgos**
 - Dimensiones de seguridad**
 - Activos**
 - Amenazas**
 - Impacto**

⊕ **Riesgo**

⊕ **Salvuardas**







☐ **CC: Criterios comunes**

Sistema de ayuda a la formulación de proyectos de establecimiento e implementación de planes de contingencia y gestión de riesgos

Que tiene como hipótesis que la organización de realizar el análisis de sus procesos de negocio para desarrollar su plan de contingencias.

El sistema incluye la siguiente funcionalidad:

Asistente para la formulación de plan de contingencia y Gestión de riesgos

- ⊕  Política de riesgos
- ⊕  Análisis de Procesos
- ⊕  Análisis de riesgos
- ⊕  Concepto de objetivo
- ⊕  Reporte de riesgos
- ⊕  Control de riesgos

Diseño del sistema de gestión de riesgos y control de riesgos

Incluye la especificación para realizar un sistema que gestione los riesgos.

Asistente del proceso de Riesgos

Introducción

Asistente del Proceso de Riesgos

Que es el Asistente del Proceso de Riesgos?

Que son los iconos en el Asistente del Proceso de Riesgos?

Qué es el Manual de convenciones?

Qué es un proceso de gestión de riesgos?

Cuál es el diseño de la arquitectura y conceptos de seguridad?

Barra de herramientas del Asistente del proceso de riesgos

Portal del proceso de riesgos

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Procedimiento

Cómo cambiar su password

Cómo manejar Dueños de riesgos

Cómo manejar Gerentes de riesgos

Cómo hacen los Dueños de riesgos para reportar nuevos riesgos al Gerente de riesgos

Cómo hacen los Gerentes de riesgos para controlar nuevos riesgos y autorizar para transferirlos a la base de datos?

Cómo hacen los Administradores para transferir nuevos riesgos a la base de datos?

Cómo hace el Administrador para integrar el Gerente de performance de procesos en el Portal de proceso de riesgos?

Información de valor

Qué es el Portal del proceso de riesgos?

Qué son los roles en el Portal del proceso de riesgos?

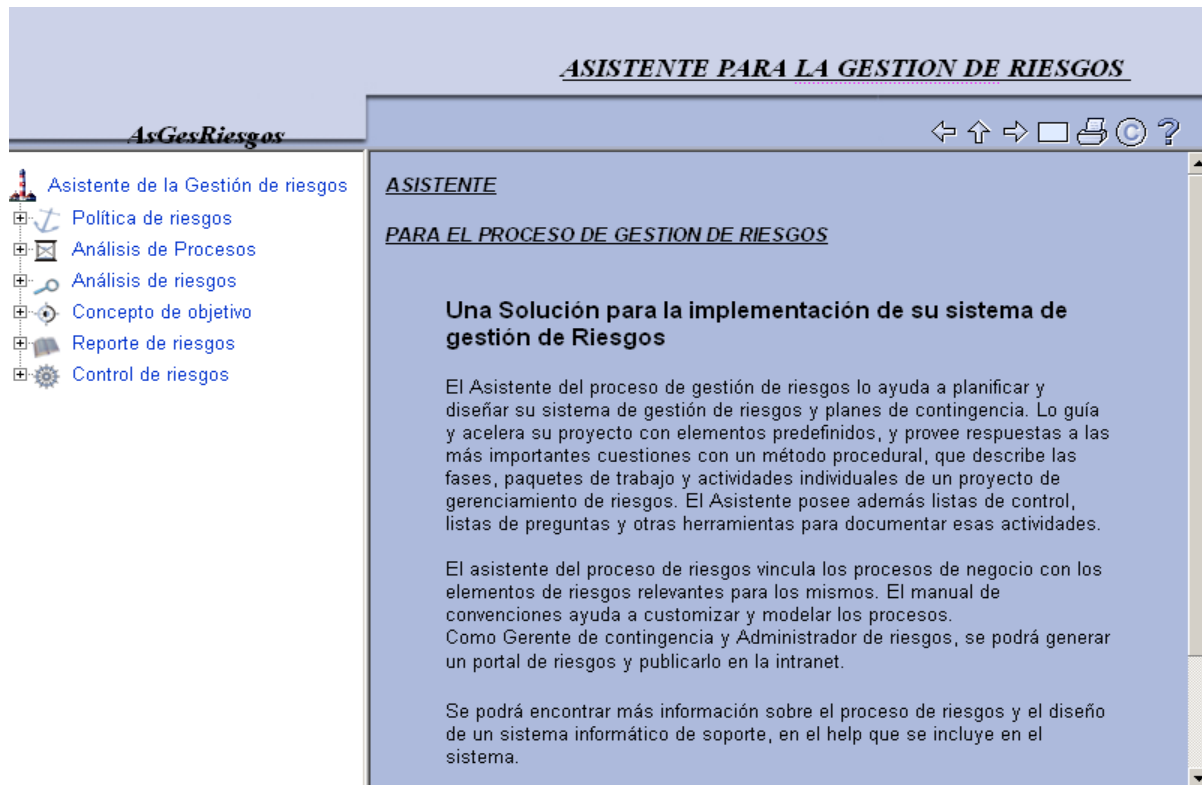
Qué son los íconos del Portal del proceso de riesgos?

Qué es el Proceso de Gestión de riesgos?

Qué es la arquitectura del sistema y los conceptos de seguridad?

Barra de herramientas del Portal de riesgos

A continuación se presentan las pantallas del Sistema enunciado arriba de ayuda a la formulación de proyectos para implementar planes de contingencia y gestionar riesgos basado en análisis de procesos:



Preparación del taller de inicio **FACILITADORES** Espécimen agenda

Objetivo

Una preparación detallada es fundamental para el éxito del taller de inicio. El objetivo es delinear una agenda y establecer las condiciones generales del Workshops.

Precondición

- La asignación del proyecto para implementar un sistema de gerenciamiento de riesgos se ha publicado a nivel compañía.
- Se ha entregado documentación sobre contingencias y riesgos a todos los invitados a participar en el taller.

Procedimiento

- Establecer la lista de participantes del Workshops. Consiga que lo atienda un representante de la gerencia.
- Defina el rol del moderador. Un miembro experimentado del staff o un consultor externo debe ser asignado como moderador del Workshops, manteniendo una posición neutral en su tarea.
- Nominar a alguien para registrar la duración de reuniones.
- Diseñar la agenda.
- Diseñar la lista de expositores que expondrán los tópicos de la agenda.
- Haga que los expositores le envíen por anticipado sus presentaciones..
- Compile la documentación para los participantes.
- Investigue que medios utilizarán los expositores y consiga el equipamiento necesario.
- Reserve un local adecuado. Asegure bebidas y comida para los intervalos.
- Producir las invitaciones en tiempo adecuado y enviarlas con tiempo a los participantes.
- Consultar para confirmar asistencias a invitados a las reuniones.

Resultado

Los participantes y expositores han sido informados en tiempo y forma sobre la reunión prevista de inicio del proyecto de riesgos.

Los recursos necesarios (sala, equipos de proyección, bebidas, etc.) están disponibles para el Workshops.

Realizar el taller de inicio

Taller de inicio

FACILITADORES Ejemplos de factores Críticos de éxito
Minutas de reuniones de un día
Minutas de Proyecto

Objetivo

En el taller de partida del proyecto de la gestión de riesgos se presenta a todo involucrado en el mismo.

El objetivo es para que los participantes aprendan y entiendan la necesidad del proyecto y de sus metas.

Las oportunidades y las mejoras potenciales, tan bien como los riesgos consecuencia del proyecto, se transforman en transparentes. La información detallada presentada a los participantes establece confianza y anima una buena voluntad de apoyar el proyecto y de promover sus ventajas a través de la compañía.

Precondición

- Las preparaciones para el taller de partida son completas y se ha establecido el equipo de proyecto.

Procedimiento

Si es posible, el representante de la gerencia debe asistir a sostener la comisión y la motivación de los involucrados para ejecutar el proyecto.

- Haga que el asesor presente la agenda e introduzca los expositores invitados.
- Introduzca el proyecto, delimitando porqué lo hicieron ser comisionado y cuáles son sus objetivos.
- Contornee las fases del proyecto, los jalones y escala de tiempo previstos.
- Explique la organización del proyecto y las tareas individuales de los miembros de equipo de proyecto.

- Identifique los factores críticos de éxito del proyecto y de los factores de riesgo.
- Establezca junto con el equipo de proyecto que métodos y medios de comunicación se utilizarán, y que períodos de información deben ser desplegados en el proyecto.
- Ofrezca la oportunidad de entrar en la discusión sobre los ítems incluidos en la agenda.
Documente los cambios discutidos.
- Establezca la fundamentación para el cambio aceptado y asegúrese que los participantes están listos y que quieren para ocuparse de los cambios establecidos para el proyecto (gerencia del cambio).
- Intente inculcar el entusiasmo por el proyecto en los participantes.
- Resuma todos los resultados del Workshops en una minuta. Use las minutas para resumir resultados de las reuniones, las minutas han de ser utilizadas en otras reuniones como base de trabajo regular, utilizar un formulario estándar para minutas de proyecto.

Resultado

Los participantes están enterados de las metas del proyecto y los efectos que su logro tendrá en la compañía.

Definición y detalle de estrategias de acción

FACILITADORES Form: Estrategias de acción

Objetivo

El objetivo es discutir con los empleados las varias opciones disponibles para las compañías para hacer frente al riesgo y establecer qué estrategias de acción deben ser implementadas en las cuales casos.

Precondición

- Se definen los términos clave y las categorías de riesgo que se analizarán se han identificado.
- Las unidades que se analizarán y los métodos de análisis se han definido.

Procedimiento

- Mostrar las cuatro estrategias básicas: Evite, reduzca y acepte el riesgo.
- Detallar como trabajan las estrategias basadas en posibles ejemplos.
- Se precisa claramente en un documento de estrategia que acciones se permiten, qué se prohíbe definitivamente, y cuánta libertad es permitida para hacer frente al riesgo.
- Precise las condiciones inequívocas que se deben cumplir para el despliegue de una estrategia específica.

Resultado

Los participantes son conscientes de sus posibilidades de ocuparse del riesgo, y se han definido las reglas para determinar qué estrategia debe ser implementada ante una situación específica.

Documentación de la política de riesgos

FACILITADORES: Ejemplo de Política de Riesgos Documentada

Objetivo

Las decisiones tomadas en las actividades precedentes se deben ahora documentar de una manera comprensible a todos los empleados.

Precondición

- Los instrumentos para la identificación del riesgo se han seleccionado.
- Las unidades que se analizarán se han determinado.
- Se definen las estrategias de acción.

Procedimiento

- Defina el formato del documento de la política del riesgo.
- Documente todas las decisiones tomadas en la forma convenida.
- Publique el documento de tal manera (p.ej. en la Intranet) que todos los empleados afectados tengan acceso a él siempre.
- Comunique los cambios a la política del riesgo que puede surgir de un cambio fundamental en estrategia corporativa general de manera inmediata, y registre los cambios en el documento.

Resultado

Todas las decisiones clave tomadas en lo referente a la política del riesgo están documentadas y disponibles para que puedan verla todos los empleados afectados.

Elaboración de un plan de proyecto

En este paquete de trabajo se planean la previsión estimada de las varias fases y paquetes de trabajo, los hitos y la asignación de los recursos para los procesos individuales implicados.

Se debe prestar atención a todas las interfaces con otros proyectos en términos de asignación de recursos. La consulta siguiente con la gerencia produce el atascamiento del plan documentado que se declara, y todos las demoras de previsión subsecuentes se clasifican como no conformidad.

La elaboración del plan estimado del proyecto abarca dos actividades que se ejecutan en secuencia:

- Desarrollar y planear la adopción del proyecto.
- Planear la puesta al día del plan de proyecto.

Desarrollo y adopción del plan de proyecto

FACILITADORES Espécimen: Plan de proyecto tentativo

Ejemplo: Instrucciones para uso del plan de proyecto

Tentativo

Objetivo

El plan estimado del proyecto precisó la previsión inicial de las varias fases y define las metas de los hitos individuales de cada fase. Las fases del proyecto se identifican en cooperación con los empleados responsables de las demás fases, de tal modo de

obtener el máximo nivel de aceptación entre los empleados y asegurando una mejor adherencia a los plazos del sistema.

Precondición

- Existe un conocimiento básico sobre gestión de riesgos.
- La política de riesgos ha sido definida de acuerdo con la Política Corporativa.

Procedimiento

- Investigar el alcance actual de la operación de la gestión de riesgos.
- Realizar una estimación de la inversión necesaria para implementar un nuevo sistema de gestión de riesgos, o ampliar uno existente, para todas las fases individuales, paquetes de trabajo y actividades del proyecto.
- Defina tentativamente las fases del proyecto y asigne los recursos a las fases individuales. Base su quiebre en las fases del asistente de proceso del riesgos. Para el planeamiento del proyecto utilice el espécimen: Plan tentativo de proyecto; y el ejemplo con las instrucciones detalladas para el uso del plan.
- Convenga la previsión de fechas con todos los miembros del personal implicados y con la gerencia
- Adopte el plan tentativo del proyecto en consulta con la gerencia.
- Ponga el plan tentativo del proyecto a disposición todos los empleados implicados.

Resultado

El plan tentativo del proyecto se ha desarrollado y se ha adoptado en cooperación con los empleados. Consecuentemente, todos los empleados son conscientes de la sincronización total de las tareas y de los puntos por los cuales los hitos individuales deben ser alcanzados.

Actualización del plan tentativo del proyecto

Objetivo

Una vez que se ha desarrollado y se ha adoptado el plan tentativo del proyecto, cambios por ejemplo los que puedan resultar de una carencia de recursos deben ser inmediatamente actualizados y publicados en el plan tentativo del proyecto.

Precondición

- Se ha desarrollado y se ha adoptado el plan tentativo del proyecto.

Procedimiento

- Elija la forma en la cual el plan tentativo del proyecto debe ser mantenido y actualizado y estar continuamente disponible para los empleados. Hágalo libremente por ejemplo accesible en la red.
- Señale que unidades de la organización necesiten ser informadas de cualquier cambio realizado y el personal que necesite además ser informado, y bajo qué

condiciones previas. Por ejemplo, los cambios de menor importancia no necesitan ser notificados directamente a la gerencia, mientras que los cambios que pueden poner en peligro el proyecto completo se deben notificar a la gerencia inmediatamente

- Elija sus métodos de revisar y de aprobar cambios.
- Determine cómo deben ser identificados los cambios, por ejemplo por la marca de color o similar, y cerciórese de que exista un sistema para señalar las distintas versiones del plan del proyecto.
- Defina la forma con la cual se notifican los cambios, P. Ej. por el e-mail o el correo interno convencional. Elija el medio de información más rápido y más eficiente.

Resultado

El plan tentativo del proyecto está continuamente actualizado. Los cambios se informan inmediatamente a la gente / a las unidades apropiadas y se documentan para que todos los consideren

Revisión de la política de riesgos

FACILITADORES Check list: Revisión de la Política de Riesgos

Objetivo

La revisión de la política de riesgos asegura de que todos los pasos en la fase referida se hayan ejecutado.

Precondición

- Los paquetes de trabajo de la fase de la política del riesgo se han ejecutado.

Procedimiento

- Invite a la gerencia representativa y a los empleados implicados en las varias fases, a una reunión de la revisión.
- Elabore en común una descripción de los paquetes de trabajo terminados.
- Presente el resultado obtenido hasta ahora de sus paquetes de trabajo a los miembros del personal relevantes.
- Determine los resultados de los pasos individuales en una discusión de grupo.
- Discuta y documente las iniciativas de la mejora.
- Supervise la puesta en práctica de las iniciativas de la mejora y repase su eficacia.
- Publique un informe detallado a todos los participantes.

Resultado

La ejecución de los paquetes de trabajo individuales se ha revisado y se ha determinado. Las mejoras también se han analizado y decidido, y se están supervisando.

Análisis de Procesos

La fundamentación para la puesta en práctica de un sistema orientado al proceso de la gestión de riesgos es el conocimiento detallado de la estructura y de los procesos de la compañía.

Pero antes los procesos y las estructuras de la organización deben ser analizadas y documentadas con un SOFTWARE PARA MODELIZACIÓN DE PROCESOS, se debe realizar un taller para determinar las convenciones de modelado y precisar un lenguaje común y un modo unificados de modelado.

Por análisis y documentación de la organización y de los procesos definidos en la política de riesgos usando el software de modelización seleccionado, las estructuras se

hacen transparentes a los empleados y el paso siguiente - identificación del riesgo - se hace más fácil.

El asistente del proceso de riesgos proporciona la ayuda eficaz en este proceso, usando las herramientas siguientes:

- Lista de modelos importantes
- Ejemplo de niveles de modelización
- Espécimen: Manual de convenciones
- Espécimen: estructura organizacional
- Espécimen: concepto de rol
- Formulario: Identificación de procesos de negocio
- Ejemplo: Modelización de procesos
- Check list: Revisión de análisis de procesos

Workshops de convenciones

Antes del modelado de procesos con el SOFTWARE DE MODELIZACIÓN DE PROCESOS, las convenciones del modelado para la compañía deben ser establecidas. Esto asegura un modelado unificado, adaptado exacto a las necesidades de la compañía, incluso cuando es realizado por diversos grupos de gente y de proyecto. En el taller de convenciones se realizan las actividades siguientes:

- Seleccionar métodos de modelado
- Definir niveles de modelado
- Definir convenciones gráficas

Selección de métodos de modelado

FACILITADORES Lista de tipos de modelos importantes

Objetivo

Existen diferentes herramientas y tipos de modelado, para modelar diferentes procesos. Consecuentemente, el objetivo de este paso es definir los métodos

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

relevantes de modelización para el proyecto e integrarlos en cualquier convención de modelización existente.

Precondición

- El team de proyecto está determinado
- La política de riesgos, en particular, los puntos de intersección con otros proyectos están definidos.

Procedimiento

- Delinee los varios procesos que se modelarán.
- Explique los diversos tipos modelo y su uso.
- Discuta en el grupo los tipos modelo que mejor adhieren con los procesos a modelar.
- Documente los resultados en minutas.
- Establezca una plantilla de objetos y modelos estándar a utilizar.

Resultado

El team de proyecto a determinado las convenciones de objetos y modelos a utilizar para levantar el mapeo de los procesos.

Definición de niveles de modelado

FACILITADORES Ejemplo de Niveles de modelización

Objetivo

Al definir niveles de modelado, es importante asegurar una navegación de arriba abajo en el uso de los modelos. Los participantes deben crear una estructura intuitiva y realizable para modelar.

Precondición

- Los tipos de modelo han sido definidos.

Procedimiento

- Comience con la definición del nivel superior. Defina los tipos modelo que se utilizarán aquí.
- Entonces defina el nivel de detalle hasta el cuál usted quiere modelar.
- Determine los tipos modelo para los otros niveles definidos.
- También defina una estructura del grupo lógico para el proyecto y los niveles de modelado (con un concepto apropiado de la autorización de acceso) en el software de modelización.

Resultado

Una estructura utilizable para la base de datos queda definida.

Definición de convenciones gráficas

FACILITADORES Espécimen: Manual de Convenciones

Objetivo

Para asegurar el máximo a los empleados, es esencial fijar a convenciones gráficas unificadas. Ésta es la única manera de asegurarse que los empleados pueden navegar alrededor de los modelos documentados en el software de modelización de procesos,

razonablemente rápidamente y eficientemente. Pueden ser utilizadas las convenciones del manual del proceso del Asistente de gestión de riesgos como plantilla.

Precondición

- Tipos de modelos y niveles de modelización están definidos.

Procedimiento

- Analice diversos modelos y decida si su vista y sensación adhiere con su filosofía corporativa. Por ejemplo, porque su proceso que modela en el software de modelización de procesos usted puede utilizar el Diagrama de procesos o el diagrama de actividades de UML.
- Resuelva a las convenciones que representen las condiciones generales en su compañía.
- Limite el número de tipos de objeto usados en sus modelos del software de modelización de procesos al mínimo necesario para su compañía y sus objetivos del sistema, para no sobrecargar a sus empleados.
- Los modelos deben ser fáciles e intuitivos leer. Determine por lo tanto la extensión máxima de los modelos.
- Adapte el filtro del software de modelización por procesos para su proyecto de gestión de riesgos según las convenciones precisadas en el manual de convenciones.

Resultado

Se han definido y documentado las convenciones gráficas unificadas como guía para todos los modeladores.

Determinar la estructura de la organización y sus responsabilidades

La claridad y la transparencia con respecto a responsabilidades son esenciales para la creación acertada y la mejora continua de un sistema de la gestión de riesgos. El objetivo de este paquete de trabajo es identificar y señalar responsabilidades y asignarlas al personal apropiado. Con este fin es sensible y recomendable hacer uso de los actuales resultados. Esto se relaciona, particularmente, con:

- Detalle en contratos de empleo.
- Descripciones de las funciones/descripción de tareas.
- Procedimientos documentados.
- Instrucciones de trabajo documentadas.
- Especificaciones en otros documentos (minutas de reuniones, de notas internas, de etc.).

El proceso de revisar, de poner al día y de documentar la estructura de la organización y las responsabilidades asociadas abarca dos actividades que se realizan a través de una secuencia:

- Recolectando y poniendo al día la estructura de organización.
- Recolectando y poniendo al día responsabilidades

Compaginando y poniendo al día la estructura de organización

FACILITADORES Espécimen estructura organizacional

Objetivo

Después de ejecutar de este paquete de trabajo, los documentos (cartas jerárquicas de organización) estarán disponibles proporcionando una descripción clara de la

estructura de organización actual. La definición de los términos usados dentro de la compañía para identificar posiciones está establecido. Por ejemplo, está claro si una posición está descrita como siendo " distribución" o "Ventas" en los procedimientos documentados.

Precondición

- Se ha establecido una estructura de organización básica sana. Una fase de substancial cambia a la estructura de organización, implicando las decisiones de principio fundamentales que están todavía pendientes, está previniendo la ejecución acertada de esta actividad.
- No se planea ningún cambio en el futuro próximo independiente de la estructura de organización del desarrollo del sistema de gestión de riesgos.

Procedimiento

- Recolecte los documentos disponibles en la compañía que explican la estructura de la organización. Esto se relaciona con las presentaciones empresariales y las presentaciones de la estructura de organización dentro de las unidades de negocio y de los departamentos.
- Elabore una descripción de la información recibida basada en una carta de estructura de la organización en el software de modelización y actualice la base de datos en su sistema de la gestión de riesgos.
- Compruebe la plausibilidad y consistencia de la presentación con respecto a los términos usados y a las asignaciones hechas. Presente

- Presente los resultados a la gerencia de la compañía/a la junta directiva.
- Informe a la gerencia/la junta directiva el control y confirme que la presentación es hasta la fecha.
- Solicite a la gerencia/la junta directiva poner al día la presentación empresarial de la estructura de la organización según las necesidades.
- Presente a los departamentos de publicación/el control de unidades y apruebe la presentación actualizada de la estructura de la organización.
- Defina los documentos apropiados que muestren los procedimientos de control y permita ilustrar la estructura de la organización (identificación de persona/ unidad de publicación, identificación del estado de la revisión, definición y documentación de la lista de distribución, definición de los procedimientos de distribución y de modificación, etc.).
- Asegúrese de que las versiones hasta la fecha de los documentos que ilustran la estructura de organización estén puestos a disposición las personas/ unidades especificados. Usted puede utilizar para esto las últimas cartas de estructura de la organización actualizadas de su portal de proceso del riesgo.
- Asegúrese de que al cambiar la estructura de organización y los términos usados, las versiones hasta la fecha de los documentos correspondientes estén modificadas y redistribuidas o hechas accesibles.
- Asegúrese de que el equipo de proyecto tenga siempre los documentos válidos que explican la estructura de la organización.

Resultado

La compañía tiene una explicación documentada, hasta la fecha, plausible y constante de la estructura de la organización. Los métodos convenientes (tales como uso del software de modelización y del portal del proceso de riesgos) se aseguran de que los documentos que ilustran la estructura de organización estén actualizados hasta la fecha

Recolección y actualización de roles y responsabilidades

FACILITADORES Espécimen: Conceptos de Roles

Objetivo

Después de ejecutar este paquete de trabajo, estarán disponibles los documentos que proporcionan una descripción clara de las responsabilidades actuales. La definición de los términos usados dentro de la compañía para identificar posiciones y responsabilidades está disponible. Es bien definido, por ejemplo, si una persona o una posición satisface el rol de un dueño del riesgo o de un encargado de riesgo dentro del sistema de gestión de riesgos.

Precondición

- Una sana estructura básica de responsabilidades se ha establecido. Una fase de substancial cambia a las responsabilidades, implicando las decisiones de principio fundamentales que son todavía pendientes, está previniendo la ejecución acertada de este paquete de trabajo.
- No se planea ningunos cambios a la independiente de las responsabilidades del desarrollo del sistema de la gestión de riesgos en el futuro próximo.

Procedimiento

- Recolecte los documentos disponibles para la compañía que explican responsabilidades. Esto se relaciona con las presentaciones empresariales así como

con las ilustraciones de las responsabilidades dentro de unidades de negocio/de departamentos.

- Elabore una descripción de la información recibida. Utilice la carta de la estructura de la organización.

- Defina exactamente los roles y las responsabilidades de los dueños del riesgo y de los encargados de riesgo en su sistema de la gestión de riesgos. Utilice el "espécimen concepto de roles"; para detallar los roles.

- Compruebe la plausibilidad y consistencia de la presentación con respecto a los términos usados y a las asignaciones realizadas.

- Presente los resultados a la gerencia de la compañía/ a la junta directiva.

- Haga que la gerencia/ la junta directiva controle la presentación hasta la fecha y, según las necesidades, haga que la gerencia/la junta directiva ponga al día la carta empresarial de responsabilidades.

- Haga el control de publicación de las personas/de unidades y apruebe la carta actualizada de responsabilidades.

- Defina los documentos apropiados de procedimientos de gestión para ilustrar las responsabilidades (identificación de la posición de publicación, identificación del estado de la revisión, definición y documentación de la lista de distribución, definición de los procedimientos de la distribución y de modificación, etc.),

- Asegúrese de que la versión hasta la fecha actual de los documentos que ilustran responsabilidades esté puesta a disposición de las posiciones especificadas,

- Asegúrese de que al cambiar responsabilidades y los términos usados, la versión hasta la fecha de los documentos correspondientes esté modificada y redistribuida o hecha accesible.
- Asegúrese de que el equipo de proyecto tenga siempre los documentos válidos que explican responsabilidades.

Resultado

La compañía tiene una carta documentada, hasta la fecha, plausible y constante de responsabilidades en el sistema de la gestión de riesgos. Los métodos y los medios convenientes de información (tales como el portal de proceso de riesgos) se aseguran de que los documentos que ilustran las responsabilidades estén mantenidos hasta la fecha.

Análisis de los procesos de negocio críticos

Antes de que los riesgos en procesos puedan ser identificados, los flujos de proceso específicos deben ser conocidos. Un proceso transforma especificaciones en resultados con la ayuda de los mecanismos que son controlados por un sistema de gestión. La especificación, la gerencia y/o los resultados pueden ser tangibles o intangibles. El resultado de un proceso puede ser la especificación para otro proceso. Consecuentemente, los procesos se pueden representar en una cadena de procesos. El método a utilizar debe contemplar un modelo de proceso que incluya, datos, responsables (puestos) y lógica.

- Preparación de análisis de proceso de negocio
- Taller del análisis de proceso de

- Documentación de procesos de negocio

Preparación de análisis de proceso de negocio

Objetivo

Para un análisis adecuado de proceso de negocio, un número importante de actividades de preparación deben ser realizadas.

El factor clave es que se ha compaginado toda la documentación necesaria, de modo que usted tenga siempre una descripción clara.

Precondición

- El análisis de los procesos de negocio críticos se ha decidido comenzar, y los procesos críticos se han identificado en la fase "Definición de las unidades a ser analizadas".

.

Procedimiento

Procedimiento

- Notifique a los participantes sobre el taller y consiga que lo atienda un miembro de la gerencia.
- Nomine al moderador del taller. Los candidatos potenciales al rol son un miembro del personal experimentado o un consultor externo.
- Establezca la agenda.
- Compagine la documentación que precise la estructura de organización y las responsabilidades y cerciórese de que todos los participantes están familiarizados con la documentación de antemano.

- Cerciórese de que las premisas y los recursos necesarios para el taller (retroproyector, PC, etc.) estén disponibles.
- Como material informativo previamente, distribuya a los participantes una introducción al tema del análisis de proceso de negocio.
- Prepare la documentación y otras ayudas de modo que todos los participantes puedan documentar los procesos ellos mismos en el taller.
- Prepare las descripciones de proceso existentes como material de la entrada para el taller
- Haga que los participantes confirmen su asistencia al taller.

Resultado

Se han designado y se han notificado a los participantes sobre el taller en tiempo adecuado.

Los recursos necesarios (sitio, flipchart, cañón, PC, etc.) y la documentación están disponibles.

Documentar los procesos de negocios

FACILITADORES Ejemplo:
modelo de proceso (utilizando ARIS)

Objetivo

Los procesos identificados en el taller del análisis de procesos de negocio se documentan con el juego de herramientas del software de modelización determinado y así que se hacen visibles para todos los empleados.

Precondición

- Se determinan y se analizan todos los procesos previamente efinidos

.

Procedimiento

- Nombre la gente o las unidades/los departamentos responsables de la documentación de proceso.
- Cerciórese de que conozcan a las convenciones de modelado predefinidas a cada uno
- Permita que los responsables del personal de la documentación realizar un curso en técnicas de documentación y la funcionalidad del juego de herramientas de modelización determinado.
- Promueva la comunicación entre el personal responsable de la documentación y el personal afectado por medio de reuniones regulares de proyecto. Utilice unos minutos del proyecto para las reuniones regulares del proyecto.
- Cerciórese de que la exactitud de los procesos documentados haya sido comprobada por el personal responsable especializado.
- También documente a los dueños de proceso designados. Para hacer así pues, en el diagrama de cadena de valor agregado del nivel superior cree un diagrama de asignación de función para las funciones respectivas. En este diagrama de asignación de función los dueños del proceso son modelados sobre la función correspondiente por la conexión: "es el responsable para" como técnico responsable. Son responsables de todos los subordinados de los procesos a esta función dentro de la jerarquía de procesos.

Resultado

Todos los procesos analizados se han documentado y se han comprobado en cooperación con los encargados de la documentación y los empleados que trabajaban en los procesos relevantes. Un modo comprensible, intuitivo de presentación fue

empleado, en conformidad con todas las convenciones de modelado definidas previamente.

Revisión de análisis de procesos

FACILITADORES Check list:

Revisión del análisis de procesos

Objetivo

La revisión del análisis de procesos se asegura de que todos los pasos en la fase referida se hayan ejecutado.

Precondición

- Los paquetes de trabajo de la fase de análisis de procesos se han ejecutado.

Procedimiento

- Invite a la gerencia representativa y a los empleados implicados en varias fases a una reunión de revisión.
- Elabore en común una descripción de los paquetes de trabajo terminados.
- Haga que los miembros del personal responsables presenten los resultados hasta ahora y el estado de sus paquetes de trabajo.
- Determine los resultados de los pasos individuales en una discusión de grupo.
- Discuta y documente las iniciativas de mejora.
- Supervise la puesta en práctica de las iniciativas de la mejora y repase su eficacia.
- Publique un sistema de minutas detallado a todos los participantes. Utilice las minutas para las reuniones que se realicen.

Resultado

La ejecución de los paquetes de trabajo individuales se han determinado y se han revisado. Las mejoras también se han decidido realizar, y se están supervisando.

Análisis de riesgos

Para ser eficaz la gestión de riesgos y responder puntualmente y adecuadamente a los desarrollos negativos o a los peligros potenciales, los procesos de negocio deben sujetarse al análisis detallado de riesgos. Los procesos de valor agregado, en particular, se deben analizar en términos de riesgos inherentes y sus interacciones. Los datos internos y externos también ayudan a analizar el la situación de riesgo de la compañía.

El análisis de riesgo cubre la identificación del riesgo así como la valoración del riesgo. La valoración entrega los datos necesarios para las fases río abajo y, particularmente, para la información de riesgo y la supervisión. Los datos se pueden documentar con el software de modelización seleccionado y los acontecimientos específicos del riesgo compaginados en una base de datos de pérdidas.

El Asistente de Gestión de riesgos provee soporte efectivo en el proceso, permitiendo utilizar las siguientes herramientas:

- Guía para entrevistas de análisis de riesgos
- Formulario: check list de Riesgos
- Formulario: Hoja de análisis de Riesgos
- Resumen de los métodos utilizables para modelar procesos y riesgos
- Ejemplo de categorización de riesgos
- Ejemplo: Modelización de Riesgos
- Espécimen: tabla de colores
- Espécimen: Estructura CRM de la base de datos de pérdidas
- Check list: Revisión de análisis de Riesgos

Identificación y determinación del riesgo

El proceso de la identificación del riesgo pregunta los empleados y a los dueños de proceso como expertos en su propio trabajo cotidiano como los auditores internos, el personal del departamento de organización y, en caso pertinente, el personal que controla el riesgo.

Estos departamentos pueden incorporar en el análisis su experiencia en el manejo del riesgo estructural (por ejemplo en presentar la prueba e informes de auditoría). Con sus propios puntos de vista, pueden ayudar a esclarecer los aspectos no considerados por los dueños de proceso y a mostrar subjetivas visiones objetivas.

En este proceso, los riesgos se determinan en base de la valoración de los datos históricos o del experto según su frecuencia de la ocurrencia y el grado de la pérdida resultante. Si la frecuencia de la ocurrencia no se sabe, el riesgo se puede determinar por la probabilidad concerniente al número de ejecuciones de las funciones.

Los controles y las contramedidas existentes también se analizan y se documentan.

La evaluación de datos externos puede contribuir con nuevos resultados en lo referente a riesgo potencial. La pérdida importante ocurre muy infrecuentemente, y por lo tanto no se detecta ni puede a menudo ser estimada.

La fase de la determinación y de la evaluación del riesgo abarca cuatro actividades, que se funcionan con en secuencia:

- Análisis de los procesos definidos
- Evaluación de pérdidas y datos externos
- Importancia del riesgo
- Derivación de iniciativas

Identificación de Riesgos basada en los procesos

FACILITADORES Guía de entrevista para análisis de riesgos
Form: Lista de control de riesgos

Form: Formulario de análisis de riesgos

Objetivo

El objetivo de este paquete de trabajo es identificar la existencia y riesgos potenciales en los procesos documentados.

Precondición

- Las unidades y los procesos de negocio que se analizarán se definen y se documentan.
- Los encargados de cada unidad y los dueños de proceso son informados.

Procedimiento

- Establezca las metas que usted quisiera que el departamento (grupo) lograra.
- Identifique los riesgos en los procesos y en las funciones individuales de los procesos por medio del método previamente seleccionado.
- También analice los procesos, por ejemplo, con el objeto de: el proceso múltiple y los lazos posteriores, ayudas manual/papel a los proceso, a la entrada de datos manual en vez de entrada automatizada, a las roturas de los medios (papel/software), a la calidad inadecuada de la ayuda de sistema, entrada de datos redundantes en diversos sistemas, carencia de interfaces entre sistemas, la infraestructura heterogénea y anticuada.
- Identifique los controles y las contramedidas existentes para reducir el riesgo (análisis de la situación real).
- Compruebe si hay defectos en el sistema de monitoreo existente.

Resultado

Los participantes han identificado los riesgos potenciales en las unidades y los procesos relevantes de negocio y se han hecho más sensibles a la identificación de riesgos adicionales en sus propias áreas.

Evaluación de pérdidas y datos externos

Objetivo

El análisis de datos de casos históricos de pérdida y de datos externos facilita y promueve la construcción de una base de datos de pérdidas. Un efecto secundario deseable es la facilidad para identificar otros puntos débiles en los procesos o en el sistema de control.

Precondición

- Los procesos bajo análisis se han investigado completamente en términos de existencia de riesgo y riesgo potencial.

Procedimiento

- Compagine los documentos internos que pueden contener datos potenciales de pérdida, tales como informes de auditoria de proceso, los informes de los auditores financieros, documentos del departamento jurídico (tal como casos fraudes, de las demandas de clientes, etc.), ÉL departamento de IT (tal como fallas del sistema registros de fallas. etc.), y de contralor, de personal, y de otros departamentos.
- Antes de procurar conjuntos de datos de iniciativas externas o de vendedores comerciales, controle en cual de las áreas del negocio los datos ofrecidos se originan. Compruebe cómo de comprensivo y completo son los datos. Los conjuntos de datos externos son problemáticos cuando los criterios que serían necesarios agregarlos a la base de datos interna siguen siendo desconocidos. Estos criterios incluyen, por ejemplo, el tamaño de la compañía, de la estructura, del procedimiento de la clasificación del riesgo, de la calidad de las estructuras internas del proceso y de control, del sistema legislativo del país referido, del etc.
- Analice qué riesgos de los conjuntos de datos que se han identificado en los varios procesos analizados en la actividad precedente.
- Marque los riesgos no previamente identificados en los procesos. Controle en que procesos y las funciones los riesgos ocurrieron en el pasado.

Resultado

Todos los riesgos que se presentaban en los conjuntos de datos se han comprobado y se ha identificado cualquier riesgo previamente no percibido.

Valoración del riesgo

FACILITADORES Overview de varios métodos de categorización de riesgos

Objetivo

En esta fase los riesgos identificados previamente en base al conocimiento de expertos o del análisis de datos se determinan en términos de grado de la pérdida resultante y frecuencia de la ocurrencia.

Precondición

- En los procesos bajo análisis han sido completamente determinados los riesgos.
- Se ha completado el análisis de los conjuntos de datos para los riesgos previamente no detectados.

Procedimiento

- Determine el grado en el cual el logro de metas es puesto en peligro por los riesgos identificados en el curso de una sesión de la reunión de reflexión. Primero establezca las clases de pérdida para que los encargados puedan hacer una valoración simplificada del riesgo.
- Elija uno de los tres métodos de valoración ofrecidos por la metodología de gestión de riesgos: Método general, orientado a proceso u orientado a simulación. Tome cuenta de las condiciones generales asociadas a los métodos respectivos de valoración.
- Resuelva los grados posibles de pérdida resultante del riesgo y de la frecuencia de su ocurrencia (por año), en lo posible basados en un sistema de ranking de tres puntos

(lo más bajo posible, frecuencia media y más alta del valor de la ocurrencia y de la pérdida). Las dificultades en la determinación de riesgos individuales pueden ser remediadas comparándolos contra riesgos conocidos y ya determinados. Estime las frecuencias de la ocurrencia explorando los períodos específicos (P.Ej. cada cuántos años arriesgan XY ocurra?). De aquí, la frecuencia anual de la ocurrencia se puede pronosticar mucho más exactamente.

- Si usted quiere un análisis orientado a procesos u orientado a simulación, analice cuántas veces el riesgo de la función o del proceso ocurre en las ejecuciones de la función o del proceso correspondiente (probabilidad relativa de la ocurrencia). En el caso del método orientado a proceso también es necesario determinar la función en la cual el riesgo ocurre en términos de su frecuencia por año.
- Determine la eficacia de las medidas existentes por la reducción de la frecuencia de ocurrencia y del nivel de pérdida consecuencia del riesgo. Usted debe también calcular el costo de las iniciativas y registrar y mantener el costo como una atributo en el sistema de gestión de riesgos.
- Documente los defectos detectados (P.ej. controles ineficaces, mecanismos de palanca o iniciativas ineficaces) y marque los riesgos residuales (riesgo incontrolado).
- Tome una decisión consciente dentro del grupo donde el nivel de riesgo residual es aceptable (en términos de costo/beneficio).

Resultado

Todos los riesgos identificados se han determinado y se han analizado.

Derivación de iniciativas

FACILITADORES Ejemplo de una categorización de riesgos

Objetivo

En esta fase los riesgos se categorizan y se asignan a las estrategias de acción definidas en la política de riesgos en base de los resultados del análisis de riesgo realizado. También se investigan, las iniciativas potenciales de reducción del riesgo dentro de estas estrategias de la acción.

Precondición

- Las estrategias de la acción se definen en la política del riesgo.
- Los riesgos identificados se han determinado y se han analizado en los modelos de proceso documentados.

Procedimiento

- Defina las categorías de riesgo tales como "riesgos de proceso", "riesgos de personal", "riesgos de sistemas", etc. y asignar los riesgos a categorías correspondientes.
- Clasifique los riesgos dentro de la matriz de toma de decisión definida en la política del riesgo.
- Defina las iniciativas potenciales para todos los riesgos dentro de la estrategia de acciones.
- Compruebe si la situación de riesgo se puede mejorar, por ejemplo mediante la optimización de los procesos organizacionales, y derive las iniciativas potenciales para cambiar la organización.
- Compruebe si los riesgos identificados pueden ser optimizados por puntos de control adicionales en el flujo del proceso y derivar iniciativas potenciales.
- De acuerdo con varios escenarios, investigue nuevamente el efecto de las iniciativas definidas sobre el riesgo en términos de reducción de su frecuencia de ocurrencia y/o de la pérdida resultante.
- Determine los costos de las medidas individuales.
- También considere las interacciones posibles entre diversas iniciativas en términos de efecto y de costo. El efecto de una medida puede ser reducido o aún consolidado por otra medida, por ejemplo, y el costo de una medida puede ser reducido por la terminación simultánea de otra medida (ejemplo: seguro).

Resultado

Después de la clasificación áspera de los riesgos por estrategia de las acciones, las iniciativas se han derivado y se han analizado en términos de su efecto sobre el riesgo y en términos de costos. Al hacer eso, se consideraron las interacciones entre las iniciativas múltiples.

Documentación de Riesgos

Solamente la documentación constante del riesgo permite el pronóstico de largo plazo del potencial del riesgo de su compañía. Esto se alcanza usando los modelos y los métodos en la base de datos de riesgos desarrollado especialmente para las necesidades de la gestión de riesgos. De acuerdo con el modelado en el software de modelización, el portal de proceso de riesgos se puede entonces generar de juego de herramientas del modelador en una fase subsecuente. El portal de proceso de riesgos procesa el riesgo y los análisis de proceso en diversas variaciones y para diversas necesidades. Para poder evaluar riesgo real y los datos asociados, es recomendable compaginar los datos en una base de datos de pérdidas, que se puede construir en base de la estructura colocada en el software de modelización e integrada en el portal de proceso de riesgos.

La fase de la documentación del riesgo abarca dos actividades, que se ejecutan en orden:

- Presentación de información de riesgos en el software de modelización
- Construcción de una base de datos de pérdidas

Presentación de la información de riesgos en la base de datos de riesgos

FACILITADORES Ejemplo: Modelo de riesgos Especímen: Tabla de Colores

Objetivo

Los riesgos previamente identificados y ahora determinados necesitan ser Documentados tan exactamente y claramente como sea posible usando el software de modelización. Los procesos modelados en la fase de análisis de procesos también se utilizan para esto.

Precondición

- Los procesos bajo análisis se documentan con el software de modelización.
- La fase de la determinación y de la evaluación del riesgo es completa.

Procedimiento

- Elabore de parte inferior hacia arriba en la jerarquía de proceso y modele los riesgos en las funciones identificadas y los procesos seleccionando el tipo de objeto "Riesgo" y utilice la conexión; "ocurre en" a la función en la cual el riesgo ocurre. Utilice un "diagrama de asignación de recursos " de la función; almacenado para la función (recomendada) si el riesgo ocurre igualmente en la misma función ubicada en otros procesos, o modela el riesgo en casos excepcionales en el mismo modelo de proceso si se aplica solamente en este proceso específico de manera precisa en esta función.
- Modele los riesgos que afectan a todos los procesos y que no puede ser asignado a un solo proceso o función, incluyendo el riesgo en el nivel superior del modelado de procesos. Estos riesgos se pueden ligar en el nivel superior a algunas funciones del diagrama de cadena de valor agregado en la conexión; "ocurre en", por ejemplo. Entonces afectan a todos los procesos debajo de ese nivel en la jerarquía de procesos.
- La valoración del riesgo puede ser administrada en los objetos de riesgos modelados en el atributo administración del riesgo. Deben ser mantenidos el máximo, promedio y mínima frecuencia y monto de pérdida por daños identificados en la valoración del riesgo.

- Si por ejemplo se ha identificado la probabilidad de ocurrencia conviene mantenerlo como un atributo del link hacia la función en lugar de un atributo del objeto de riesgos.
- Estos datos pueden ser recuperados por el Gerente de performance e importados a Excel para análisis.
- Si no se conoce el número exacto de ejecuciones anuales, se puede simular el comportamiento del proceso durante un período determinado.
- Ahora registre la identificación de iniciativas en un "diagrama de indicador clave de performance". Se debe documentar el costo de la iniciativa, los efectos de la iniciativa sobre el riesgo y el dueño del riesgo que tiene la responsabilidad de la iniciativa.
- Crear un modelo del "Diagrama de riesgos" escriba en qué categoría está cada riesgo identificado. Las categorías pueden también tener subcategorías de otras categorías. Para permitir la codificación poli cromática de las categorías - y de los riesgos, es recomendable asignar a las varias categorías un color en código de color específico.

Resultado

Todos los riesgos identificados se han modelado en el software de modelización para las funciones de los procesos claves y la valoración ha sido documentada manteniendo los atributos actualizados de riesgo.

Construcción de una base de datos de pérdidas

FACILITADORES Espécimen: ERM de la estructura de una base de datos de Pérdidas

Objetivo

El haber identificado, los riesgos potenciales y los ya existentes implica supervisar en términos de su ocurrencia y pérdida real contraída en cada caso. Los eventos concretos del riesgo se deben por lo tanto compaginar en una base de datos de pérdidas. De los datos recopilados, las conclusiones se pueden entonces extraer en cuanto a su cantidad media de daños y de frecuencias de ocurrencia para concretizar cualquier estimación inicial en un cierto plazo.

Precondición

- Se han identificado y se han documentado los riesgos posibles.

Procedimiento

- La estructura básica de la base de datos de pérdidas se establece según las categorías de riesgos en el diagrama de riesgos modelado, para asegurar la integración.
- Las campos de información siguientes referentes a la ocurrencia de un riesgo específico se deben completar siempre: Categoría de pérdida, lugar de la ocurrencia, fecha y hora del evento de la pérdida, valor de la pérdida, correlaciones entre las causas, localizaciones del daño y casos de la pérdida, así como el dueño del riesgo. Para definir su uso en la base de datos de pérdidas utilizar el diagrama de entidades y relaciones (ERM).
- Usted puede modificar una base de datos existente de pérdidas para requisitos particulares o crear una nueva para incluir en el sistema de gestión de riesgos.
- Cerciórese de que solamente el encargado de riesgo tenga/tiene acceso a todos los datos en la base de datos, e informe a los dueños del riesgo de las competencias relevantes.

Resultado

La estructura de la base de datos se ha establecido y todas las responsabilidades de mantenerla se han definido y se han comunicado a los dueños de los riesgos.

Revisión de análisis de Riesgos

FACILITADORES Check list: Revisión de análisis de riesgos

Objetivo

La revisión del análisis de riesgo asegura de que todos los pasos de esta fase se han ejecutado.

Precondición

- Los paquetes de trabajo de la fase de la identificación del riesgo han terminado.

Procedimiento

- Invite a un representante de la gerencia y al personal involucrado en las fases individuales a una reunión de la revisión.
- Elabore una descripción de los paquetes de trabajo terminados.
- Haga que los miembros relevantes del personal presenten los resultados y el estado de sus paquetes de trabajo respectivos.
- Determine los resultados de los pasos individuales en una discusión de grupo.
- Supervise la conformidad con las acciones de mejora propuestas y repase su eficacia.
- Discuta y documente las acciones de la mejora.
- Publique un informe detallado a todos los participantes.

Resultado

La ejecución de los paquetes de trabajo individuales se han revisado y se han determinado. También, las mejoras se han decidido ejecutar y se están supervisando

.

Concepto objetivo

Cada proyecto debe ser económicamente justificado y entregar siempre un cociente positivo del costo/beneficio.

El concepto de "el riesgo orientado a la optimización de los procesos de negocio; permite dos objetivos a ser logrados, a partir de una base común (de los datos). En primer lugar se alcanza el objetivo primario - la gerencia del riesgo operacional y salvaguardia de procesos -. Al mismo tiempo, los procesos de negocio bajo análisis también se optimizan y así se hacen más eficientes y rentables.

La calidad superior del proceso, en el sentido de procesos seguros y eficientes, es el criterio primario en el cual la reestructuración del riesgo debe ser basada la optimización de la vista del proceso. La visión del nuevo proceso debe ser eficiente en términos de optimización del riesgo operacional - es decir, el gasto en la ejecución de iniciativas no debe exceder el riesgo potencial.

Si los procesos no se pueden salvaguardar completamente por iniciativas o la reestructuración, por contingencia crítica de los riesgos y procesos alternativos y procesos para control de los indicadores clave del riesgo deben ser definidos.

El Asistente del proceso de riesgos proporciona la ayuda eficaz en esto, incluyendo las herramientas siguientes:

- Ejemplo de un proceso de contingencia en caso de fuego
- Check list: revisión del concepto objetivo

Optimización de Procesos de Negocio

A menudo las actividades se realizan de cierta manera porque se siempre se han hecho de esa manera. En operaciones cotidianas la pregunta porqué las copias múltiples de algunos documentos se producen y se distribuyen a una gama de diversos departamentos y de gente se hace raramente. Hay también a menudo una carencia de la comunicación interna, porque las estructuras no se fijan para ella y los individuos no tienen ninguna comprensión del cuadro total.

Los requisitos de proceso para algunos documentos y procedimientos bien pueden haber cambiado en un cierto plazo. Pero el flujo de trabajo no se ha adaptado a las

nuevas demandas. Por todas estas razones, la optimización y la mejora continua de los procesos de negocio es sumamente importante.

Estas estructuras establecidas desde hace mucho tiempo dan lugar a menudo a potencial creciente del riesgo en procesos de negocio individuales. El potencial del riesgo de los procesos y de las funciones individuales se pueden documentar por medio de análisis de riesgo orientado proceso.

El análisis de riesgo también identifica los riesgos posibles que no pueden ser rechazados alterando los procesos. Pueden, sin embargo, ser reducidos definiendo las iniciativas específicas identificadas y determinadas ya en análisis de riesgo.

La optimización de los procesos de negocio abarca dos actividades, que se ejecutan en orden secuencial:

- Optimización de los procesos de la organización
- Definición de iniciativas

Definición de iniciativas

Objetivo

Para los riesgos que no se pueden remediar por la optimización de procesos, se definen las iniciativas concretas para reducir la cantidad de daños y/o la frecuencia de la ocurrencia del riesgo.

En particular los conceptos de planes de contingencia son útiles para entender las iniciativas a producir para mitigar o eliminar los riesgos.

Precondición

- Los riesgos se han identificado y se han determinado en el análisis de riesgo.
- Se han identificado y se han analizado las iniciativas posibles.
- Los riesgos relacionados a los procesos han sido eliminados en gran parte por la optimización de procesos.

Procedimiento

- Determine qué iniciativas necesitan ser ejecutadas repasando si la reducción de la pérdida y/o de la frecuencia de la ocurrencia justifica el costo de las iniciativas.
- Entonces compruebe si el resultado es influenciado por la interacción de otros factores.
- Documente las iniciativas nuevas definidas en el sistema de gestión de riesgos en indicador del riesgo asociado al riesgo del diagrama de asignación de recursos.
- Ponga al día los atributos relevantes en el grupo de atributos de la gestión de riesgos en la iniciativa (" Promedio de costos totales) y en la conexión de la iniciativa al riesgo (" Reducción de la frecuencia de la ocurrencia del riesgo" y " Reducción de la cantidad de daños en riesgos").

Resultado

Las mejores iniciativas en términos de la relación de costo/beneficio se definen y se documentan. El costo de la iniciativa y su efecto sobre el riesgo también se han registrado

Definición de mecanismos de control y escalabilidad

Para poder controlar y supervisar riesgos, deben ser definidos los procesos de control apropiados. Sin embargo, puesto que muchos riesgos no son directamente mensurables y así que son difíciles de controlar, los indicadores claves se deben identificar para mejorar la supervisión y para ayudar a detectar riesgos.

La introducción de sistemas limitados a la política de riesgos se diseña para asegurarse de que ciertos máximos y mínimos no se infringen. Esto es supervisada por los mecanismos de control que proporciona un sistema automático como el Administrador de performance de procesos o por cada dueño del riesgo.

Para el stock de los riesgos relacionados, sin embargo, los planes de emergencia deben también ser implementados para asegurar procesos controlados y la reasunción más rápida posible del negocio normal en caso de emergencia.

Además, los procesos alternativos para la ocurrencia de ciertos riesgos deben ser documentados y ser comunicados. Esto es clave para la planificación funcional de contingencia del negocio.

La definición de escalables mecanismos de control abarca dos actividades, que se funcionan en secuencia:

- Derivación de Indicadores Claves
- Definición de procesos de control y de emergencia

Derivación de indicadores claves

Objetivo

En el sistema de gestión de riesgos a los riesgos pueden ser asignados indicadores clave de la iniciativa o identificar el riesgo implicado. Los indicadores clave no producen generalmente iniciativa al riesgo en sí mismo, sino dan las indicaciones para la detección de riesgos específicos analizando disconformidad y buscando las causas (análisis de síntoma).

Precondición

- Se han identificado y se han determinado los riesgos.
- Las iniciativas se han tomado para reducir riesgo.

Procedimiento

- Defina uno o más indicadores clave para sus riesgos, tales como número de entradas de cancelación o número de quejas, lo más completos posible.
- Defina los valores planeados para los indicadores claves.
- Defina los límites (los mínimos y los máximos) para los indicadores claves, por ejemplo estipular cuando los planes de emergencia necesitan ejecutarse.
- Para tener un monitoreo automático de un indicador clave, realizar la consulta para generar el indicador clave del Query del sistema.
- Si usted no lo ha hecho ya así pues, señale a un dueño del riesgo para ser responsable de supervisar el riesgo y también el indicador clave.
- Modele el indicador clave y al dueño del riesgo en la base de datos de gestión de riesgos mediante un diagrama de la asignación de tareas, asociando el indicador clave al riesgo del indicador de funcionamiento clave asociado al riesgo en cuestión. y el dueño del riesgo por el "está bajo" la responsabilidad; conectarlo al riesgo. Los valores planeados límite y del indicador de funcionamiento clave se pueden mantener en los atributos relevantes del objeto la gestión de riesgos bajo "Indicador" del funcionamiento clave.

Resultado

Los indicadores clave definidos con valores límites planeados son una ayuda importante para el supervisar y detectar los riesgos. La designación de un dueño del riesgo ha asignado inequívocamente la responsabilidad del riesgo y su supervisión.

Definición de procesos de control y de contingencia

FACILITADORES Ejemplo de un proceso de contingencia en caso de fuego
Framework de Plan de contingencia

Objetivo

Este paso se definen los procesos de contingencia y de control claves a la gestión de riesgos.

Precondición

- Los riesgos han sido identificados.
- Para los riesgos identificados se han definido los indicadores de funcionamiento claves a los que alternativamente se han asignado planes y valores límites.

Procedimiento

- Compruebe si los valores previamente definidos de indicadores clave de funcionamiento se pueden supervisar por el gerente de performances de procesos.
- Si puede, defina el proceso de monitoreo en la gerencia de performances de procesos y vincule la misma a su base de datos de pérdidas para importar acontecimientos del riesgo en ella.
- Si no puede, defina un proceso del control del cual el dueño del riesgo es responsable. También defina los intervalos en los cuales o las condiciones bajo las cuales las iniciativas del control deben ser ejecutadas.

- Defina los planes de alternativa y de contingencia para los riesgos críticos, para ser desplegado cuando el flujo del todo el proceso se ha roto. Para otras situaciones extremas, también, por ejemplo los robos, ataques o fuegos, se deben definir los procedimientos de escalada exactos, con el objetivo de definir pasos estandarizados para tomar en tales situaciones excepcionales. Estas iniciativas se implementarán a través de toda la gerencia de continuidad de negocios.
- Defina los canales de comunicación (p.ej. vía el gerente departamental al encargado de riesgo) en caso de que el evento de riesgo ocurre realmente.
- Documentar los procesos en el Modelador de procesos asignando uno o mas Modelos de proceso al riesgo, conteniendo modelos de procedimiento en caso de fuego por ejemplo, o el procedimiento específico a seguir para implementar un proceso de control Defina el proceso referido por la categoría de proceso, modele el atributo en el modelo de proceso. Usted puede también asignar una documentación más detallada (tal como documentos de MS Office, documentos de PDF, etc.) al objeto que identifica el riesgo por un " Link" en un atributo de sistema vinculado.

Resultado

Los planes de contingencia se han definido para la seguridad de todos los empleados y se han diseñado para permitir la reasunción normal más rápida posible de negocios. Los procesos de control supervisan la eficacia de iniciativas y también sirven detectar una posible ocurrencia del riesgo una etapa tan temprana como sea posible.

Revisión del concepto a alcanzar (blanco)

FACILITADORES Check list:

Revisión de conceptos objetivo

Objetivo

La revisión del concepto a alcanzar (blanco) asegura que todos los pasos de esta fase se hayan ejecutado.

Precondición

- Los paquetes de trabajo de la fase del concepto de la blanco se han terminado.

Procedimiento

- Invite a un representante de la gerencia y al personal involucrado en las fases individuales a una reunión de revisión.
- Elabore una descripción de los paquetes de trabajo terminados.
- Haga presentar los resultados y el estado de sus paquetes de trabajo respectivos a los miembros del personal relevantes.
- Determine los resultados de los pasos individuales en una discusión de grupo.
- Discuta y documente las acciones de la mejora.
- Supervise la conformidad con las acciones propuestas de mejora y repase su eficacia.
- Publique un informe detallado a todos los participantes.

Resultado

La ejecución de los paquetes de trabajo individuales se ha revisado y se ha determinado. También, las mejoras se han decidido ejecutar y se están supervisando.

Reportes de Riesgos

La comunicación apuntada es clave para un sistema eficaz de la gestión de riesgos. Debe ser asegurado que los datos compaginados en las fases precedentes están puestos a disposición rápidamente de los responsables competentes dentro de la compañía. Esto se logra por la creación y la publicación del portal de proceso de riesgos. El Rol del asistente de proceso de riesgos asegura además de que todos los miembros del personal reciban la información exacta prevista para ellos.

Notifican a todos los miembros del personal de los procesos de emergencia y de los procesos alternativos referentes al caso de ocurrencia del riesgo. Además, cualquier dueño del riesgo puede informar riesgos nuevamente identificados al encargado de riesgo competente en el portal de riesgos.

La documentación comprensiva, y la publicación de esa documentación, hacen que la toma de decisiones de la organización y la valoración del riesgo transparente, de tal modo que se incrementa el nivel de aceptación de los empleados. Y puede también servir como guía por ejemplo para la valoración de riesgos futuros,.

La documentación del sistema de la gestión de riesgos documentada en el software de modelización y el portal de proceso de riesgos puede también proporcionar evidencia de apoyo en defensa de la gerencia en casos de la responsabilidad, por ejemplo con respecto a los controles, leyes del gobierno y la transparencia del negocio. Al mismo tiempo forma la base para las auditorías, por los auditores internos o externos.

El Asistente del proceso de riesgos proporciona una ayuda eficaz en esto, incluyendo las herramientas siguientes:

- Ejemplo: Portal de Procesos de Riesgos
- Check list: Reporte de Riesgos

Desarrollo del portal de proceso de riesgos

Todos los datos relevantes para la gestión de riesgos se han modelado con el software de modelización y se ponen a disposición del personal relevante. La transparencia de procesos dentro de la compañía y de la disponibilidad continua de los datos para la gestión de riesgos ayuda a los miembros individuales del personal a supervisar riesgos existentes así como para identificar nuevos riesgos.

Por motivos de seguridad, no todos los modelos son accesible a la vista de todo el personal. Por lo tanto, las responsabilidades definidas en el sistema de gestión de riesgos se presentan en el portal según vistas de usuarios específicos cuando cada usuario ingresa al sistema en base a permisos. Solamente los encargados de riesgos, señalados independientemente de los objetos modelados, tienen acceso a todos los datos.

La fase de desarrollo del proceso del portal de riesgos de proceso abarca tres actividades, que se funcionan en orden secuencial:

- Control de corrección del modelo
- Creación del Portal de Proceso de Riesgos
- Publicación del Portal de Proceso de Riesgos

Control de la corrección del modelado

Objetivo

Al crear el portal de proceso de riesgos un número de usuarios específicos para el análisis pueden ser seleccionados. Las condiciones previas para esto son correcto modelado en el software de modelización y mantenimiento de los atributos clave. El modelado correcto es también clave para el traslado de responsabilidades de sistema modelado a un rol de usuario específico, permitiendo diversas visitas de diversos usuarios.

Precondición

- Las fases precedentes han sido completadas.

Procedimiento

- Compruebe que todos los procesos clave para la gestión de riesgos se han modelado.

- Cerciórese de que, en el nivel de proceso superior en el sistema de modelización, las unidades organizacionales responsables de los procesos se hayan registrado mediante diagramas de asignación de tareas.
- Compruebe que todos los riesgos modelados en los procesos también se han asignado en el diagrama de riesgos y viceversa. Además, por lo menos un dueño del riesgo debe ser definido para cada riesgo en el sistema de gestión de riesgos.
- Compruebe que todos los atributos necesarios basados en el método de cálculo elegido se mantienen actualizados en el software de modelización.
- Compruebe que todas las responsabilidades modeladas con respecto a la gestión de riesgos también están mapeadas en el organigrama de la organización.
- Compruebe que los indicadores claves definidos referentes a los riesgos y las iniciativas se han definido de acuerdo con las estrategias de la acción.
- Compruebe que los procesos de emergencia y del control se han definido para los riesgos críticos.
- Cuando sea necesario, aplique la plantilla de gestión de riesgos a los modelos en el sistema de gestión de riesgos modelado, a los atributos clave en el lugar apropiado para mostrar el riesgo en el modelo seleccionado.

Resultado

Los objetos requeridos para las evaluaciones y el concepto de Rol se han modelado completamente en el Software de modelización y por consiguiente están terminados para su uso.

Creación de un Portal de Proceso de Riesgos

FACILITADORES Ejemplo:

Portal de proceso de riesgos

Objetivo

El objetivo de este paso es crear el portal de proceso de riesgos en Internet, que luego, se debe poner a disposición todos los empleados afectados.

Precondición

- El modelado de los datos clave para la gestión de riesgos y a la creación del portal de proceso de riesgos está completado.

Procedimiento

- Al lanzar la base de datos de la gestión de riesgos aparece un asistente para colaborar en la creación del Portal.
- Desde el asistente seleccione el modelo de proceso de nivel superior (por ejemplo un diagrama de cadena de valor agregado) y el diagrama del riesgo así como la carta de la estructura de la organización. Todas las unidades de la compañía y específicamente las unidades relevantes a la gestión de riesgos, se modelan en la carta de la estructura de la organización. Por el análisis requerido es importante que todos los modelos especificados se deban seleccionar correctamente.
- En el paso siguiente seleccione el método del cálculo para el cual usted también ha registrado los valores en la base de datos de riesgos. Si usted ha elegido el método orientado o simulación orientado del proceso, usted puede seleccionar solamente el nivel medio. Para el método general los otros gravámenes están también disponibles para seleccionar. Aquí, también, la condición previa para el análisis es que las cualidades relevantes están mantenidas en la base de datos de riesgos.
- Con respecto a los valores de la advertencia y de alarmas, usted puede especificar el valor esperado del riesgo en la unidad de tiempo establecida (año) cuál es el riesgo en la zona de cuidado (warning) en (amarillo) o la zona de la alarma (roja).
- Usted puede ajustar la escala del modelo para exhibir sus modelos más pequeños y más manejable en el portal del riesgo.
- Cuando usted ha seleccionado una carpeta en la cual grabar el portal del riesgo, comienza la generación del portal de proceso del riesgo.

Resultado

El portal de proceso de riesgos se ha generado, basado en los modelos con el contenido apropiadamente mantenido. El portal presenta todos los elementos de la importancia a la gestión de riesgos en una forma clara y sucinta, con varias opciones del análisis. Las responsabilidades se han asignado a través de diversas vistas del portal del riesgo durante el ajuste de los privilegios de acceso de cada usuario responsable.

Publicación del Portal de Proceso de Riesgos

Objetivo

El contenido del Portal de Proceso de Riesgos es de importancia para los dueños de procesos y los dueños de riesgos. El Portal de proceso de Riesgos debe sin embargo hacerse accesible también a todas las unidades organizacionales.

Precondición

- El Portal de proceso de riesgos ha sido correctamente creado.

Procedimiento

- Informe a las unidades relevantes la creación del portal de proceso del riesgo.

- Cerciórese de disponer de todas las personas implicadas para tener acceso al portal de proceso del riesgo. Para esto usted necesitará instalar un Web Server (servidor del Intranet) e integrar el lenguaje PHP de escritura (versión 4) como módulo en su Web Server. Usted encontrará el PHP en Internet o en su proveedor de software. Siga las instrucciones en la guía de instalación que permiten instalar estos componentes en su portal de proceso del riesgo.
- Conexión al portal de proceso de riesgos por primera vez entrando como administrador (conexión: sistema, contraseña: encargado). Coloque encendido en el botón " Administración" abotone y compruebe los datos de usuario del SISTEMA DE BASE DE DATOS DE RIESGOS contra los datos de usuario del portal de proceso de riesgos (por el botón " Verifique los datos de usuario en forma cruzada de BASE DE DATOS DE RIESGOS). Entonces utilice el " Dueños de manejo del riesgo" que ejecutan para asignar todos los dueños de proceso y a los dueños del riesgo las contraseñas individuales que permiten a ellos el acceso a los datos del proceso y/o del riesgo de los cuales son responsables. También cambie la contraseña del administrador a una contraseña de encargado.
- Utilice el "Manager de manejo del riesgo" funciona para configurar a los encargados de riesgo que deben tener acceso sin restricción a todos los datos, especialmente la página de análisis, y les asigna contraseñas iniciales también.

Resultado

Todas las personas afectadas han sido informadas de la creación del Portal de proceso de riesgos han restringido o no el acceso a la información contenida en él, según los roles asignados que les corresponden.

Informe de Revisión del riesgo

FACILITADORES Check list:
Reporte de revisión de Riesgos

Objetivo

La revisión de información del riesgo se asegura de que todos los pasos de esta fase se hayan ejecutado.

Precondición

- Los paquetes de trabajo de la fase de la información del riesgo se han terminado.

Procedimiento

- Invite a un representante de la gerencia y al personal involucrado en las fases individuales a una reunión de la revisión.
- Elabore una descripción de los paquetes de trabajo terminados.
- Entregue los resultados a los miembros del personal relevante y el estado de sus paquetes de trabajo respectivos.
- Determine los resultados de los pasos individuales en una discusión de grupo.
- Discuta y documente las acciones de la mejora.
- Supervise la conformidad con las acciones propuestas de mejora y repase su eficacia.
- Publique un informe detallado a todos los participantes.

Resultado

La ejecución de los paquetes de trabajo individuales se ha repasado y se han determinado. También, las mejoras se han decidido poner en marcha y se están supervisando.

Control de riesgos

Los monitores de un sistema de la gestión de riesgos arriesgan y proporcionan la advertencia posible más temprana de los acontecimientos de existencia del riesgo.

Debe ser observado que este sistema no se puede crear y adoptar sobre una base única, pero debe ser renovado y ser adaptado continuamente a las condiciones de base cambiantes y a cualquier cambio en la dirección y la política de la compañía. De esta manera la nueva, previamente desapercibida oportunidad y riesgo se pueden hacer visibles y calculables a la gerencia de la compañía.

El problema de la gerencia con ceguera, especialmente a las ediciones publicadas dentro de la compañía, es en realidad una ocurrencia relativamente frecuente. Sin embargo, el control de riesgo y la introducción de un sistema de alarma temprano basado en los indicadores claves animan a ejecutivos conscientes a evaluar su propia percepción de condiciones cambiantes del riesgo, para poder detectar posiblemente el riesgo en un primer momento. Un esquema de entrenamiento comprensivo puede también ayudar a hacer a encargados sensibles al control de riesgo.

El asistente del proceso de riesgos provee soporte efectivo en esto, incluyendo las siguientes herramientas:

- Formulario: Necesidades de entrenamiento
- Check list: Registro de Control de los riesgos
- Check list: Revisión de control de riesgos

Definición y monitoreo de iniciativas de control activo

En control de riesgos, las ideas conceptuales predefinidas como objetivo deben ser trasladadas en realidad concreta.

Para alcanzar esto, tiene sentido de proveer del personal el entrenamiento en gestión de riesgos donde hay déficits y también de introducir un sistema de incentivo ajustado al riesgo para consolidar conocimiento del riesgo. Los planes de emergencia definidos se deben también repasar en términos de su viabilidad y aceptación entre la fuerza de trabajo.

El control inmediato del riesgo y la supervisión de las iniciativas asociadas, tan bien como el entrenamiento en habilidades del control y de la supervisión, asimismo desempeñan un papel principal. Con este fin, la consideración se debe también dar a la posibilidad de desplegar los sistemas tales como el encargado de proceso del funcionamiento, que supervisan automáticamente indicadores claves y alarmas predefinidas del disparador cuando se infringen los límites aceptables.

Para cerrar el circuito de gestión de riesgos, es también necesario integrar en el procedimiento de gestión de riesgos las nuevas demandas, tales como las que surgen de nueva legislación u otros, y adaptar el sistema completo a condiciones cambiantes y nuevos riesgos detectados.

Control de riesgos comprende tres paquetes de trabajo, que se ejecutarán en secuencia:

- Entrenamiento y promoción de reconocimiento de riesgos
- Control Inmediato
- Desarrollo continuo del sistema de gestión

Entrenamiento y promoción del reconocimiento del riesgo

FACILITADORES Form:
Necesidades de entrenamiento

Objetivo

La creación del Portal de riesgos asegura que todos los miembros del staff han accedido a los datos de la gestión de riesgos de acuerdo a su respectivo rol. En orden de una fuerte aceptación y reconocimiento del riesgo, sin embargo, entrenamiento y otras iniciativas pueden ser realizadas.

Precondición

- El portal de riesgos ha sido creado.
- Todas las unidades organizacionales incluidas en el proceso de gestión de riesgos tienen acceso a los datos relacionados a su área de responsabilidad.

Procedimiento

- Establecer un sistema ajustado a un fuerte reconocimiento del riesgo. Las mejoras propuestas por los empleados deben ser reconocidas y premiadas.

- Determinar las necesidades de entrenamiento individual de los empleados en el campo de la gestión de riesgos y ofrecer a los empleados cursos generales y tutoría especializada en el portal de riesgos.
- Organizar cursos de entrenamiento para implementar iniciativas de reducción de riesgos para los dueños de los riesgos para los dueños de riesgos.
- Ejecutar prácticamente los procedimientos de emergencia definidos con todos los miembros del staff afectados.
- Asegurarse que todos los recursos de emergencia están disponibles permanentemente. Por ejemplo, debe controlarse que las locaciones de back up de IT estén disponibles en caso de que los sistemas queden fuera de servicio por fuego por ejemplo.

Resultado

Los empleados están entrenados en la gestión de los riesgos y que pasos implementar en caso de emergencia.

Control Inmediato

FACILITADORES Check list: Log de control de riesgos

Objetivo

El objetivo de este paso es realizar salvaguarda y control inmediato del riesgo y un adecuado resguardo del riesgo.

Precondición

- El proceso de control de riesgos ha sido definido en el concepto objetivo.

Procedimiento

- Entrenar al staff en la implementación del proceso de control definido.

- Asegurarse que los indicadores de riesgos son monitoreados de manera continua para proveer detección temprana del riesgo. La integración del encargado del proceso de funcionamiento es beneficiosa en este contexto. Puede automáticamente supervisar los indicadores claves predefinidos, que se pueden también exhibir por el portal de riesgos en la página del objeto del indicador clave.
- Para todos los riesgos no monitoreados automáticamente, controlar en la base de logs que los controles funcionaron correctamente y en los intervalos específicos.
- Controlar que los riesgos ocurridos son reportados correctamente al gerente de riesgos.

Resultado

En el mejor caso el proceso de control es implementado correctamente, en intervalos apropiados. Un reporte correcto de la ocurrencia de eventos de riesgos es asegurado.

Desarrollo continuo del sistema de gestión

Objetivo

La incorporación de nuevas demandas en el sistema de gestión de riesgos es una de las tareas clave del proceso de control de riesgos. Sólo el desarrollo continuo asegura que el sistema de gestión de riesgos estará siempre actualizado y refleja la situación de riesgos corriente.

Precondición

- El portal de proceso de riesgos ha sido publicado.
- Los riesgos son inmediatamente controlados.

Procedimiento

- Prestar atención a los nuevos requerimientos legales e incorporarlos en el sistema de gestión de riesgos.
- Asegurarse que nuevos riesgos no identificados o no existentes en la fase de identificación de riesgos son reportados luego al gerente de riesgos.
- Para informar el riesgo, utilice el "Registro de Riesgo" seleccione en el portal de proceso de riesgos en la página del objeto de la función en la cual el riesgo fue detectado. El nombre de la función y del modelo de proceso en los cuales la función ocurre se remite automáticamente al encargado de riesgo seleccionado por medio del "Transmitir" funcione una vez que ciertos detalles del riesgo se han incorporado en la pantalla del riesgo. La entrada se puede corregir nuevamente en caso de necesidad por el menú de ingreso de la información antes de ser transmitido.
- Entonces haga que los riesgos informados sean comprobados para saber si hay exactitud, y corrija cuanto sea necesario, el encargado relevante del riesgo en el banco de trabajo del encargado de riesgo.
- Una vez que todos los riesgos que se importarán han sido procesados y comprobados por los encargados individuales, el administrador del portal del proceso de riesgos puede activar el "Importar el nuevo riesgo a la base de datos" de RIESGOS; funcione para crear un archivo que contiene todos los riesgos lanzados para la importación en la BASE DE DATOS DE RIESGOS.
- Los riesgos entonces se importan en la BASE DE DATOS DE RIESGOS por el "Importar Riesgos". En esto, un check debe ser hecho si el riesgo (en casos excepcionales) puede ocurrir solamente en la función específica o si puede también ocurrir en todas las ocurrencias de la función en otros modelos de proceso. Entonces seleccione la opción apropiada de la importación basada en esa opción. El riesgo se crea automáticamente en el modelo relevante y el juego del reporte de la información se mantiene como el dueño responsable del riesgo.
- Compruebe los riesgos nuevamente importados en La BASE DE DATOS DE RIESGOS y corríjalos o agregue los datos que sean apropiados, por ejemplo un indicador clave del riesgo.
- Compruebe en intervalos regulares que los objetos modelados todavía se ajustan a la realidad y ajustarlos si hay cualquier condición cambiada, tal como costos

crecientes de iniciativas emprendidas, los valores actuales de las pérdidas calculadas en la base de datos de pérdidas, etc..

- Asegúrese de que el portal de proceso de riesgos esté regenerado y publicado después de cualquier cambio en los MODELOS DE PROCESOS, de modo que todos los procesos implicados sean siempre hasta la fecha. En el proceso, fijar a cualquier dueño nuevo definido de riesgo también automáticamente como usuarios en el portal de proceso de riesgos.

Resultado

El sistema de la gestión de riesgos está actualizado hasta la fecha actual, así que las decisiones se pueden tomar siempre en base de los últimos datos.

Revisión del control del Riesgo

FACILITADORES Check list: Revisión del control de riesgos

Objetivo

La revisión del control de riesgos asegura que todos los pasos de esta fase han sido implementados

Precondición

- Los paquetes de trabajo de la fase de control de riesgos han sido completados.

Procedimiento

- Invitar la Superioridad representativa y el staff involucrado en las fases individuales de la reunión de revisión.
- Dibujar un resumen (overview) de los paquetes de trabajo completados.
- Los miembros relevantes del staff presentado los resultados y el status de sus paquetes de trabajo respectivos.
- Comprender los resultados de los pasos individuales en una discusión de grupo.
- Discutir y documentar acciones de mejora.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

- Monitorear conformidad con las acciones de mejora propuestas y revisar su efectividad.
- Entregar un reporte detallado a todos los participantes.

Resultado

La ejecución de los paquetes de trabajo individuales han sido revisados y comprendidos. Asimismo, se ha decidido monitorear las mejoras.

CAPITULO V

CONCLUSIONES Y TRABAJOS FUTUROS

CAPITULO V - CONCLUSIONES Y FUTUROS TRABAJOS

Los elementos diseñados y construidos pretenden ser un punto de partida, una respuesta que permita contestar la pregunta ¿por donde empezar a gestionar la seguridad de la información? Sin que sea una única alternativa, simplemente un complemento para hacer más simple el estudio de conceptos técnicos y de gestión de la seguridad de la información, un marco de trabajo para desarrollar proyectos de gestión de contingencias y de riesgos orientados a describir la organización por procesos, en particular los denominados procesos clave del negocio. La propuesta es presentar un marco de trabajo en Internet, tal como el construido, que apunta a resolver la organización y gestión de un proyecto de implementación de la gestión de planes de contingencia y riesgos, basado en el análisis de los procesos de negocio y derivando de ellos los activos a proteger, los dueños de los procesos y activos, las amenazas a que se ven sometidas los activos cuando ejecutan los procesos, los riesgos que pueden producir las acciones derivadas de las amenazas, el análisis y valoración de los riesgos y finalmente el establecimiento de las salvaguardas necesarias para proteger los activos clave para la continuidad de las operaciones de la organización. El conjunto de salvaguardas es el denominado Plan de contingencias.

En complemento a este marco de trabajo orientado a procesos, se presentan dos soluciones que permiten, una vez implementado el Plan y la gestión de riesgos, administrar el sistema basado en un sistema informático que surge de construir lo diseñado en el denominado Navegador del SGR, que también es un diseño para la construcción posterior del sistema de software.

Finalmente se presenta un diseño que permita construir el denominado Portal del proceso de riesgos, es decir aquel sistema que una vez implementado presenta el estado de los riesgos y genera las alertas necesarias para poner en marcha los mecanismos de salvaguarda establecidos. También es un diseño o sea el establecimiento de la mínima funcionalidad requerida y la estructura de actividades que deben ser contempladas para construir el sistema.

Para determinar el estado de la situación de la gestión de planes de contingencia y riesgos, el autor realizó una encuesta en un grupo de empresas de desarrollo de software y servicios informáticos, que fueron auditadas personalmente durante 2007 y 2008, cuyo resultado se presenta como Anexo II, donde analizando las respuestas, surge que en general existen planes de contingencia fundamentalmente orientados a cubrir los riesgos de los equipos de procesamiento de información y que no es un uso generalizado el plan de contingencias en la Web.

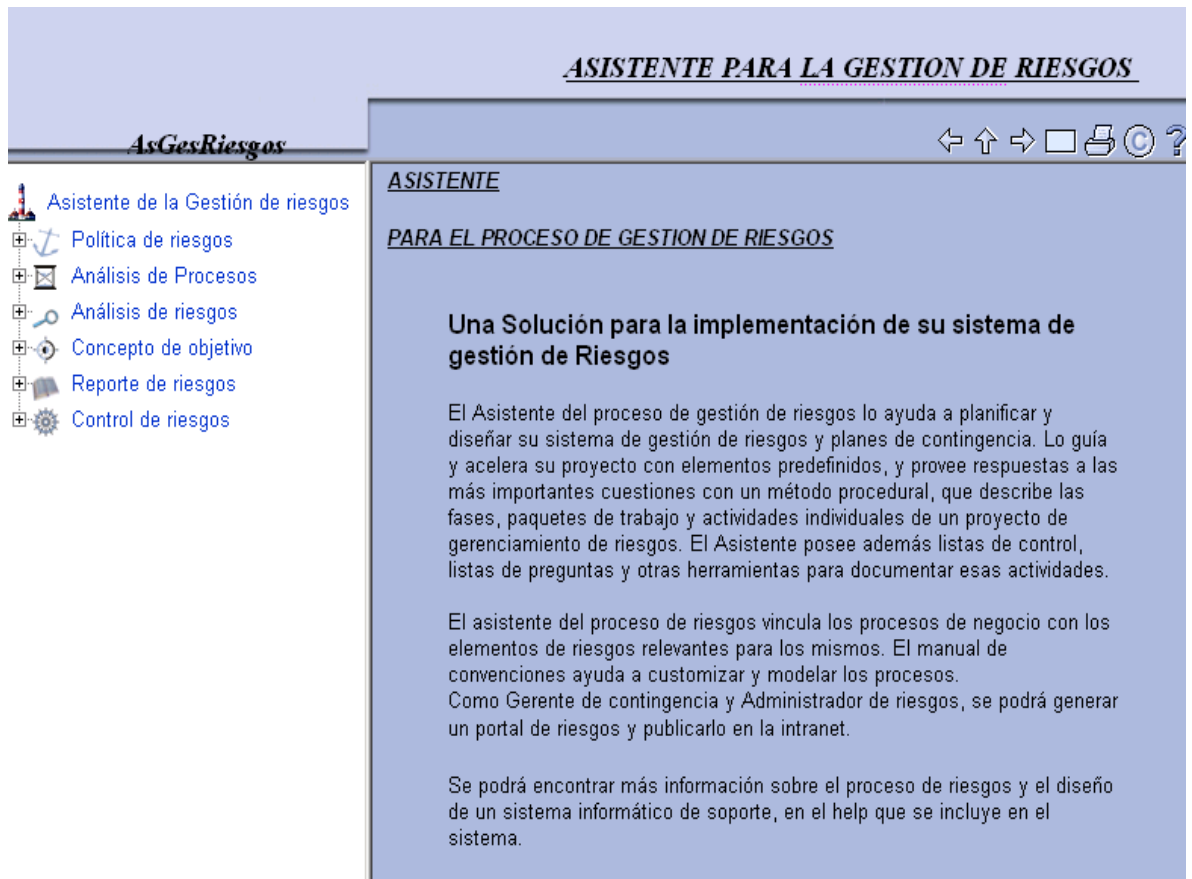
Con respecto a la administración de los riesgos, en el Anexo III se describe el sistema de gestión de riesgos basado en la norma IRAM 17550, que establece los conceptos fundamentales para gestionar riesgos en una organización y que son base de los sistemas diseñados e implementados de ayuda a la construcción del SGR presentado en esta tesis. El autor participó activamente en la estructuración y redacción de la norma, siendo miembro del Comité de riesgos de IRAM, Organismo argentino de Normalización.

Con respecto al Plan de contingencias a implementar, se plantea un modelo de Plan que se describe detalladamente en el Anexo V de la Tesis y se vincula en los sistemas de navegación construidos, para dar soporte y ayuda a quienes tienen a su cargo los proyectos de elaboración de los Planes y quienes construyen los sistemas de software de las empresas.

Finalmente, a continuación se plantean los tres sistemas diseñados en el formato de navegadores Web, para soporte al diseño, desarrollo e implementación del Plan de contingencias y la gestión de riesgos:

El primero es un:

Sistema de ayuda a la formulación de proyectos de formulación de planes de contingencia y gestión de riesgos



Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

El segundo sistema navegador Web es que proporciona el:

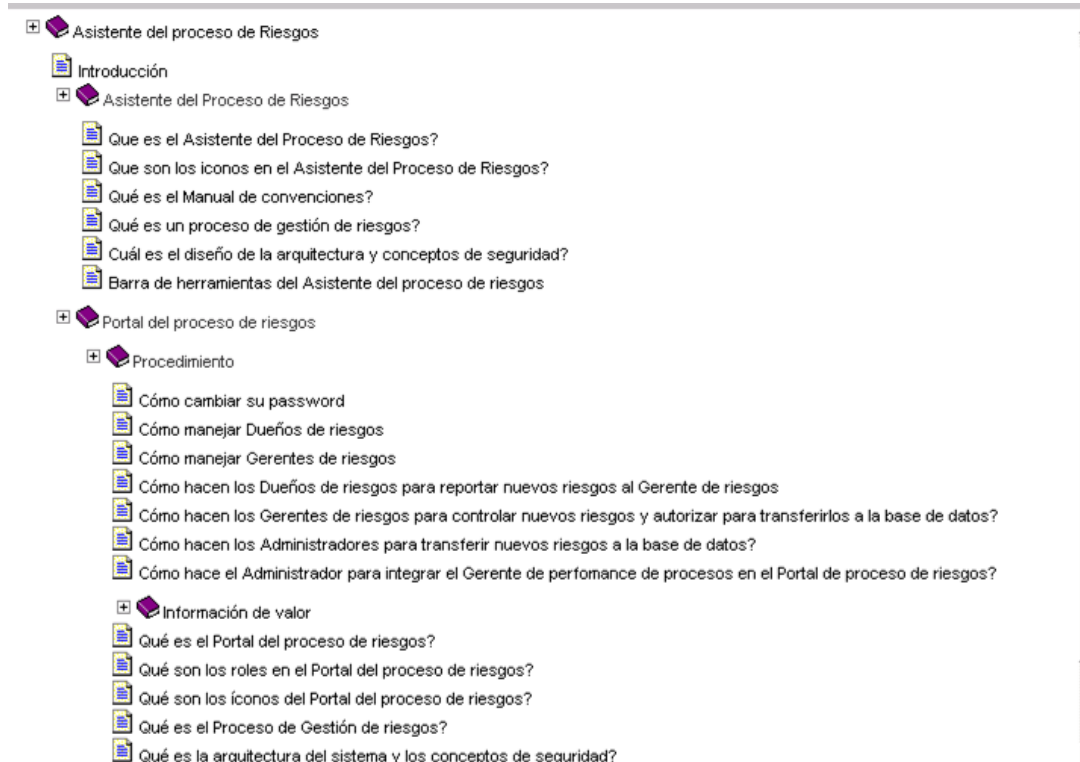
Diseño de un sistema de planes de contingencia y gestión de riesgos

The screenshot displays a web application interface for the SGR system. On the left, there is a vertical navigation menu with the following items: SGR, Sobre la gestión de riesgos, Instalación, Elementos (with sub-items: Bibliotecas, Proyectos, Activos (en el SGR), Dominios de seguridad, Salvaguardas (en el SGR), Perfiles de seguridad, Niveles de valoración, Niveles de madurez, Niveles de criticidad), Primera pantalla, Análisis y gestión de riesgos, Magerit, and CC: Criterios comunes. The main content area on the right has a light blue background and contains the following text: **Sistema de Gestión Planes de Contingencia y de Gestión de Riesgos**, *Asistente para el Análisis y Gestión de Riesgos y la implementación de Planes de Contingencia*, **Diseño del Sistema Web Service**, and *versión 1.0*.

En el Anexo VI se presentan las pantallas de navegación del sistema SGR.

El tercero es un sistema navegador Web que brinda el diseño del Portal de riesgos:

Diseño del sistema de gestión de riesgos y control de riesgos



En el Anexo VII se presenta la estructura de pantallas de navegación de la aplicación diseñada.

Hacia el futuro y como input a proyectos de tesis de maestría o de investigación aplicada, la idea es que se continúe esta experiencia con el desarrollo y la construcción de los sistemas informáticos de soporte, es decir que cada organización en base a esos marcos de trabajo y diseños propuestos pueda desarrollar sus sistemas de gestión informatizada de manera eficiente y a un bajo costo de implementación.

También, hacia el futuro, la idea es se continúe con este Framework, diseñando y desarrollando, un sistema complementario para la gestión de las auditorías del Plan de contingencia y los riesgos, pues es fundamental en un sistema de este tipo verificar el cumplimiento efectivo de la aplicación de los controles establecidos como salvaguardas a los riesgos. En el Anexo IX se presenta la funcionalidad de ese cuarto sistema necesario, para obtener la integridad de la gestión de planes de contingencia y riesgos organizacionales, que es el de gestión de auditoría de controles.

En esta descripción vale aclarar que el sistema sirve de soporte a los auditores de tercera parte que verifican el cumplimiento efectivo de la realización de los controles establecidos en el sistema de gestión de la seguridad, en particular en el caso presentado, se trata de analizar los controles aplicados a los procesos relevantes para el sistema de control de soporte al cumplimiento de la ley Sarbanes Oxley de Estados Unidos.

Esta guía de conceptos facilita el diseño de una aplicación complementaria a las planteadas en la tesis respecto de contar con un sistema de auditoria de aplicación efectiva de los controles y procedimientos de gestión de riesgos y contingencia planteados.

En particular, Sarbanes-Oxley requiere de la certificación por una Entidad internacional del efectivo cumplimiento de los controles implementados para mitigar los riesgos, en especial los financieros de las compañías.

De la construcción de los sistemas de soporte a la gestión de riesgos y planes de contingencia automatizados a través de procesos Web, la organización puede alcanzar el nivel de madurez III disponiendo de un sistema de gestión de riesgos integrado y administrado por procesos.

CAPITULO VI – BIBLIOGRAFÍA

REFERENCIADA

- *RB 1 – Norma IRAM – ISO / IEC 27002:2008 (ex IRAM – ISO/IEC 17799) mejores prácticas para La gestión de La seguridad de La información.*
- *RB 2 - CAF "Academic Computing Policy Statements" Archive (ejemplos de políticas seguidas en diversos sitios) – The Electronic Frontier Foundation (EFF) – 1999*
- *RB 3 - Tecnología de Salas Cofres – 2006 / 2007 – Norma ICREA STD – 131/2007.*
- *RB 4 – Dijker, Barbara L., ed. Short Topics in System Administration. Vol. 2, A Guide to Developing Computing Policy Documents. Berkeley, CA: The USENIX Association for SAGE, the System Administrators Guild, 1996.*

Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000.

GartnerGroup, "Disaster Management Plan for Remote Access," September 20, 2001.
- *RB 5 - Portales relativos a seguridad informática*
 - <http://securityfocus.com>
 - www.insecure.org
 - www.hispasec.com
 - <http://secinf.net>
 - www.securityportal.com.ar
 - www.itsec.gov.uk
 - www.privacyexchange.org
 - www.microsoft.com/latam/net/introduccion/default.asp
 - www.isec-global.com
 - <http://www.isetec.com.ar>
 - <http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/>
 - www.iso27000.es
 - <http://www.microsoft.com/latam/net/introduccion/default.asp>

- *RB 6 – Norma ISO / IEC 15408 Criterio común para los requisitos de la seguridad de la información*
- *RB 7 – Norma IRAM – ISO/IEC 9000 introducción a los sistemas de gestión*
- *RB 8 - Contingency Planning and Management Online. Volume VI, Number 5, September/October 2001. <http://www.contingencyplanning.com> Contingency Planning and Management, Master Source 2001, Buyer's Guide Issue, Volume 6, 2001.*
- *RB 9 – IDS Scheer AG – Software ARIS TOOLSET y metodología para gestión de procesos de negocio.*
- *RB 10 - Guía para elaborar Planes de contingencia del NIST, National Institute of Standards and Technology, del Departamento de Comercio de los Estados Unidos. National Institute of Technology and Standards, Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995.*
- *RB 11 - Magerit V2, Metodología de análisis y gestión de riesgos de los sistemas de información del Ministerio de administración Pública de España.*
- *RB 12 - Norma ISO 27001, requisitos de los sistemas de gestión de la seguridad de la información.*
- *RB 13 - Disaster Recovery Journal. Volume 14, Issue 4, Fall 2001. <http://www.drj.com/drj2/drj2.htm> DRI International. <http://www.drii.org/index.htm> Computer Security Act of 1987, 40 U.S. Code 759 (Public Law 100-235), January 8, 1988. Contingency Planning and Management Online. Volume VI, Number 5, September/October 2001. <http://www.contingencyplanning.com> Contingency Planning and Management, Master Source 2001, Buyer's Guide Issue, Volume 6, 2001.*
- *RB 14 – Norma IRAM 17551 – requisitos de los sistemas de gestión de riesgos.*
- *RB 15 - Modelización orientada a Objetos del lenguaje UML y el software JUDE Community (www.judecommunity.com).*

- *RB 16 – Política del estado Argentino - Normas de Control Interno para Tecnología de la Información Res. 48/2005 SIGEN Sector Público Nacional - la Decisión Administrativa 669/2004*
- *RB 17 – COBIT - Cobit (Control Objectives for Information Technology) "Audit Guidelines" 3ra. Edición. 2000.*
Cobit (Control Objectives for Information Technology) "Control Objectives" 3ra. Edición. 2000.
- *RB 18 – Norma ISO / IEC 20000-1 requisitos para los sistemas de gestión la tecnología de la información.*

Normas utilizadas como investigación del trabajo:

- IRAM / ISO-IEC 17799 Mejores prácticas de la seguridad de la información
- IRAM / ISO-IEC 27001 Requisitos de los sistemas de gestión de la seguridad de la información
- IRAM / ISO-IEC 27002 Mejores prácticas de la seguridad de la información
- ISO / IEC 15408 requisitos de la seguridad de la información de los sistemas de información (Common Criteria)
- TECHNICAL REPORT ISO/IEC 13335-1:1997 Guías para administrar la seguridad de la información – Administración y planificación de la seguridad de la tecnología de la información
- TECHNICAL REPORT ISO/IEC 13335-2:1997 Guías para administrar la seguridad de la información – Conceptos y modelos para la seguridad de la tecnología de la información
- TECHNICAL REPORT ISO/IEC 13335-3:1997 Guías para administrar la seguridad de la información – Técnicas para la administración de la seguridad de la información
- TECHNICAL REPORT ISO/IEC 13335-3:1997 Guías para administrar la seguridad de la información – Selección de salvaguardas
- TECHNICAL REPORT ISO/IEC TR 15947:2000 Técnicas de seguridad de la información – Marco de trabajo para la detección de intrusiones
- ISO/IEC TR GUÍA 73 – términos y vocabulario de la gestión de riesgos

COMPLEMENTARIA

- Dijkstra, Barbara L., ed. Short Topics in System Administration. Vol. 2, A Guide to Developing Computing Policy Documents. Berkeley, CA: The USENIX Association for SAGE, the System Administrators Guild, 1996. Dijkstra - USENIX Association for SAGE (System Administration Guild) 1996
- RFC (Request for Comments) 1281, 1244 - Site Security Handbook, Internet Engineering Task Force (IETF), 1991
- Site Security Policy Development - Rob McMillan, Information Technology Services - Griffith University, Australia, 1995
- Practical UNIX & Internet Security - Garfinkel & Spafford, O'Reilly
- Consideraciones para la elaboración de políticas de seguridad en cómputo para una organización - César Vega Calderón,
- Internet Security Policy: A Technical Guide - NIST Special Publication 800-XX - Barbara Guttman, Robert Bagwill, 1997
- Security Policies for the Internet - Stephen L. Arnold, Ph.D.
- Information Security Policies Made Easy - Charles Cresson Wood, 1997
- Acharya, Soubir and Susan G. Friedman. "Backup Strategies for Networked Storage," InfoStor, November 2001.
- Disaster Recovery Journal. Volume 14, Issue 4, Fall 2001.
<http://www.drj.com/drj2/drj2.htm>
- DRI International. <http://www.drii.org/index.htm>
- Computer Security Act of 1987, 40 U.S. Code 759 (Public Law 100-235), January 8, 1988.
- Engelschall, Ralf. "Load Balancing Your Web Site," Web Techniques, May 1998.
<http://www.Webtechniques.com/archives/1998/05/engelschall/>
- Federal Emergency Management Agency. Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations (COOP), July 1999.
- Federal Emergency Management Agency. The Federal Response Plan, April 1999.
- Flesher, Tom. "Remote Journaling: A New Trend in Data Recovery and Restoration," Contingency Planning & Management, March 2000.
http://www.contingencyplanning.com/article_index.cfm?article=243
- GartnerGroup, "Fault-Tolerant Networks: Is There Such a Thing?" Research Note, June 14, 2001.

- GartnerGroup, "Disaster Recovery: Weighing Data Replication Alternatives," Research Note, June 15, 2001.
- GartnerGroup, "High Availability: A Perspective," Technology Overview, June 15, 2001.
- General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999.
- General Accounting Office, Executive Guide: Information Security Management: Learning From Leading Organizations, GAO/AIMD-98-68, May 1998.
- Information Assurance Technical Framework (IATF), Release 3.0, October 2000.
<http://www.iatf.net/>
- INT Media Group, Incorporated. Webopedia. <http://www.Webopedia.com/>
- LoadBalancing.net. "Frequently Asked Questions."
<https://www.loadbalancing.net/faq.html>
- Leary, Mark F., CPP. "A Rescue Plan for Your LAN," Security Management Online.
<http://www.securitymanagement.com/library/000496.html>
- Maxwell John. "Part II - Storage Virtualization: Beyond the basics," InfoStor, October 2001.
http://is.pennnet.com/Articles/Article_Display.cfm?Section=Archives&Subsection=Display&ARTICLE_ID=123539
- National Institute of Technology and Standards, Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, November 1999.
- NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "Security Self-Assessment Guide for Information Technology Systems" Marianne Swanson, 2001.
- NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "Automated Tools for Testing Computer System Vulnerability" W. Timothy Polk, 1992.
- National Institute of Technology and Standards, Special Publication 800-30, First Public Exposure DRAFT, Risk Management Guide, June 2001.
- NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "Generally Accepted Principles and Practices for Securing Information Technology Systems". Marianne Swanson y Barbara Guttman, 1996.

- NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "Guide for Developing Security Plans for Information Technology Systems" Marianne Swanson, 1998.
- Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.
- PCWorld.com. "HassleFree Backups," PC World Magazine, October 2001.
<http://www.pcworld.com/howto/article/0,aid,18040,00.asp>
- Presidential Decision Directive 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 1998.
- Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.
- Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.
- Seagate Technology. "Types of Backups," Technical Bulletin #4062.
<http://www.seagate.com/support/kb/tape/4062.html>
- Solinap, Tom. "RAID: An In-Depth Guide to RAID Technology," SystemLogic.net, January 24, 2001. <http://www.systemlogic.net/articles/01/1/raid/>
- Sun Microsystems, Inc. "Remote Mirroring," Technical White Paper.
<http://www.sun.com/storage/white-papers/remote-mirroring.wp.html>
- Tanner, Dan. "Storage virtualization: What, how, and why," InfoSto, March 2001.
http://is.pennnet.com/Articles/Article_Display.cfm?Section=Archives&Subsection=Display&ARTICLE_ID=94313
- U.S. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication (FIPS PUB) 87, Guidelines for ADP Contingency Planning, March 1981.
- Whatis.com. TechTarget.net. <http://whatis.techtarget.com/>
- Mario Gerardo Piattini Velthius, Emilio del Peso Navarro. 1998. Auditoría Informática: un enfoque práctico. Alfa-Omega - Ra-ma.
- José Antonio Echenique. 1996. Auditoría en Informática. Mc Graw Hill.
- Humberto David Rosales Herrera. Determinación de riesgos en los centros de cómputos. 1996. Editorial Trillas.
- David Pitts, Hill Ball. Red Hat Linux Unleashed. The comprehensive solution. 1998. Sams Publishing.

- BCRA (Banco Central de la República Argentina). "Anexo a la Comunicación "A" 2659 – Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática". 1998. www.bcra.gov.ar
- BCRA (Banco Central de la República Argentina). "Anexo a la Comunicación "C" 30275 – Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática- Fe de erratas". 2001. www.bcra.gov.ar
- BCRA (Banco Central de la República Argentina). "Anexo a la Comunicación "A" 3198 – Texto ordenado actualizado de las Normas sobre Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática". 2001. www.bcra.gov.ar
- ISO (International Standard Organization). "Estándar de Seguridad ISO 17799"
- ISO (International Standard Organization). "The Common Criteria for Information Technology Security Evaluation" v2.1
- DoD (Department of Defense) Rainbow Series Library. "Trusted Network Interpretation of the TCSEC - Red Book". 1987.
- DoD (Department of Defense) Rainbow Series Library. "Password Management Guideline – Green Book". 1985.
- SIGEN (Sindicatura General de la Nación). "Normas generales control interno". Resolución SIGEN N° 107/98. 1998.
- AGN (Auditoría General de la Nación). "Normas de auditoria externa de la Auditoria General de la Nación". 1993.
- ISACA (Information Systems Audit and Control Association). "Planning the IS Audit". 1998.
- ISACA (Information Systems Audit and Control Association). "Normas generales para la auditoría de los sistemas de información". 1997.
- Cisco Systems. "Cisco SAFE: A Security Blueprint for Enterprise Networks". Sean Convery y Bernie Trudel. 2000.
- Cisco Systems. "Beginner's guide to network security". 2001
- CERT (Computer Emergency Response Team) "Tutorial de seguridad". "IT Baseline Protection Manual - Standard security safeguards". Bundesanzeiger – Verlag, Alemania. 2001.
- Hal Tipton, Micki Krause. "Handbook of Information Security Management". Consulting Editors, 1998. "Internet Security Professional Reference, Second Edition". New Riders Publishing. 1997. Gonzalo Alvarez Marañón. "Manual onLine de

- Criptografía y Seguridad". Consejo Superior de Investigaciones Científicas (CSIC), Madrid, España. 1997.
- Tomas Olovsson. "A Structured Approach to Computer Security". Department of Computer Engineering, Chalmers University of Technology (Gothenburg – SWEDEN). Technical Report No 122, 1992.
 - Peter Vincent Herzog. "Open-source security testing methodology manual", Idea Hamster, GNU, 2001.
 - "Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network" Macmillan Computer Publishing. 1998.
 - Steven Shaffler y Alan Simon. "Network Security". AP Professional, 1994.
 - Jorge Tomás Curras. "Transacciones comerciales en Internet". Columbus Internet Marketing & Consulting. Madrid. www.columbus-digital.com
 - "SET Software Compliance Testing". SET Secure Electronic Transaction LLC. www.setco.org
 - "Seguridad en Internet". Microsoft. www.microsoft.com
 - Ministerio de Economía de la Nación www.mecon.ar
 - Tim Dierks. "SSL as a protocol security solution". Consensus Development Corp. www.consensus.com
 - "Internet Firewalls and Security". 3Com. www.3com.com
 - "Microsoft TechNotes" - www.microsoft.com/technet
 - El Coordination Center (CERT/CC) creado en 1988, centro de expertos en seguridad en Internet del Software Engineering Institute, de la Universidad de Carnegie Mellon University.

Información general sobre seguridad en redes

- Abrams, Marshall D.; Podell, Harold J.; and Jajodia, Sushil. Information Security: An Integrated Collection of Essays. Los Alamitos, CA: IEEE Computer Society Press, 1995.
- Ahuja, Vijay. Network and Internet Security. Boston, MA: AP Professional, 1996.
- Allen, Julia H. The CERT® Guide to System and Network Security Practices. Boston, MA: Addison-Wesley, 2001.
- Anderson, Ross J. Security Engineering: A Guide to Building Dependable Distributed Systems . New York, NY. John Wiley & Sons, 2001.

- Atkinson, Randall J. "Toward a More Secure Internet." IEEE Computer 30, 1 (Jan. 1997): 57-61.
- Bosselaers, Antoon, Preneel, Bart. Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040. Lecture Notes in Computer Science: 1007. Berlin and New York: Springer, 1995.
- Cohen, Frederick B. Protection and Security on the Information Superhighway. New York, NY: Wiley, 1995.
- Comer, Douglas E. Internetworking with TCP/IP, volume 1: principles, protocols, and architecture. Third Edition. New York, NY: Prentice-Hall, 1995.
- Davis, Peter T., ed. Securing Client/Server Computer Networks. New York, N.Y.: McGraw-Hill, 1996.
- Denning, D.E. Information Warfare and Security. New York, N.Y: Addison-Wesley Publishing Company, Inc., 1999.
- Denning, P.J. and Denning, D.E. Internet Besieged: Countering Cyberspace Scofflaws. New York, N.Y: Addison-Wesley Publishing Company, Inc., 1998.
- Gollmann, Dieter. Computer Security. Chichester, England: John Wiley & Sons, 1999.
- Howard, Michael & LeBlanc, David. Writing Secure Code. Redmond: Microsoft Press, 2002.
- Kaufman, C.; Perlman, R.; and Speciner, M. Network Security: Private Communication in a Public World. Englewood Cliffs, NJ: PTR Prentice-Hall, Inc., 1995.
- Kyas, O. Internet Security, Risk Analysis, Strategies and Firewalls. Boston, MA: Int'l Thompson, 1997.
- McGraw, Gary, and Felten, Edward W. Java Security. New York: John Wiley and Sons, Inc., 1996.
- NCSCGlossary of Computer Security Terms. Ft. George G. Meade, MD: National Computer Security Center: Washington, DC: For sale by the Supt. of Docs., U.S. G.P.O., 1989.
- National Research Council. Computers at Risk: Safe Computing in the Information Age. Washington, D.C.: National Academy Press, 1991
- Pfleeger, Charles P. Security in Computing (Second Edition). Upper Saddle River, NJ: Prentice Hall, 1997.
- Ryan Peter, Steve Schneider, et al. Modelling and Analysis of Security Protocols. Harlow, England: Addison-Wesley, 2001.

- Schneider, Fred B. ed. Trust in Cyberspace. Washington, DC: National Academy Press, 1999.
- Schwartau, Winn. Time-Based Security. Seminole, FL: Interpact Press, 1999.
- Stevens, W. Richard. TCP/IP Illustrated, Volume 1: The Protocols. Reading, MA: Addison-Wesley, 1994.
- Summers, Rita C. Secure Computing. New York, NY: McGraw-Hill, 1997.
- Wadlow, Thomas A. The Process of Network Security. Reading, MA: Addison-Wesley, 2000.

Guías de seguridad en redes

- Internet Engineering Task Force, Network Working Group. Guidelines for the Secure Operation of the Internet, (RFC 1281). <ftp://ftp.isi.edu/in-notes/rfc1281.txt> (1991)
- Internet Engineering Task Force, Site Security Policy Handbook Working Group. Site Security Handbook, (RFC 2196, FYI 8). <ftp://ftp.isi.edu/in-notes/rfc2196.txt> (1997)
- Internet Security Policy: A Technical Guide. Washington, DC: National Institute of Standards and Technology, 1998. Available at <http://csrc.nist.gov/isptg>.
- Kabay, Michel E. The NCSA Guide to Enterprise Security: Protecting Information Assets. New York, NY: McGraw-Hill, 1996.
- Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook. Indianapolis, IN: New Riders Publishing, Macmillan, 1999.
- Wireless Network Security: 802.11, Bluetooth, and Handheld Devices. Washington, DC: National Institute of Standards and Technology, 2003. Available at http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

Guías para administradores

- Howard, John; and Longstaff, Tom. A Common Language for Computer Security Incidents. (SAND98-8997). Albuquerque, NM: Sandia National Laboratories, 1998.
- Kimmins, John; Dinkel, Charles; and Walters, Dale. Telecommunications Security Guidelines for Telecommunications Management Network. NIST Special Publication: 800-13. Organization National Institute of Standards and Technology (U.S.). Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 1995.

- Kuncicky, D.; and Wynn, B. A. Short Topics in System Administration, Vol 4, Educating and Training System Administrators: A Survey. Berkeley, CA: The USENIX Association for the System Administrators Guild (SAGE), 1998.
- Oppenheimer, David L.; Wagner, David A.; and Crabb, Michele D. Short Topics in System Administration, Vol. 3, System Security: A Management Perspective. Berkeley, CA: The USENIX Association for the System Administrators Guild (SAGE), 1997.
- Phillips, G. Short Topics in System Administration, Vol. 5, Hiring System Administrators. Berkeley, CA: The USENIX Association for the System Administrators Guild (SAGE), 1999.
- Schweitzer, James A. Protecting Business Information: A Manager's Guide. Boston, MA: Butterworth-Heinemann, 1996.

Manejo de intrusiones

- Amoroso, Edward. Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Sparta, NJ: Intrusion.Net Books, 1999.
- Base, Rebecca Gurley. Intrusion Detection. Indianapolis, IN: MacMillan Technical Publishing, 2000.
- Computer Security Incident Handling Step By Step Guide, v1.5. Bethesda, MD: The SANS Institute. May, 1998.
- Escamilla, Terry. Intrusion Detection: Network Security Beyond the Firewall. New York, NY: Wiley Computer Publishing, 1998.
- Maiwald, Eric. "Automating Response to Intrusions," Proceedings of the Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.
- Marchany, Randy. "Incident Response: Scenarios and Tactics." Proceedings of the Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.
- Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook. Indianapolis, Indiana: New Riders Publishing, 1999.
- Schultz, Eugene. "Effective Incident Response." Proceedings of The Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.

- Toigo, Jon William. Disaster Recovery Planning for Computers and Communication Resources. New York, NY: John Wiley, 1996.

Criptografía

- Bauer, F.L. Decrypted Secrets, Methods and Maxims of Cryptology. New York: Springer-Verlag, 1996.
- Garfinkel, Simpson. PGP: Pretty Good Privacy. Sebastopol, CA: O'Reilly and Associates, Inc., 1995.
- Internet Engineering Task Force, Network Working Group. The MD5 Message-Digest Algorithm, (RFC 1321). <ftp://ftp.isi.edu/in-notes/rfc1321.txt> (1992)
- Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY: John Wiley and Sons, 1996.
- National Institute of Standards and Technology (U.S.). "Secure Hash Standard." Gaithersburg, MD: Computer Systems Laboratory, National Institute of Standards and Technology, U.S. Dept. of Commerce, Technology Administration: Springfield, VA: <http://www.itl.nist.gov/fipspubs/fip180-1.htm> (1995)
- Stallings, William. Practical Cryptography for Data Internetworks. Los Alamitos, CA.: IEEE Computer Society Press, 1996.
- Stallings, William. Protect Your Privacy: The PGP User's Guide. Englewood Cliffs, N.J.: Prentice Hall PTR, 1995.
- Sutherland, Ivan Edward. A View of the Task You Face: A Report to the NRC Committee on Cryptography. Series Title Perspectives (Sun Microsystems Laboratories): 96-2. Mountain View, CA: Sun Microsystems Laboratories, 1996.
- Wayner, Peter. Disappearing Cryptography: Being and Nothingness on the Net. Boston, MA: AP Professional, 1996.

Firewalls

- Chapman, D. Brent, Cooper, Simon, Russell, Deborah, and Zwicky, Elizabeth D. Building Internet Firewalls (2nd edition). Sebastopol, CA: O'Reilly and Associates, 2000.
- Cheswick, William R. and Bellovin, Steven M. Firewalls and Internet Security. Reading, MA: Addison-Wesley, 1994.

- "Firewalls Market Survey." SC Magazine, Framingham, MA: West Coast Publishing, Inc., April, 1999. Available at <http://www.infosecnews.com>.
- "Stateful Inspection Technology Tech Note." Check Point Software Technologies Ltd., 1999. Available at http://www.sofaware.com/html/tech_stateful.shtml.
- Avolio, Blask. "Application Gateways and Stateful Inspection: A Brief Note Comparing and Contrasting." Trusted Information Systems, Inc., 1998. Available at <http://www.avolio.com/apgw+spf.html>.
- Cooper, Deborah and Pfleeger, Charles. "Firewalls: An Expert Roundtable." IEEE Software, New York, NY (September/October 1997).
- Goncalves, Marcus. Firewalls: A Complete Guide. New York, NY: McGraw Hill, 2000.
- Grennan, Mark. Firewalling and Proxy Server HOWTO. Version 1.0.8. July 4, 2000. Available at <http://metalab.unc.edu/LDP/HOWTO/IPCHAINS-HOWTO.html>.
- Hall, Eric. "Internet Firewall Essentials." Network Computing Online. Manhasset, NY: CMP Media, Inc., November, 1996. Available at <http://www.networkcomputing.com/netdesign/wall1.html>.
- Internet Security Policy: A Technical Guide. Washington, DC: National Institute of Standards and Technology, 1998. Available at <http://csrc.nist.gov/isptg>.
- Lodin, Steve and Schuba, Christoph. "Firewalls Fend Off Invasions from the Net." IEEE Spectrum. New York, NY: IEEE, February, 1998.
- Luk, Ellis, et al. Protect and Survive: Using IBM Firewall 3.1 for AIX, 3rd edition. Research Triangle Park, NC: IBM, 1998. Available at <http://www.redbooks.ibm.com>.

Seguridad Web

- Garfinkel, S.; Spafford, G. Web Security and Commerce. Sebastopol, CA: O'Reilly and Associates, Inc., 1997.
- Larson, Eric & Stephens, Brian. Web Servers, Security & Maintenance. Upper Saddle River, NJ: Prentice Hall, 2000.
- Rubin, A. D.; Geer, D.; and Ranum, M. Web Security Sourcebook. New York: John Wiley and Sons, Inc., 1997.
- Spainhour, Stephen & Quercia, Valerie. Webmaster in a Nutshell. Sebastopol. CA: O'Reilly and Associates, 1996.
- Stein, Lincoln. Web Security: A Step-by-Step Reference Guide. Reading, PA: Addison-Wesley, 1998.

- World Wide Web Consortium. W3C Security Resources. <http://www.w3.org/Security/>.

Supervivencia de sistemas

- Salter, Chris; Saydjari, O. Sami; Schneier, Bruce; Wallner, Jim. "Toward a Secure System Engineering Methodology." New Security Paradigms Workshop, 1998. <http://www.counterpane.com/secure-methodology.html>.

Para computadores y sistemas operativos específicos

- AS/400
- Park, Joseph S. AS/400 Security in a Client/Server Environment. New York, NY: J. Wiley, 1995.
- PC
- Alexander, Michael. The Underground Guide to Computer Security: Slightly Askew Advice on Protecting Your PC and What's on It. Reading, Mass.: Addison-Wesley Pub. Co., 1996.
- Cobb, Stephen. The NCSA Guide to PC and LAN Security. New York: McGraw-Hill, 1996.
- Park, Joseph S. AS/400 Security in a Client/Server Environment. New York, NY: J. Wiley, 1995.
- Windows NT
- Rutstein, Charles B. Windows NT Security: A Practical Guide to Securing Windows NT Servers and Workstations. New York: McGraw-Hill, 1997.
- Securing Windows NT Installation. Microsoft. http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp (1999)
- Sheldon, Tom. Windows NT Security Handbook. Berkeley, CA: Osborne McGraw-Hill, 1997.
- Sutton, Stephen A. Windows NT Security Guide. Reading, MA: Addison-Wesley Developers Press, 1997.
- Windows NT Security Guidelines. Trusted Systems Services, Inc. <http://www.trustedsystems.com/NSAGuide.htm> (1998)

- Windows NT Security Step by Step. SANS NT Security, <http://www.sans.org/ntstep.htm> (1998)
- Unix
- Curry, Dave. Improving the Security of Your UNIX System (Technical Report ITSTD-721-FR-90-21). Menlo Park, CA: SRI International, April 1990.
- Curry, David A. UNIX System Security: A Guide for Users and System Administrators. Reading, MA: Addison-Wesley Publishing Co., Inc., 1992.
- Ellis, Jim; Fraser, Barbara; and Pesante, Linda. "Keeping Internet Intruders Away." UNIX Review, vol. 12, no. 9 (September 1994), pp. 35-44.
- Garfinkel, Simson, and Spafford, Gene. Practical UNIX and Internet Security, 2nd ed. Sebastopol, CA: O'Reilly and Associates, Inc., 1996.
- Otros
- Barrett, Daniel J. Bandits on the Information Superhighway. Sebastopol, CA: O'Reilly and Associates, 1996.
- Best, Reba A. and Piquet, D. Cheryl. Computer Law and Software Protection: A Bibliography of Crime, Liability, Abuse, and Security, Jefferson, N.C.: McFarland, 1993.
- Cappel, James J.; Vanecek, Michael T.; and Vedder, Richard G. "CEO and CIO Perspectives on Competitive Intelligence." Communications of the ACM. (August 1999).
- Ermann, D. M.; Williams, M. B.; and Shauf, M. S. Computers, Ethics, and Society (Second Edition). New York: Oxford University Press, 1997.
- NIST Federal Information Processing Standards (FIPS) on Computer Security. <http://csrc.nist.gov/fips/>
- Power, Richard. "1999 CSI/FBI Computer Crime and Security Survey." Computer Security Journal, Volume XV, 2. San Francisco, CA: Computer Security Institute, 1999.
- Regan, Priscilla M. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: University of North Carolina Press, 1995.
- Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York, NY: Bantam Books, 1992.
- Stoll, Cliff. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York, NY: Doubleday, 1989.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

ANEXOS

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

ANEXO I

DESCRIPCIÓN DE LOS SISTEMAS DE SOFTWARE BASADO EN SERVICIOS WEB

ANEXO I

DESCRIPCIÓN DE LOS SISTEMAS DE SOFTWARE BASADO EN SERVICIOS WEB

¿Que es un servicio Web?

La otra conceptualización teórica del trabajo consiste en utilizar los sistemas basados en servicios Web para construir un modelo de plan de contingencia que este soportado sobre este tipo de aplicación para agilizar e independizar el Plan, de los recursos físicos e informáticos que pueda recibir la organización, pasibles de ataques y susceptibles a riesgos. Para ello veremos los siguientes puntos:

- Definiciones

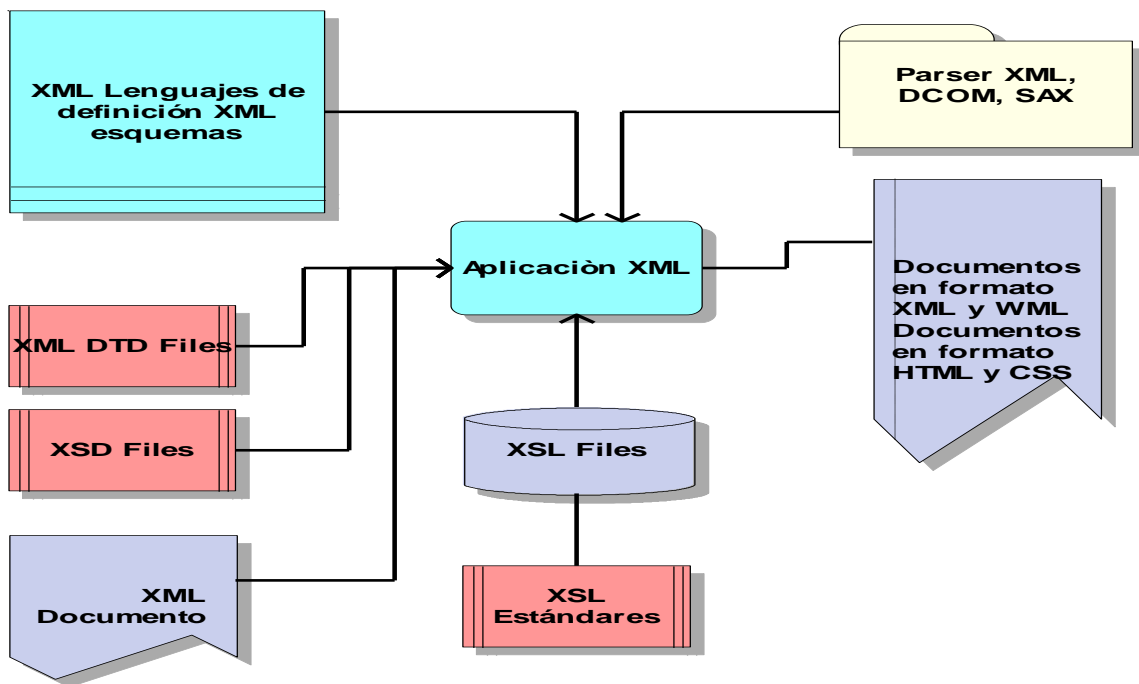
Los Servicios Web pueden definirse como entidades programables que actúan como cajas negras para proporcionar una determinada funcionalidad.

Los Servicios Web hacen uso de estándares de Internet, tales como HTTP o XML, por lo que dependen fuertemente de la aceptación de dichos estándares para solucionar el problema de interoperabilidad presente en las tecnologías actuales.

El siguiente gráfico muestra la estructura de una aplicación basada en XML, sus componentes y relaciones, figura:

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello



Los servicios Web XML, son los bloques de construcción básicos en la transición al proceso distribuido en Internet.

Un servicio Web se trata de un método perfecto para lograr que los objetos o componentes de un servidor acepten las solicitudes procedentes de los Clientes utilizando protocolos estándar de Internet, como HTTP o SMTP, figura extraída del documento descriptivo del framework .net en:

www.microsoft.com/latam/net/introduccion/default.asp



- Ud puede preguntar por un sitio o dispositivo y sus Web Servicios, o usar un directorio de servicios como UDDI
- Web Servicios son definidos en términos de los formatos y el orden de mensajes
- Web Servicio de Clientes puede send y receive mensajes usando SOAP
- Todas las capacidades son construidas usando el protocolo internet abierto



Ejemplos:

Servicio de índices de cotización que genera índices gráficos o información financiera en tiempo real.

Servicio de tráfico que ofrezca información sobre el estado del tráfico en Red de calles.

Servicios de cálculos (Calculadoras financieras o de hipotecas).

Noticias... El tiempo... etc.

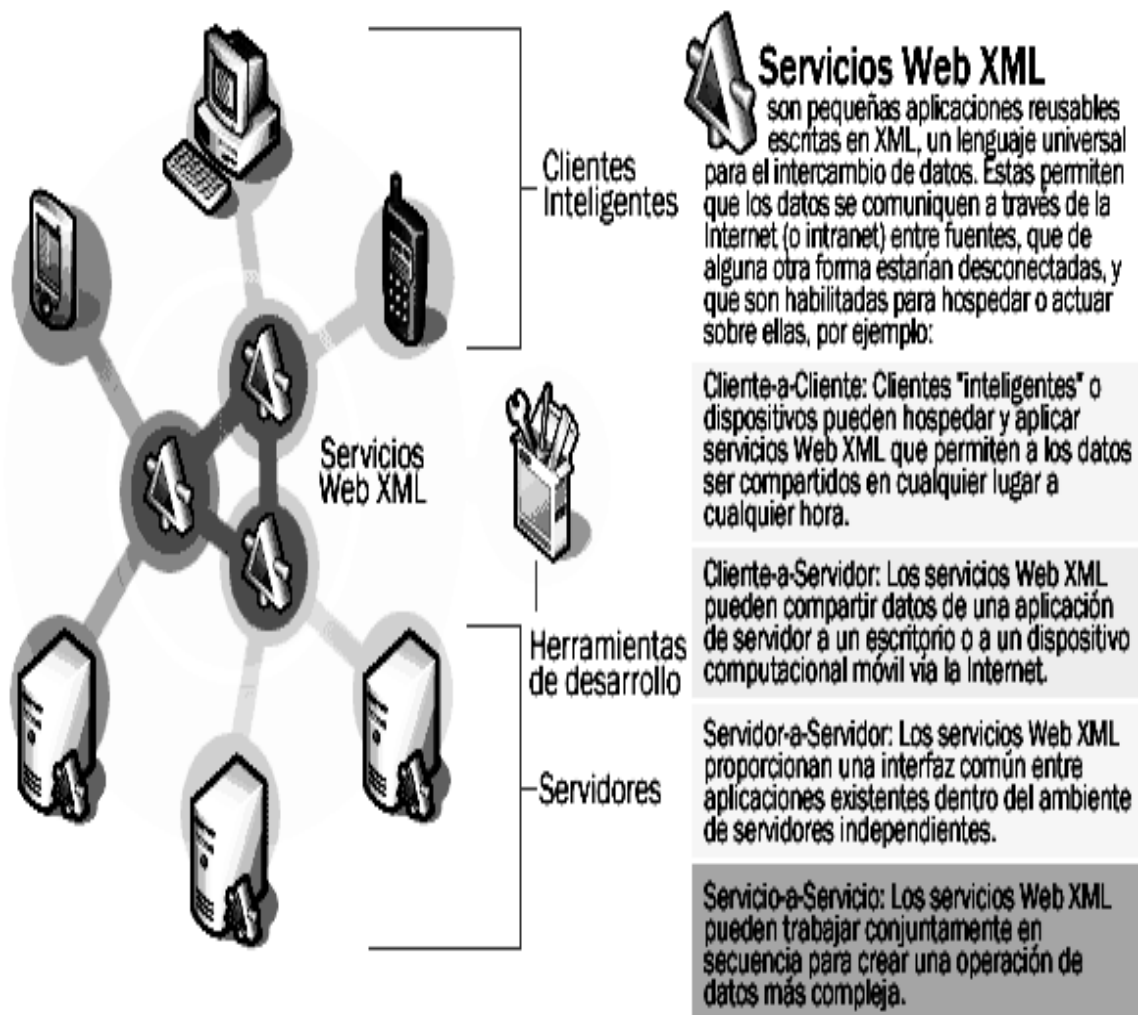
Un usuario podría desarrollar una aplicación de compras para obtener automáticamente la información de precios de varios fabricantes, que permitiera

seleccionar un fabricante, enviar el pedido al seleccionado y a continuación realizar seguimiento del envío hasta que sea recibido.

La aplicación del fabricante, además de exponer sus servicios en la Web, podría a su vez utilizar servicios Web XML para verificar el crédito del Cliente, (Veraz) realizar un cargo en su cuenta y realizar el envío con una empresa de transporte seleccionada al efecto.

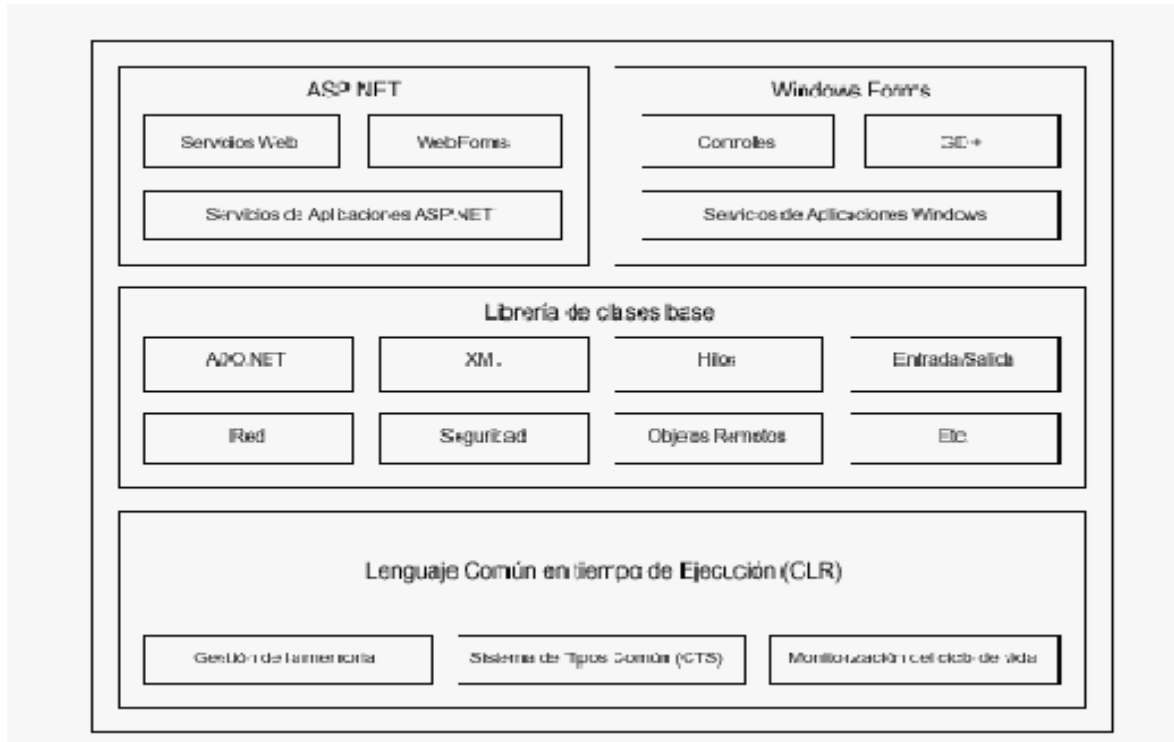
La siguiente figura muestra el concepto de Web services en la plataforma .NET de Microsoft, también obtenido del sitio

<http://www.microsoft.com/latam/net/introduccion/default.asp>



Descripción tecnologías utilizadas en Servicios Web

La estructura de un framework para desarrollo de sistemas basados en servicios Web, se corresponde con el siguiente gráfico tomado del framework Microsoft .Net, en la dirección: <http://www.microsoft.com/latam/net/introduccion/default.asp>, figura 1.1.



Servicios de Directorio en la Web:

Proporcionan una localización centralizada de un Servicio Web

Para la localización se ha definido la especificación Universal de Descubrimiento, Descubrimiento e Integración UDDI

UDDI son las páginas amarillas de los Servicios Web

Una entrada de directorio UDDI es un archivo XML–Páginas Blancas. Describen la compañía que ofrece el Servicio

–Páginas Amarillas. Incluyen Categorías Industriales.

–Páginas Verdes. Describen el interfaz al Servicio.

UDDI, en sí mismo, es un Servicio Web

Servicios de Localización:

La localización o descubrimiento es el proceso de descubrir uno o más documentos WSDL relacionados que describen un servicio Web.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Localización estática. Fichero .disco apunta a fichero WSDL

Localización dinámica. Lista los Servicios Web bajo una determinada URL.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

ANEXO II

ENCUESTAS REALIZADAS PARA ESTABLECER SITUACIÓN DE LOS PLANES DE CONTINGENCIA EN EMPRESAS DE SOFTWARE

ANEXO II

Encuestas realizadas para establecer situación de los Planes de contingencia en empresas de software

Estimado Domingo, no hay inconvenientes, espero le sea de utilidad, Saludos afectuosos

Cualquier inconveniente me avisa

----- Original Message -----

From: [DOMINGO DONADELLO](#)

To: [Liliana Cecilia Romanin](#)

Sent: Wednesday, November 19, 2008 11:51 AM

Subject: Consulta sin compromiso

Estimada Liliana,

Estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización,

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas,

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

Aguas Bonaerenses S.A.

Servicios Públicos de distribución y saneamiento de agua.

Captación, Potabilización, distribución de agua potable y tratamiento de desagües cloacales.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Calle 56 N° 534, La Plata (C.P. 1900)

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no) Si

en que porcentaje aproximado? 70%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no) No

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no) NO en su totalidad, existen backups en otros sitios fuera del Head Quarter, pero no un sitio de réplica fuera del Head Quarter

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no) No

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no) NO

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no) SI

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no) NO

10.-Existe el plan en la Web o en intranet? (si/no) NO

Desde ya muchas gracias por su colaboración,

Saludo atte..

Domingo Donadello

Estimado Domingo, le respondo al pie de cada pregunta.

Saludos cordiales

Silvia Iglesias

----- Original Message -----

From: [DOMINGO DONADELLO](#)

To: [IT Secures Business -Silvia Iglesias & Asoc.](#)

Sent: Wednesday, November 19, 2008 1:10 PM

Subject: consulta sin compromiso

Estimada Silvia,

Molesto su atención porque estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización ITSB Silvia Iglesias & Asoc. Auditoría y Consultoría, CABA

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas, Saludo atte..

Domingo Donadello

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

ITSB Silvia Iglesias & Asoc.

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no) si

en que porcentaje aproximado? 90%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no) no

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no) si

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no) si

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra) mensualmente

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no) no

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no) si

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no) si

10.-Existe el plan en la Web o en intranet? (si/no) no

Desde ya muchas gracias por su colaboración,

Saludo atte.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Domingo Donadello

Hola Domingo,

Lindo tema seleccionaste!!!

te cuento que fui testada en mi desarrollo por especialistas Americanos de IBM y tengo un nivel alto en el tema , o sea para lo que necesitessolo avísame.

Saludos

Liliana

te contesto entre párrafos

2008/11/19 DOMINGO DONADELLO <DDONADELLO@iram.org.ar>

Estimada Liliana,

Molesto su atención porque estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización, o las que Ud. asesora.

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas,

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

Rubro Bancario

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no)

Si

en que porcentaje aproximado?

70%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no)

Si

4.- En particular existe un plan de recuperación de desastres para

Si

los sistemas informáticos? (si/no)

5.- En el caso de estos planes incluyen

una revisión periódica de los mismos? (si/no)

Si

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

Depende de la criticidad del negocio /componente.-

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no)

Si

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no)

Si

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no)

Si

10.-Existe el plan en la Web o en intranet? (si/no)

Si

Desde ya muchas gracias por su colaboración,

Saludo atte.

Domingo Donadello

Hola Domingo. No es ninguna molestia. Le respondo mas abajo.

Aprovecho para saludarlo y consultarle, ya que yo también estoy entregando mi tesis de grado sobre como implementar ISO 90003 en empresas de software, y si me permite quisiera incorporarlo en la sección de agradecimientos de la tesis, ya que en los trabajo que hemos mantenido durante estos años me a transferido muchos conocimientos y experiencias las cuales me han sido de mucha utilidad y he aplicado parte de ello en este entregable. Si no le molesta me gustaría incorporarlo en esta sección de agradecimientos especiales.

Saludos y aguardo su respuesta para avanzar.

Walter

De: DOMINGO DONADELLO [mailto:DDONADELLO@iram.org.ar]

Enviado el: miércoles, 19 de noviembre de 2008 13:06

Para: Walter Grasso

Asunto: consulta sin compromiso

Estimado Walter,

Molesto su atención porque estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización, TSOFT y Tecnosoftware,

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas,

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

TSOFT - IT – Capital Federal

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no)

en que porcentaje aproximado?

SI – 90%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no)

SI

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no)

SI

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no)

SI

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

No esta establecido el periodo en la actualidad

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no)

SI

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no)

SI

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no)

NO requeridos actualmente

10.-Existe el plan en la Web o en intranet? (si/no)

INTRANET

Desde ya muchas gracias por su colaboración,

Saludo atte.

Domingo Donadello

Estimado Domingo

Como esta?

en su mail las respuestas

Saludos cordiales

Jorge Palacios

-----Original Message-----

From: "DOMINGO DONADELLO" <DDONADELLO@iram.org.ar>

To: "Jorge Edgardo Palacios" <jpalacios@fxinformatica.com>

Date: Wed, 19 Nov 2008 13:01:50 -0200

Subject: consulta sin compromiso

Estimado Jorge,

Molesto su atención porque estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización,

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas,

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

FX Informatica s.a.

Desarrollo de software

Ciudad Jardin Lomas del Palomar , Buenos Aires

2.- La gestión organizacional se basa en el uso de tecnología informática y

comunicaciones? (si/no)

en que porcentaje aproximado?

SI en un 80%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no)

SI

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no)

SI

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no)

SI

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

12 meses

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no)

SI

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no)

SI

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no)

SI

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

10.-Existe el plan en la Web o en intranet? (si/no)

en intranet

Desde ya muchas gracias por su colaboración,

Saludo atte.

Domingo Donadello

Buenos días.

Le paso los datos solicitados, que me proporcionaron en Lagash (están abajo en letra azul).

Saludos.

Andrea Laura Luna

Lagash Systems S.A.

Venezuela 4269 Piso 4.

Ciudad Autónoma de Buenos Aires.

C.P.: C1211ABE.

Tel/Fax: (54 11) 4982-4185 / 4982-3303.

De: DOMINGO DONADELLO [mailto:DDONADELLO@iram.org.ar]

Enviado el: Miércoles, 19 de Noviembre de 2008 12:04 p.m.

Para: Andrea Luna

Asunto: consulta sin compromiso

Estimada Andrea,

Molesto su atención porque estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización,

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas,

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

Lagash Systems S.A. – Desarrollo de Software y Consultoría especializada – Cap. Fed.

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no) SI

en que porcentaje aproximado? 90%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no) parcialmente

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no) parcialmente

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no) si

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra) los sistemas de backup y seguridad reportan su estado diariamente y además se hace una prueba trimestral.

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no) parcialmente

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no) parcialmente

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no) si

10.-Existe el plan en la Web o en intranet? (si/no) no

Desde ya muchas gracias por su colaboración,

Saludo atte.

Domingo Donadello

Hola Domingo

Al contrario, no representa ninguna molestia!! Te pido disculpas por la demora en responderte, pero estaba de viaje y con bastante lío.

Te envió mis respuestas:

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

Nombre: Avanzit Tecnología S.A.

Rubro: Suministros y Servicios Informáticos para Telecomunicaciones

Lugar de Residencia: Ciudad de Buenos Aires

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no) en que porcentaje aproximado?

En la actualidad el porcentaje de la gestión organizacional que se basa en el uso de tecnología informática es de un 50%. Sin embargo nos encontramos en proceso de implementación de un sistema ERP que elevará ese porcentaje a un 70% aproximadamente, a partir del 1 de enero de 2009.

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no)

Si. Tenemos un procedimiento de backup documentado.

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no)

No. No está documentado el plan de recuperación de desastres. Sólo está documentado el procedimiento de resguardo de la información.

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no)

Si. En el caso del procedimiento de backup citado en la respuesta 3, este forma parte de nuestro sistema de gestión de la calidad, y como tal, sufre revisiones. Además, llevamos un registro de los resguardos de datos periódicos que indica fecha y tipo.

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

Nuestro sistema de gestión de calidad indica que las revisiones deben realizarse cada 2 años.

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no)

Si. Lo puede ver en la intranet.

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no)

Si. Se realiza capacitación ante cualquier modificación del documento que la requiera.

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no)

No

10.-Existe el plan en la Web o en intranet? (si/no)

Si. El procedimiento de respaldo de datos está disponible en la intranet.

Espero que las respuestas te sean de ayuda, y te deseo que tengas mucha suerte con la tesis!

Saludos

Ricardo

Asunto: RE: consulta sin compromiso

Estimado Domingo,

Jorge Buchter nos ha enviado su consulta referente al plan de contingencia, aquí le paso las respuestas a las mismas.

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

Nombre: Posbeyikian, Buchter & Asoc. S.R.L.

Rubro: Consultora de Sistemas

Actividad: Desarrollo de Software para Freight Forwarders

Lugar de Residencia: Vicente Lopez, Buenos Aires.

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no)

SI

- en que porcentaje aproximado?

100%

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no)

No

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no)

Si. En nuestros procedimientos de calidad tenemos un plan para mantenimiento de Software y Hardware con sistema de backups diarios, tanto de la información de la

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

aplicación como de la base de pedidos y seguimiento de temas de nuestros clientes online.

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no)

Si

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

12 Meses

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no)

No

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no)

No

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no)

No

10.-Existe el plan en la Web o en intranet? (si/no)

No

Muchas Gracias

De: Patricia Scalzone [mailto:patricias@vemn.com.ar]

Enviado el: miércoles, 26 de noviembre de 2008 11:54 a.m.

Para: DOMINGO DONADELLO

Asunto: RE: consulta sin compromiso

Hola Domingo.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Antes que nada perdón por la demora, se me había escondido.

Por otro lado, pareciera que somos un desastre, si bien tengo todo bajo control, y todo de forma local y en servidor, la realidad es lo que contesté allí.

Si está mal interpretado, por favor acémelo saber. Lo tomé como Vemn, y no como mis clientes.

Saludos,

Patricia

From: DOMINGO DONADELLO [mailto:DDONADELLO@iram.org.ar]

Sent: Miércoles, 19 de Noviembre de 2008 01:15 p.m.

To: DOMINGO DONADELLO; patricias@vemn.com.ar

Subject: RE: consulta sin compromiso

Perdón me equivoque el texto, considera el siguiente:

Estimada Patricia

Molesto su atención porque estoy finalizando mi tesis de Maestría en Ingeniería Informática, en la cual expongo sobre planes de contingencia y gestión de riesgos en organizaciones,

En caso de no resultarle muy molesto, le solicito sin ningún compromiso la posibilidad de que Ud. complete algunos datos referidos a la situación de los Planes de contingencia y gestión de riesgos en su organización, o a las empresas a las que das servicios,

Por supuesto que si son datos confidenciales no considere este pedido y por favor pido disculpas,

1.- Datos de la organización (nombre, rubro o actividad principal, lugar de residencia sin dirección)

 VEMN S.A., Consultora en Informática, Desarrollo de Soluciones
Informáticas, Ituzaingó, Buenos Aires

2.- La gestión organizacional se basa en el uso de tecnología informática y comunicaciones? (si/no)

en que porcentaje aproximado?

Todo nuestro desarrollo se basa en el uso de tecnologías.

3.- Existe documentado un Plan de contingencias que incluya los procesos y tecnología informática? (si/no)

4.- En particular existe un plan de recuperación de desastres para los sistemas informáticos? (si/no)

5.- En el caso de estos planes incluyen una revisión periódica de los mismos? (si/no)

6.- En caso de si, con qué frecuencia? (3,6,12,18 meses, otra)

7.- El personal tiene accesible la documentación del Plan de Contingencia? (si/no)

8.- Periódicamente se actualiza la información y la capacitación del personal involucrado? (si/no)

9.- Se realizan pruebas y simulaciones de eventos a la seguridad? (si/no)

10.-Existe el plan en la Web o en intranet? (si/no)

Desde ya muchas gracias por su colaboración,

Saludo atte.

Domingo Donadello

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

ANEXO III

SISTEMAS Y MÉTODOS PARA LA GESTIÓN DE RIESGOS

ANEXO III

SISTEMAS Y MÉTODOS PARA LA GESTIÓN DE RIESGOS

En este anexo se desarrolla el concepto de gestión de riesgos, para ello tomamos como base lo establecido en la norma IRAM 17550, publicada por IRAM en 2008, en la cual participó el autor de la tesis, como miembro del Comité de Riesgos, de IRAM, que desarrolla las normas en dicho organismo en particular en el Comité de Seguridad de la información y en el Comité de gestión de la calidad en el cual está establecido el subcomité de gestión de riesgos.

A continuación se describen consideraciones planteadas en la norma con comentarios de aplicabilidad.

Premisas

La adopción de un sistema de gestión de riesgos debería ser una decisión estratégica de la organización.

Aunque el concepto de riesgo es a menudo interpretado en términos de peligros o impactos negativos respecto de la gestión y economía de la organización, la norma interpreta al riesgo como exposición a las consecuencias de la incertidumbre, o cambios potenciales respecto de lo que está planeado o se espera que suceda. El proceso que describe la norma se aplica tanto a la gestión de los beneficios potenciales como de las pérdidas potenciales, siendo en la práctica aplicada para analizar pérdidas potenciales.

No es el propósito de la Norma proporcionar uniformidad en la estructura de los sistemas de gestión de riesgos o en la documentación asociada a los mismos, ya que cada organización puede desarrollar un sistema de gestión distinto que cumpla con los requisitos establecidos y permita gestionar los riesgos de manera adecuada.

Por esto es que los sistemas diseñados mediante el trabajo presentado en la presente tesis, incluyen guías, procedimientos, herramientas y documentos que ayuden a las organizaciones a implementar sus sistemas de gestión de riesgos y contingencias de una manera eficaz que permita una continua actualización de conceptos y de la gestión.

Aplicación:

Esta norma puede ser utilizada por partes internas de una organización y externas a la misma, incluyendo organismos de certificación, para evaluar la capacidad de la organización para administrar riesgos en su actividad y para implementar y mejorar en forma continua un sistema que le permite mantener los riesgos bajo control y cumpliendo las restricciones y requisitos de todas las partes interesadas incluyendo, reglamentaciones, legislación y procedimientos propios de la organización.

Significado de la gestión de riesgos

Gestionar riesgos significa administrarlos para lograr un balance apropiado, maximizando las oportunidades de obtener beneficios y minimizando los impactos adversos (daños y perjuicios).

La gestión de riesgos, es una parte integral de una buena práctica gerencial y un elemento esencial de buen gobierno corporativo. Tanto es así que todas las empresas que cotizan en la Bolsa de Nueva York, deben implementar sistemas de control de riesgos tanto informáticos como financieros basándose en la Ley Sarbanes Oxley, que obliga a una auditoria de tercera parte que garantice la aplicación de los controles establecidos sobre los procesos y activos de la organización.

En este sentido, un ejemplo de aplicabilidad de lo planteado como diseño de sistemas de soporte en esta tesis, fue aplicado en la Corporación Siemens y se muestra en el capítulo IV del cuerpo principal de la Tesis.

La gestión de riesgos es un proceso iterativo que permite la mejora continua del proceso de toma de decisiones y facilita a las organizaciones optimizar su desempeño, aumentando la probabilidad de arribar a los objetivos propuestos en forma consistente.

Gestionar los riesgos implica establecer una infraestructura y una cultura organizacional apropiada y aplicar un método lógico y sistemático para establecer el contexto esto es:

Identificar, analizar, evaluar, tratar, supervisar y comunicar riesgos asociados con cualquier actividad, función o proceso clave de la organización, de forma tal que permita a las mismas, minimizar pérdidas, daños y perjuicios y maximizar beneficios en su gestión.

Para ser más eficaz, la gestión de riesgos debería formar parte de la cultura de la organización. Es decir, deberá estar incorporada en la filosofía, prácticas y procesos de negocio, más que ser vista o practicada como una actividad separada y obligatoria. Cuando se logra esto, todos en la organización pasan a estar involucrados en el sistema de gestión de riesgos.

La premisa subyacente en la gestión de riesgos es que cada organización -con o sin fines de lucro- del ámbito privado o gubernamental, existe con el fin de proveer valor a las personas, grupos u organizaciones que puedan tener algún interés o ser consideradas partes interesadas.

Situaciones de incertidumbre:

Toda organización se enfrenta a situaciones de incertidumbre. El desafío es evaluarlas y determinar el grado de incertidumbre que la organización está dispuesta a aceptar.

La incertidumbre representa tanto amenazas como oportunidades, con el potencial de erosionar o enriquecer el valor. La gestión de riesgos de la organización provee una estructura conceptual para que la gestión conviva de manera racional con la incertidumbre y con los riesgos y oportunidades asociados, lo cual enriquece su capacidad para generar valor agregado.

La gestión de riesgos es una disciplina de rápida evolución en la que pueden encontrarse diferentes criterios sobre cuales son los elementos que incluye, cómo debe ser conducida y, fundamentalmente, para qué sirve. En este sentido, en el marco de la norma se encuentran los acuerdos sobre:

- Objetivo de la gestión de riesgos.
- Terminología relacionada.
- Proceso mediante el cual deberá ser llevada a cabo la gestión de riesgos.

Propósito de la Norma IRAM:

La norma presenta los requisitos para certificar por un organismo de certificación externo, un sistema de gestión de riesgos (SGR) y se deberá utilizar en conjunto con la norma IRAM 17550 Sistema de gestión de riesgos - Directivas generales, para el desarrollo e implementación de un sistema de gestión de riesgos consistente.

Enfoque en los procesos:

La norma promueve la adopción del enfoque basado en procesos para establecer, implementar, operar, realizar el seguimiento, mantener y mejorar la eficacia de un SGR en una organización.

La Norma adopta la siguiente definición de la IRAM-ISO 9000:2000: "Para que las organizaciones operen de manera eficaz, tienen que identificar y gestionar numerosos procesos interrelacionados y que interactúan. A menudo el resultado de un proceso constituye directamente el elemento de entrada del siguiente proceso. La identificación y gestión sistemática de los procesos desarrollados y operativos en una organización y en particular las interacciones entre tales procesos se conocen como "enfoque basado en procesos".

Una ventaja del enfoque basado en procesos es el control continuo que proporciona sobre los vínculos entre los procesos individuales dentro del sistema de gestión de toda la organización, así como sobre la combinación e interacción de los mismos.

El enfoque basado en procesos incentiva a los usuarios a enfatizar la importancia de:

- a) comprender los requisitos del sistema de gestión de riesgos de la Organización y la necesidad de establecer políticas, procedimientos y objetivos para éste;
- b) implementar y operar actividades de control dentro del marco de la gestión de riesgos de la organización en forma completa;
- c) realizar el seguimiento, revisar el desempeño y la eficacia del SGR;
- d) implementar la mejora continua basada en mediciones objetivas.

El modelo P-D-C-A:

La norma propone adoptar el marco metodológico "Planificar-Hacer-Verificar-Actuar" (PHVA), aplicado a los procesos del SGR del modo siguiente:

Planificar: establecer los objetivos y procesos necesarios para conseguir un efectivo SGR de acuerdo con las políticas y objetivos de la organización.

Hacer: implementar el proceso de gestión de riesgos.

Verificar: realizar el seguimiento y la evaluación de los procesos respecto de las políticas, objetivos y requisitos del SGR, e informar sobre los resultados.

Actuar: tomar acciones para mejorar continuamente el desempeño de los procesos.

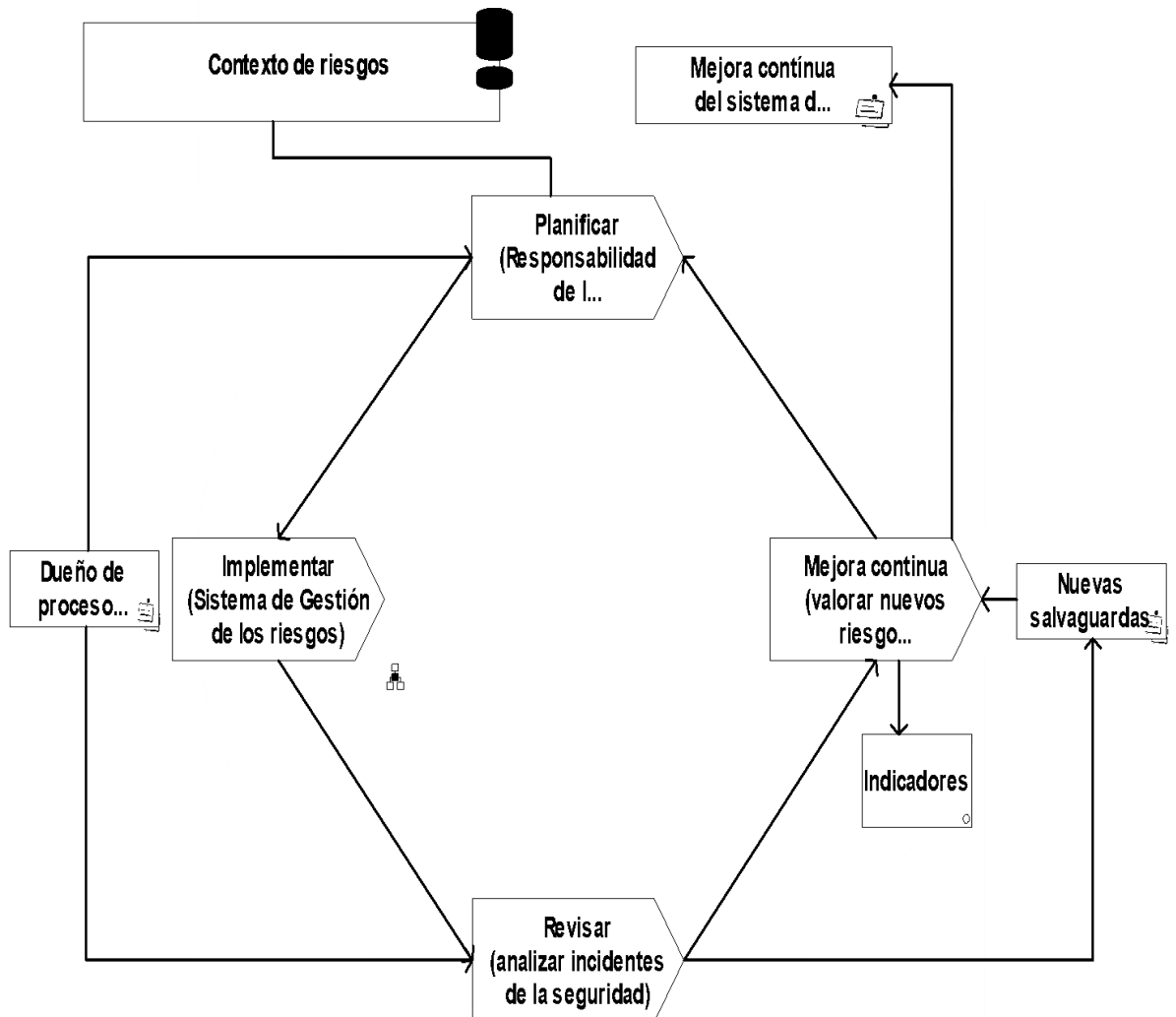


Figura Anexo III - 1 – Modelo de un Sistema de Gestión de Riesgos (SGR) basado en Procesos

Referencias normativas:

Los documentos normativos que se indican a continuación son indispensables para el desarrollo e implementación de un SGR.

Para los documentos normativos en los que se indica el año de publicación, se aplican las ediciones citadas.

Para los documentos normativos en los que no se indica el año de publicación, se aplican las ediciones vigentes, incluyendo todas sus modificaciones.

IRAM 17550 Sistema de gestión de riesgos - Directivas generales.

IRAM-ISO 19011 Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiental.

ISO/IEC Guide 73:2002 Risk management - Vocabulary - Guidelines for use in standards

ISO/IEC CD Guide 73:2007 Risk management - Vocabulary”

El sistema organizacional para la de gestión de riesgos:

Para que una organización establezca, documente, implemente y mantenga actualizado un sistema de gestión de riesgos y mejore continuamente su eficacia de acuerdo con los requisitos de la norma, la organización deberá:

- a) identificar los procesos organizacionales dentro de los cuales se deban gestionar riesgos e incluirlos en el alcance del SGR,
- b) determinar la secuencia de interacción de estos procesos,
- c) documentar el proceso de gestión de riesgos utilizado por la organización, incluyendo la forma en que le organización establece el contexto, identifica, analiza, evalúa y trata los riesgos, los supervisa, los revisa, y los consulta.
- d) determinar los criterios y los métodos necesarios para asegurarse de que tanto la operación como el control de estos procesos sean eficaces;
- e) asegurar la disponibilidad de recursos e información necesarios para apoyar la operación y el seguimiento de estos procesos,
- f) realizar el seguimiento, la medición y el análisis de estos procesos, e
- g) implementar las acciones necesarias para alcanzar los resultados planificados y la mejora continua de estos procesos.

En los casos en que la organización opte por contratar externamente cualquier proceso que afecte la gestión de riesgos (transferencia de riesgos), la misma deberá asegurarse de gestionar los riesgos dentro de tales procesos externalizados. La gestión de riesgos sobre dichos procesos contratados externamente deberá también

estar identificada dentro del SGR. Alternativamente se podrá aceptar, en caso de poseerlo, el SGR utilizado por la tercera parte contratada.

Los procesos necesarios para el sistema de gestión de riesgos a los que se ha hecho referencia anteriormente deberían incluir los procesos para las actividades de gestión, la provisión de recursos, la evaluación de los resultados de la gestión de riesgos y las mediciones de los indicadores asociados a los procesos del sistema.

Documentación:

La documentación del SGR deberá incluir:

- a) declaraciones documentadas de la política de gestión de riesgos y los objetivos de control;
- b) la declaración de aplicabilidad de la Política establecida (si algún requisito no es aplicable para la organización).
- c) el alcance del SGR y la descripción del proceso de gestión de riesgos, que deberá estar acorde a lo descrito en la norma IRAM 17550;
- d) los procedimientos y controles de apoyo del SGR, incluyendo los procedimientos documentados necesarios para que la organización asegure la planificación efectiva, la operación y el control eficaz del proceso de gestión de riesgos;
- e) el informe de evaluación de riesgos;
- f) los planes de tratamiento de riesgos;
- g) los registros requeridos por la norma;

Aclaraciones: El término "procedimiento documentado" que se menciona, significa que el procedimiento está establecido, documentado, implementado y es mantenido. La documentación y los registros pueden estar en cualquier formato o tipo de medio. Se recomienda la conformación de un manual del SGR que contenga la documentación del SGR referenciada anteriormente.

Gestión y control de los documentos del SGR:

Los documentos requeridos por el SGR deberán estar protegidos y controlados. Para tal fin, la organización deberá establecer un procedimiento documentado para definir e implementar las acciones de gestión necesarias para:

- a) aprobar los documentos en cuanto a su adecuación, en forma previa a su emisión y distribución;
- b) revisar y actualizar los documentos cuando sea necesario, y aprobarlos nuevamente;
- c) asegurar que los cambios y el estado de revisión actual de los documentos son identificados;
- d) asegurar que las versiones pertinentes de los documentos aplicables están disponibles en los puntos de uso;
- e) asegurar que los documentos se mantengan legibles y fácilmente identificables;
- f) asegurar que los documentos de origen externo estén identificados;
- g) asegurarse que la distribución es controlada, tanto para los documentos externos o internos de la organización;
- h) prevenir el uso no intencionado de documentos obsoletos;
- i) aplicar una adecuada identificación de los documentos obsoletos, si se retienen por cualquier causa.

Registros del SGR:

Complementando lo determinado para el control de documentos se deberá gestionar y controlar los registros del SGR:

- j) Los registros se deberán establecer, proteger, controlar y mantener para proporcionar evidencia de la operación eficaz del SGR.
- k) Los registros deberán permanecer legibles, fácilmente identificables y recuperables. Para tal fin, la organización deberá establecer un procedimiento documentado para definir e implementar los controles necesarios para la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición final de los registros.

- l) La organización deberá definir y mantener los registros para brindar evidencia del desempeño de los procesos del SGR y de todos los incidentes significativos del mismo.

Política de Gestión de riesgos

La alta dirección debe asegurarse de que la política de gestión de riesgos:

- a) sea adecuada al propósito de la organización,
- b) proporcione un marco de referencia para establecer y revisar los objetivos de la gestión de riesgos
- c) sea comunicada y entendida dentro de la organización, y
- d) se revise periódicamente para asegurar su continua adecuación.

Revisión por la Dirección de la organización:

La alta dirección debe, a intervalos planificados, revisar el sistema de gestión de riesgos implementado, para asegurarse de su conveniencia, adecuación y eficacia continuas. La revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de efectuar cambios en el sistema de gestión de riesgos incluyendo la política de gestión de riesgos y los objetivos de la gestión de riesgos.

Deben mantenerse registros de las revisiones del SGR efectuadas por la dirección.

Información para la revisión

La información de entrada para la revisión por la dirección debe incluir, como mínimo:

- a) resultados de auditorías de cumplimiento de los procedimientos establecidos en el SGR
- b) retroalimentación de partes interesadas.
- c) desempeño de los procesos de gestión de riesgos y los episodios adversos denunciados mediante gestión de incidentes que puedan ocasionar pérdidas, daños y perjuicios.
- d) estado de las acciones correctivas y preventivas
- e) acciones de seguimiento de revisiones por la dirección previas
- f) cambios que podrían afectar al sistema de gestión de riesgos, y
- g) recomendaciones para la mejora

Resultados de la revisión

Los resultados de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con

- a) la mejora de la eficacia del sistema de gestión de riesgos y sus procesos
- b) las necesidades de recursos

Cobertura de cargos, roles y competencia:

La organización deberá

- a) determinar la competencia necesaria para el personal que realiza trabajos que afecten a la gestión de riesgos
- b) proporcionar formación o tomar otras acciones para satisfacer dichas necesidades
- c) evaluar la eficacia de las acciones tomadas
- d) asegurarse de que su personal es consciente de la pertinencia e importancia de sus actividades y de cómo contribuyen al logro de los objetivos de la gestión de riesgos, y

- e) mantener los registros apropiados de la educación, formación, habilidades y experiencia de todo el personal afectado.

El Proceso de gestión de riesgos

Aquí se describe una breve visión general del proceso de gestión de riesgos.

La gestión de riesgos es una parte integrante del sistema de procesos de gestión de la organización. La gestión de riesgos es un proceso multifacético, por lo que las tareas involucradas son a menudo llevadas a cabo por un equipo multidisciplinario. Es un proceso definido de mejora continua, cuya incorporación en procesos de negocio clave existentes resulta beneficiosa.

Podrá ser aplicada a todos los niveles de una organización: a nivel estratégico y a niveles tácticos y operacionales. También puede ser aplicada a proyectos específicos, para sustentar decisiones específicas o para administrar áreas específicas con riesgo reconocido. Para cada etapa del proceso deberían mantenerse registros adecuados, suficientes como para satisfacer a una auditoría interna o una auditoría independiente.

Elementos principales:

Los elementos principales del proceso de gestión de riesgos, son los siguientes:

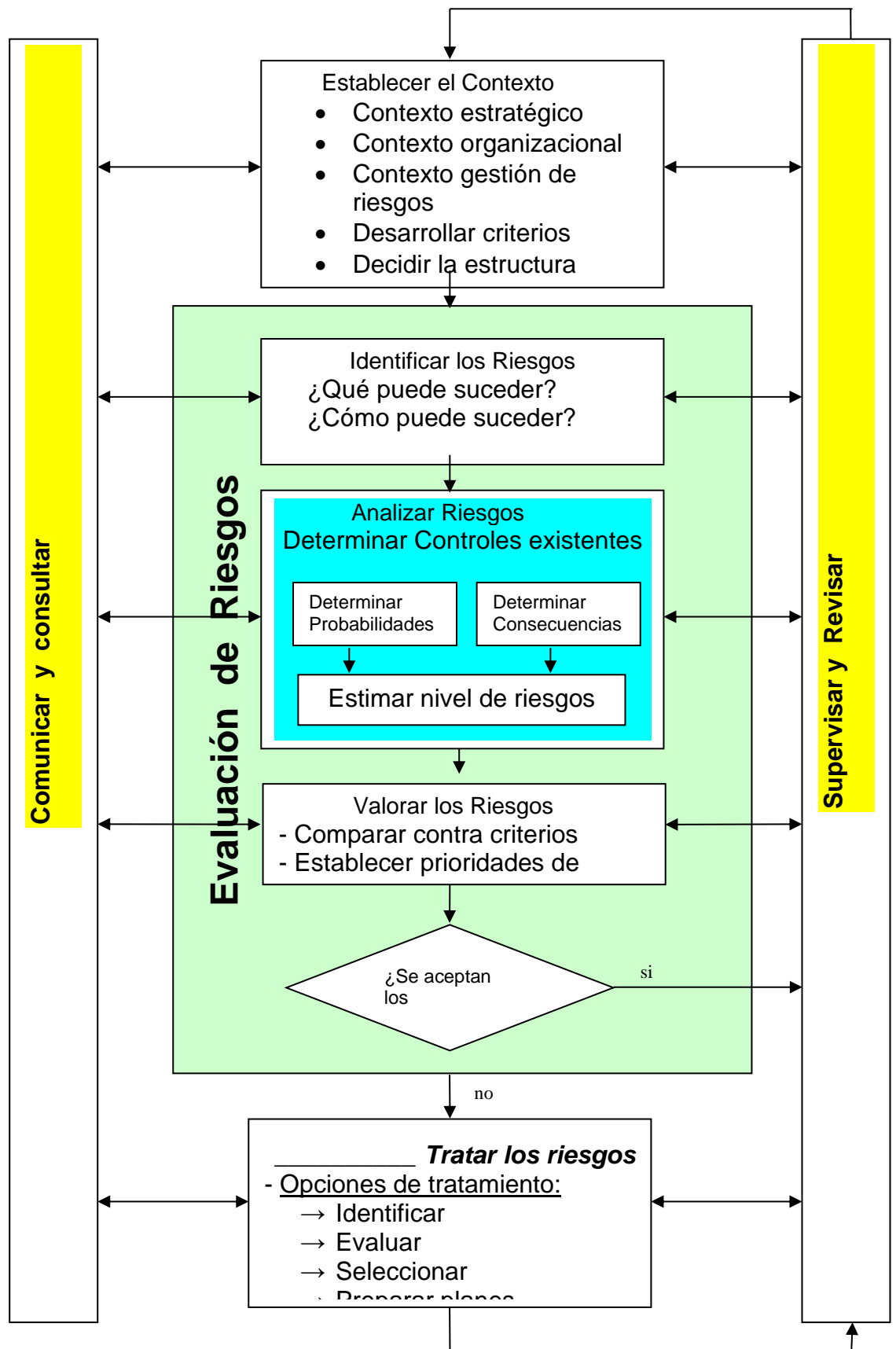
- a) Establecer el contexto: establecer los contextos estratégico, organizacional y de gestión de riesgos en los cuales tendrá lugar el resto de los procesos. Deberán establecerse los criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.
- b) Identificar riesgos: identificar qué, por qué, dónde, cuándo y cómo los eventos a la seguridad, podrían afectar (impedir, degradar, demorar o facilitar) el logro de los objetivos estratégicos y operativos de la organización.
- c) Analizar riesgos: determinar y analizar los riesgos potenciales, en términos de consecuencia y probabilidad en el contexto de los controles existentes. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que esas consecuencias puedan ocurrir. Consecuencia y probabilidad se podrían combinar para producir un nivel estimado de riesgos.
- d) Valorar riesgos: comparar los niveles estimados de riesgo contra los criterios que se hayan preestablecido y considerar el balance entre beneficios potenciales y resultados adversos. Esto posibilita que se ordenen los riesgos

como para identificar las prioridades de los mismos respecto de su impacto en la gestión. Si los niveles de riesgo establecidos son bajos podría caer en una categoría aceptable es decir de convivir con el riesgo y no se requeriría tratamiento ni salvaguardas.

- e) Tratar los riesgos: desarrollar e implementar estrategias, salvaguardas y planes de acción específicos, analizando el costo-beneficio para aumentar los beneficios potenciales y reducir los costos potenciales. En base al análisis y valoración de riesgos (puntos c y d), si es que de dicho análisis surgiera la necesidad. Si los niveles de riesgo establecidos son bajos y son tolerables entonces no se requiere tratamiento ni salvaguardas.
- f) Supervisar y revisar continuamente: supervisar y revisar a intervalos planificados, el desempeño del sistema de gestión de riesgos y procurar detectar cambios significativos, que pudieran afectar la adecuación o la relación costo-beneficio de los controles implementados.
- g) Comunicar y consultar: comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del proceso de gestión de riesgos, interpretando al proceso como un todo.
- h) Evaluación de riesgos: proceso global de identificar riesgos, analizar riesgos y valorar riesgos.
- i) Documentar y registrar: registrar en forma adecuada cada etapa del proceso de gestión de riesgos. Documentar las hipótesis, métodos, fuentes de datos, los análisis efectuados, los resultados y las razones para las decisiones tomadas.

Ver cuadro adjunto con el proceso de gestión de riesgos tomado de la IRAM 17550.

Figura Anexo III - 2 Proceso de Gestión de Riesgos detallado



Planificación continúa del proceso de gestión de riesgos:

La organización debe planificar y controlar el proceso de gestión de riesgos en forma periódica.

Durante la planificación del proceso de gestión de riesgos la organización debe determinar

- a) las etapas del proceso de gestión de riesgos
- b) la revisión, verificación y validación, apropiadas para cada etapa, y
- c) las responsabilidades y autoridades del personal en todos los niveles, para el proceso de gestión de riesgos

La organización debe gestionar las interfaces entre los diferentes grupos involucrados en el proceso de gestión de riesgos para asegurar la comunicación eficaz y una clara asignación de responsabilidades.

Los resultados de la planificación deben actualizarse, según sea apropiado, a medida que progresa el proceso de gestión de riesgos

Elementos de entrada para al proceso de gestión de riesgos

Deben determinarse los elementos de entrada relacionados con los requisitos del proceso de gestión de riesgos y mantenerse registros.

Estos elementos de entrada deben incluir:

- a) los requisitos legales, reglamentarios y regulaciones específicas de la actividad aplicables y que deberán ser considerados en los procedimientos que se definan para el SGR.
- b) la información proveniente de procesos previos de gestión de riesgos similares, cuando sea aplicable, y
- c) cualquier otro requisito esencial para el proceso de gestión de riesgos

Resultados del proceso de gestión de riesgos:

Los resultados del proceso de gestión de riesgos deben proporcionarse de tal manera que permitan la verificación respecto a los elementos de entrada y deben aprobarse antes de su liberación e implementación.

Los resultados del proceso de gestión de riesgos deberán:

- a) cumplir los requisitos de los elementos de entrada
- b) proporcionar información apropiada para los procesos relacionados
- c) contener o hacer referencia a los criterios de control de riesgos, y
- d) especificar los objetivos mínimos para que los resultados sean considerados aceptables.

Revisión del proceso de gestión de riesgos

En las etapas adecuadas deben realizarse revisiones sistemáticas del proceso de gestión de riesgos de acuerdo con lo planificado.

Evaluar la capacidad de los resultados para cumplir los requisitos, e

- a) identificar cualquier problema y proponer acciones correctivas necesarias

Los participantes en dichas revisiones deben incluir representantes de las funciones relacionadas con la(s) etapa(s) del proceso de gestión de riesgos que se está(n) revisando, deben mantenerse registros de los resultados de las revisiones y de cualquier acción que sea necesaria realizar.

Verificación del proceso de gestión de riesgos

Se deberá realizar la verificación, de acuerdo con lo planificado, para asegurarse de que los resultados del proceso de gestión de riesgos cumplen los requisitos de los elementos de entrada. Deben mantenerse registros de los resultados de las revisiones y de cualquier acción a realizar que sea necesaria.

Validación del proceso de gestión de riesgos

Se deberá realizar la validación del proceso de gestión de riesgos de acuerdo con lo planificado para asegurarse de que los resultados satisfacen los requisitos para su

aplicación específica. Siempre que sea factible, la validación debe completarse antes de la puesta en marcha del proceso de gestión de riesgos. Deben mantenerse registros de los resultados de la validación y de cualquier acción que sea necesaria.

Control de los cambios del proceso de gestión de riesgos

Los cambios del proceso de gestión de riesgos deberán identificarse y deberán mantenerse registros. Los cambios deberán revisarse, verificarse, validarse, según sea apropiado, y aprobarse antes de su implementación. La revisión de los cambios del proceso de gestión de riesgos deberán incluir la evaluación del efecto de los cambios en los resultados.

Deberán mantenerse registros de los resultados de la revisión de los cambios y de cualquier acción que sea necesaria.

Procesos de gestión de riesgos relacionados con terceras partes

Transferencia del riesgo

La organización deberá evaluar y seleccionar los proveedores que reciben y/o comparten los riesgos transferidos por la organización en función de su capacidad de cumplimiento. Deberán establecerse los criterios para la selección, la evaluación y la reevaluación de estos proveedores. Deberán mantenerse registros de los resultados de las evaluaciones y de cualquier acción que resulte necesaria y que se derive de éstas.

Evaluación, análisis y mejora del SGR implementado

La organización deberá planificar e implementar los procesos de seguimiento, evaluación, análisis y mejora que sean necesarios para demostrar la eficacia de los procesos implementados del sistema de gestión de riesgos, mejorar continuamente la eficacia del sistema de gestión de riesgos, determinar los métodos aplicables, incluyendo, las técnicas estadísticas, y el alcance de su utilización.

Auditoría interna del SGR

La organización deberá llevar a cabo auditorías internas del SGR a intervalos planificados para determinar si los objetivos de control, los controles, los procesos de gestión de riesgos y los procedimientos establecidos:

Satisfacen los requisitos legales y reglamentarios y a las regulaciones específicas del sector que dan marco a la gestión de la organización;

Satisfacen los requisitos de la gestión de riesgos identificados;

Están eficazmente diseñados, implementados y mantenidos;

Se deberá planificar un programa de auditorías, teniendo en consideración el estado y la importancia de los procesos y las áreas a auditar, así como los resultados de las auditorías previas. Se deberán definir previamente los criterios de cada auditoría, su alcance, la frecuencia y el método de verificación de controles a ser utilizado. La selección de auditores y la realización de auditorías deberán asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propia tarea.

Se deberá definir un procedimiento documentado para establecer las responsabilidades, los requisitos para la planificación y realización de auditorías, informar sobre sus resultados y mantener registros de la actividad realizada.

La dirección responsable del área que está siendo auditada deberá asegurarse de que se tomen las acciones que se definan necesarias en la auditoría, sin demora injustificada para eliminar las no conformidades detectadas y sus causas. Las actividades de seguimiento deberán incluir la verificación de las acciones tomadas y el informe de los resultados de la verificación.

Se recomienda utilizar la metodología establecida en la Norma IRAM-ISO 19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental" para realizar auditorías internas del SGR.

Seguimiento y evaluación del proceso de gestión de riesgos

La organización deberá aplicar métodos apropiados para el seguimiento, y cuando sea aplicable, la evaluación de los procesos del sistema de gestión de riesgos implementados. Estos métodos deberán demostrar la capacidad de los procesos para alcanzar los resultados planificados. Cuando no se alcancen los resultados previstos

deberán llevarse a cabo las correcciones necesarias y realizar las acciones correctivas, según sea conveniente, para asegurarse el cumplimiento de los objetivos de la gestión de riesgos correspondientes.

Seguimiento y evaluación de los resultados de los procesos de gestión de riesgos:

La organización deberá evaluar y hacer un seguimiento los resultados de los procesos de gestión de riesgos para verificar que se cumplen los requisitos del mismo. Esto deberá realizarse en las etapas apropiadas de los procesos de gestión de riesgos de acuerdo con las disposiciones planificadas y el estado de los indicadores que hayan sido determinados.

Deberá mantenerse evidencia de la conformidad con los criterios y requisitos de la gestión de riesgos. Los registros deben indicar la(s) persona(s) responsable de dicha verificación.

Gestión de las no-conformidades de sistema y de los incidentes a la seguridad (episodios adversos)

La organización deberá asegurarse de que las no-conformidades del sistema de gestión de riesgos implementado, los incidentes a la seguridad y los episodios adversos como pérdidas, daños y perjuicios, se identifican, analizan y se realizan las acciones necesarias para mitigar o limitar sus consecuencias sobre la gestión de la organización. Los controles, las responsabilidades y las autoridades relacionadas con el tratamiento de dichos episodios deberán estar definidos en un procedimiento documentado.

La organización deberá tratar las no-conformidades del sistema, los incidentes y episodios adversos mediante una o más de las siguientes maneras

Tomando acciones para cancelar o mitigar las consecuencias

Tomando acciones para impedir repetición de los mismos (acción correctiva)

Retroalimentar la información en el correspondiente proceso de gestión de riesgos determinando oportunidades de mejora.

Se deben mantener registros de la naturaleza de las no-conformidades del sistema, incidentes, episodios adversos y de cualquier acción tomada posteriormente.

Análisis de Datos:

La organización deberá determinar, recopilar y analizar los datos apropiados para demostrar la idoneidad y la eficacia del sistema de gestión de riesgos y para evaluar dónde puede implementarse acciones de mejora continua de la eficacia del sistema de gestión de riesgos. Esto deberá incluir los datos generados del resultado del control, seguimiento, evaluación y de cualquier otra fuente pertinente.

El análisis de datos deberá proporcionar información sobre:

La conformidad con los requisitos y procedimientos del sistema de gestión de riesgos,

Las características y tendencias del sistema y sus resultados, incluyendo las oportunidades para llevar a cabo acciones preventivas, y

La gestión de los proveedores que reciben y/o comparten los riesgos transferidos por la organización.

Mejora continua del SGR:

La organización deberá mejorar continuamente la eficacia del SGR mediante el uso y continua actualización de la política de gestión de riesgos, los objetivos establecidos para SGR, los resultados de las auditorías internas y externas, el análisis de datos, las acciones correctivas determinadas y las acciones preventivas establecidas así como la realización de las decisiones establecidas en **la última reunión de revisión por la dirección.**

Acciones correctivas

La organización deberá tomar acciones correctivas para eliminar las causas de las no conformidades que se presenten en el SGR, que hayan surgido de incidentes, episodios adversos, pérdidas, daños y perjuicios o en su defecto introducir medidas de control de los riesgos adicionales con objeto de prevenir que vuelvan a ocurrir. Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades del sistema

implementado y en operación, a corregir los incidentes, episodios adversos, pérdidas, daños y perjuicios encontrados durante la operación del SGR.

Se debe establecer un procedimiento documentado para definir los requisitos para:

Revisar las no conformidades del SGR, los incidentes a la seguridad , los episodios adversos, las pérdidas y los daños y perjuicios;

Determinar sus causas;

Evaluar la necesidad de adoptar acciones para asegurarse de que no vuelvan a ocurrir;

Determinar e implementar las acciones correctivas necesarias;

Registrar los resultados de las acciones tomadas; y

Revisar las acciones correctivas tomadas para determinar su eficacia.

Acciones preventivas

La organización deberá determinar acciones para eliminar las causas de no conformidades del SGR, incidentes, episodios adversos, pérdidas, daños y perjuicios potenciales que pudieran ocurrir, para prevenir su ocurrencia o ante su imposibilidad, mitigar sus consecuencias. Las acciones preventivas deberán ser apropiadas a los efectos de los problemas potenciales.

Se deberá establecer un procedimiento documentado para definir los requisitos para:

Determinar las no conformidades del SGR, que surjan de incidentes, episodios adversos, pérdidas, daños y perjuicios potenciales y sus causas;

Evaluar la necesidad de actuar para prevenir su ocurrencia;

Determinar e implementar las acciones necesarias;

Registrar los resultados de las acciones tomadas; y

Revisar las acciones preventivas tomadas.

Se debe determinar la prioridad en las acciones preventivas sobre la base de los resultados de la valoración de los riesgos potenciales.

Conclusión:

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Los sistemas planteados dan una respuesta completa a los problemas de implementar la gestión de la seguridad en las empresas incluyendo gestión de planes de contingencia y de gestión de riesgos.

Tomando como input lo establecido en la norma ISO 27001, que incluye el capítulo de gestión de riesgos y el control de implementar los planes de contingencia, lo definido como requisito en la norma IRAM 17550, requisitos de un sistema de gestión de riesgos y considerando la complejidad que deriva de establecer el sistema mediante constancias documentales tal como piden las normas, transformando el concepto de documento en gestión de procesos a través del soporte que brindan los sistemas Web.

ANEXO IV

GLOSARIO DE TÉRMINOS

ANEXO IV

GLOSARIO DE TÉRMINOS

ACCESO: es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal, desde donde pueden ser vistos, modificados o eliminados.

ACTIVE X: es un lenguaje de programación apoyado en controles OLE, Visual Basic y librerías del entorno Windows (OCX) de Microsoft. Active X permite que interactúen aplicaciones Windows con el World Wide Web (Internet).

ADSL: (Asymmetric Digital Suscribe Line - Línea de Usuario Digital Asimétrica). Usa la infraestructura telefónica actual para proveer servicios de transmisión de datos en alta velocidad.

AMENAZA: cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal o equipo informático, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: fallas de suministro eléctrico, virus, sabotadores o usuarios descuidados.

ANTIVIRUS: son todos aquellos programas que permiten analizar memoria, archivos y unidades de disco en busca de virus. Una vez que el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.

ARCHIVO DE PROCESO POR LOTES (.BAT o BATCH): los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se va ejecutando de forma secuencial.

ARCHIVO, DOCUMENTO: estos términos tienen el mismo significado y hacen referencia a la información que se encuentra en un soporte de almacenamiento informático.

Es el trabajo real que realiza cada usuario (textos, imágenes, bases de datos, hojas de cálculo, etc.). Cada uno de ellos se caracteriza por tener un nombre identificador. El nombre puede estar seguido de un punto y una extensión, compuesta por tres caracteres que identifican el tipo de fichero del que se trata. Algunas extensiones

comunes son: EXE y COM (ficheros ejecutables, programas), TXT y DOC (ficheros de texto), etc.

ATAQUE: término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

ATAQUE ACTIVO: acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

ATAQUE PASIVO: intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la interceptación de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

AUDITORÍA: llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

AUTENTICIDAD: capacidad de determinar si una lista de personas han establecido su reconocimiento y/o compromiso sobre el contenido del documento electrónico.

BASES DE DATOS: Es un conjunto de datos interrelacionados y un conjunto de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

BACKUP: Resguardo de la información

BIOS: es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. La BIOS es un programa que se no se encuentra en la memoria RAM (Random Access Memory – memoria de acceso aleatorio) pues al apagar el ordenador se borraría, sino en la memoria principal o ROM (Read Only Memory - Memoria de Sólo Lectura), cuyo almacenamiento es permanente.

CARPETA: se trata de divisiones (no físicas sino lógicas) en cualquier tipo de disco donde son almacenados determinados ficheros. Forman parte de una manera de organizar la información del disco, guardando los documentos como si de una carpeta clasificadora se tratase.

CHAT: se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo

CONFIDENCIALIDAD: capacidad de mantener datos inaccesibles a todos, excepto a una lista determinada de personas.

COOKIE: procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación. En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

CPD: centro de procesamiento de datos, centro de cómputos.

CRIPTOGRAFÍA: (encriptación) es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

DATOS: los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

DEPARTAMENTO DE CÓMPUTO: es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos

Computacionales de la institución. Es la entidad encargada de desarrollar el plan estratégico que favorezca la prestación de servicios eficientes, eficaces y de utilidad en la transmisión de datos para apoyar efectivamente los requerimientos del usuario. Es la entidad encargada de ofrecer sistemas de información administrativa integral

permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias del centro.

DOMINIO: conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado un servidor de dominios.

DOS: estas siglas significan Disk Operating System (DOS). Se refieren al sistema operativo (SO) anterior a Windows que, en su momento, creó la empresa Microsoft.

EQUIPO DE CÓMPUTO: dispositivo con la capacidad de aceptar y procesar Información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

EQUIPO DE TELECOMUNICACIONES: todo dispositivo capaz de transmitir y/o Recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

FILTRO DE PAQUETES: programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

FINGER: programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectados a un sistema remoto. Habitualmente se muestra el nombre y apellido, hora de la última conexión, tiempo de conexión sin actividad y terminal. Puede también mostrar archivos de planificación y de proyecto del usuario.

FIREWALL: es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewall pueden estar implementados en hardware o software, o una combinación de ambos. Los firewall son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

FIRMA DIGITAL: valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente

con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

FTP: (File Transfer Protocol) protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

GUSANO: es programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.

HACKER: persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

OFF SITE: fuera de sitio

HOST: (sistema central) computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

Hot Sites: cuando se refiere a Hot Sites son centros de procesamiento totalmente equipados que pueden estar en funcionamiento en pocas horas.

HTML: lenguaje de marcado de hipertexto, (Hyper-Text Markup Language) es el lenguaje con que se escriben los documentos en el World Wide Web (Internet).

HTTP: Protocolo de Transferencia de Hipertextos (Hyper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

HUB: Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples puertos. Cuando un paquete llega al puerto, es copiado a los otros puertos, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes puertos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al puerto correcto.

IDENTIFICACIÓN: un subtipo de autenticación, verifica que el emisor de un mensaje sea realmente quien dice ser.

INCIDENTE: cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

INFECCIÓN: es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro ordenador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

INTEGRIDAD: se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

INTRANET: una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

IP ADDRESS: (Dirección IP) dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

ISP: (Internet Service Provider – Proveedor de servicios de Internet) Empresa que presta servicios de conexión a Internet.

LOCAL AREA NETWORK: (LAN) (Red de Área Local) red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

MACRO / VIRUS DE MACRO: una macro es una secuencia de operaciones o Instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los ficheros creados con este tipo de aplicaciones

se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas.

MAN: Metropolitan Area Network. Red de Área Metropolitana.

MENSAJE DE DATOS: la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama o el telefax.

MIRRORING: duplicación de la información en línea, es decir, en el momento que se realiza una transacción, se duplica.

NAT: (Network Address Translation) las direcciones NAT son utilizadas comúnmente cuando se requiere conectividad de una LAN a Internet pero solo se tiene acceso a una sola dirección IP de Internet.

NAVEGADOR: (browser): término aplicado normalmente a programas usados para conectarse al servicio WWW.

POP: (Protocolo de Oficina de Correos - Post Office Protocol) programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita información de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

PRIVACIDAD: se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundidas o transmitida a otros.

PROGRAMAS (FICHEROS .EXE y .COM): los ficheros, documentos o archivos se componen de un nombre (cuyo número de caracteres antiguamente se limitaba a 8) y una extensión que puede no existir o contener, hasta tres caracteres como máximo. Esta extensión especifica el tipo de fichero. Si es EXE o COM, el fichero será un programa ejecutable. De esta forma si hacemos doble clic sobre él o escribimos su nombre, se realizarán determinadas acciones.

PROTOCOLO: descripción formal de formatos de mensaje y de reglas que dos Computadores deben seguir para intercambiar dichos mensajes.

PROXY: una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

REDIRECCIONAR: esta acción permite aplicar un nuevo destino. En el caso de los virus, se puede hablar de éste término cuando un virus es capaz (por ejemplo) de hacer que el sistema en lugar de acceder a una dirección en la que debería encontrar determinados componentes, es obligado por el virus a saltar o acceder a otra dirección diferente.

ROUTER: (direccionador) dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento.

SATAN: (Security Analysis Tool for Auditing Networks). Herramienta de Análisis de Seguridad para la Auditoria de Redes. Conjunto de programas para la detección de problemas relacionados con la seguridad.

SCRIPT: archivos con su extensión SCR que sirven para determinar los parámetros ("condiciones") con los que se deben ejecutar unos determinados programas. Permiten iniciar un programa con unas pautas fijadas de antemano.

SEGURIDAD: se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

SENDMAIL: aplicación de administración de correo electrónico propia del sistema operativo Linux.

SHTTP: (secure HTTP - HTTP seguro). Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

SISTEMA OPERATIVO (S.O.): existen dos términos muy utilizados en informática.

Estos son los conceptos de hardware y software. El primero de ellos se refiere a todo lo que es físico y tangible en el ordenador, como unidades de disco, tarjetas gráficas, microprocesador, memoria, etc. Por otro lado está el software que se define como el conjunto de programas (o información) con la que puede trabajar el hardware (ficheros, directorios, programas ejecutables, bases de datos, controladores, etc.). El sistema operativo pertenece al software y más concretamente es el conjunto de programas (y ficheros o archivos de otro tipo) que permite que se pueda utilizar el hardware. Se puede tener el mejor ordenador del mundo (el mejor hardware), pero si éste no tiene instalado un sistema operativo, no funcionará (ni siquiera se podrá encender). Algunos ejemplos de sistemas operativos son: MS/DOS, UNIX, OS/2, Windows 95/98/2000/NT, etc.

SMTP: (Simple Mail Transfer Protocol - Protocolo de Transferencia Simple de correo). Es el protocolo usado para transportar el correo a través de Internet.

SPAM: Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

SSL: (Secure Sockets Layer - Capa de Socket Segura). Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

TCP: (Transmission Control Protocol - Protocolo de control de Transmisión). Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TELNET: Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto.

TEXTO PLANO: (Plain Text) se llama así al documento antes de ser encriptado.

TROJAN HORSE: (Caballo de Troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

URL: (Localizador Uniforme de recursos - Uniform Resource Locator). Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El URL esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.ar) más el directorio y el archivo referido.

WAN: Wide Area Network. Red de Área Extensa.

WARN SITES: son centros de Procesamientos que tienen una estructura parcial.

COLD SITES: son centros que tienen una estructura básica, pero para que funcionen hay que montar todo el centro de procesamiento.

WEBMIN: es una aplicación con interfaz gráfica para la administración de sistemas Unix.

WWW: World Wide Web. Estrictamente la Web es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a browsers generalmente gráficos como Netscape o Internet Explorer.

TÉRMINOS Y DEFINICIONES DE LA GESTIÓN DE RIESGOS

Se aplican los siguientes términos y definiciones definidos en el capítulo 3 de la norma ISO 27001 (NOTA IRAM. La numeración entre paréntesis es la obrante en la ISO/IEC 27001:2005)

3.1 (3.10)

Aceptación del riesgo

Decisión de asumir un riesgo.

[Guía ISO/IEC 73:2002]

3.2 (3.1)

Activo

Cualquier cosa que tiene valor para la organización.

[ISO/IEC 13335-1:2004]

3.3 (3.11)

Análisis de riesgo

uso sistemático de la información para identificar las fuentes y estimar el riesgo.

[Guía ISO/IEC 73:2002]

3.4 (3.3)

Confidencialidad

La propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[ISO/IEC 13335-1:2004]

3.5 (3.16)

Declaración de aplicabilidad

Declaración documentada que describe los objetivos de control y los controles pertinentes y

aplicables al SGSI de la organización.

NOTA. Los objetivos de control y los controles se basan en los resultados y conclusiones de los procesos de evaluación de riesgos y tratamiento de riesgos, requerimientos legales o reglamentarios, obligaciones contractuales y los requerimientos del negocio de la organización en cuanto a la seguridad de la información.

3.6 (3.2)

Disponibilidad

Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.

[ISO/IEC 13335-1:2004]

3.7 (3.12)

Evaluación del riesgo

Proceso global de análisis de riesgo y valoración del riesgo.

[Guía ISO/IEC 73:2002]

3.8 (3.5)

Evento de seguridad de la información

Presencia identificada de una condición de un sistema, servicio o red, que indica una posible

violación de la política de seguridad de la información o la falla de las salvaguardas, o una

situación desconocida previamente que puede ser pertinente a la seguridad.

[ISO/IEC TR 18044:2004]

3.9 (3.14)

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

[Guía ISO/IEC 73:2002]

3.10 (3.6)

Incidente de seguridad de la información.

Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y

Amenazar la seguridad de la información.

[ISO/IEC TR 18044:2004]

3.11 (3.8)

Integridad

Propiedad de salvaguardar la exactitud y estado completo de los activos.

[ISO/IEC 13335-1:2004]

3.12 (3.9)

Riesgo residual

Nivel restante de riesgo después del tratamiento del riesgo.

[Guía ISO/IEC 73:2002]

3.13 (3.4)

Seguridad de la información

Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con

obligación de reportar (*accountability*), no repudio y fiabilidad.

[ISO/IEC 17799:2005]

3.14 (3.7)

Sistema de gestión de la seguridad de la información SGSI

Parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio,

cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar

la seguridad de la información.

NOTA. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, res -

ponsabilidades, prácticas, procedimientos, procesos y recursos.

3.15 (3.15)

Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo.

[Guía ISO/IEC 73:2002]

NOTA. En la presente norma el término "control" se usa como sinónimo de "medida".

3.16 (3.13)

Valoración del riesgo

Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la

importancia del riesgo.

[Guía ISO/IEC 73:2002]

Las siguientes definiciones proceden de la norma IRAM 17550 Tecnología de la información requisitos del sistema de gestión de riesgos.

A.1 consecuencia. Hecho o acontecimiento que sigue o resulta de otro o de un **evento** (A.4).

NOTA 1: Puede haber más de una consecuencia de un mismo evento.

NOTA 2: Las consecuencias pueden estar en el rango de positivas a negativas.

NOTA 3: Las consecuencias se pueden expresar cualitativa o cuantitativamente.

NOTA 4: Las consecuencias se determinan en relación con el logro de objetivos.

A.2 auto-evaluación de control – (C.S.A. – Control Self Assessment). Revisión periódica y sistemática de los procesos de negocio para asegurar que el **control del riesgo** (3.15) es aún eficaz y apropiado.

A.3 costo. Cualquier impacto negativo, ya sea directo o indirecto, incluyendo pérdidas de dinero, de tiempo o de mano de obra, por interrupciones de imagen organizacional, políticas e intangibles.

A.4 evento. Hecho imprevisto, o que puede suceder.

NOTA 1: El evento puede ser cierto o incierto.

NOTA 2: El evento puede ser una ocurrencia única o una serie de ocurrencias.

A.5 peligro. Amenaza o contingencia inminente de que suceda algún mal.

A.6 pérdida. Cantidad o cosa perdida. Cualquier **consecuencia** negativa (3.1), económica, financiera o de otro tipo.

A.7 Supervisar. Verificar, supervisar, observar críticamente o medir el progreso de una actividad, acción o sistema, en forma regular para identificar cambios respecto del nivel de desempeño requerido o esperado.

A.8 organización. Grupo de gente e instalaciones con un arreglo de responsabilidades, autoridades y relaciones.

NOTA 1: El arreglo es generalmente ordenado

NOTA 2: Una organización puede ser pública o privada.

NOTA 3: Esta definición es válida para los propósitos de las normas de sistemas de la gestión de calidad. El término *organización* es definido en forma diferente en la ISO/IEC Guide 2.

A.9 probabilidad. Intervalo dentro del cual es probable que ocurra un **evento** (A.4).

NOTA 1: La IRAM 34552-1 da la definición matemática de probabilidad como un número real dentro del intervalo 0 a 1 asociado a un suceso de azar. Éste puede ser relacionado con la frecuencia relativa de ocurrencia en el largo plazo o al grado de convicción de que ocurrirá un evento. Para un alto grado de credibilidad, la probabilidad es cercana a 1.

NOTA 2: Se puede utilizar *frecuencia* más que *probabilidad* en la descripción de un **riesgo**.

NOTA 3: Los grados de credibilidad acerca de la probabilidad se pueden escoger como clases o ámbitos, tales como:

- raro / improbable / moderado / probable / casi certeza, o
- improbable / remoto / ocasional / probable / frecuente.

A.10 riesgo residual. El nivel de **riesgo** restante (3.11) luego del **tratamiento del riesgo** (3.26).

A.11 riesgo. Contingencia o proximidad de que suceda algo que tendrá un impacto en los objetivos. Se lo mide en términos de una combinación de la **probabilidad** (3.9) de un **evento** (A.4) y su **consecuencia** (3.1).

NOTA: Para aspectos relacionados con seguridad ver la ISO/IEC Guide 51.

A.12 análisis de riesgos. Uso sistemático de la información disponible para determinar cuán frecuentemente pueden ocurrir eventos determinados y la magnitud de las consecuencias, para establecer el nivel de riesgo.

A.13 proceso de evaluación de riesgos. Proceso general de identificación, análisis y evaluación del riesgo, (ver figura 1).

A.14 evitar un riesgo. Una decisión informada de no verse involucrado, o una acción de retiro de una situación de **riesgo**.

A.15 control de riesgos. La parte de la gestión de riesgos que involucra la provisión de políticas, normas y procedimientos para mitigar los **riesgos** adversos.

A.16 criterios de riesgo. Principios u otras reglas de decisión mediante las cuales se evalúa la importancia de los **riesgos** para determinar si se recomiendan acciones de **tratamiento para ellos**.

NOTA: Los criterios de riesgo pueden incluir costos y beneficios asociados, requerimientos legales y estatutarios, aspectos socioeconómicos y ambientales, las preocupaciones de los **interesados** (3.28), prioridades y otros aspectos de la evaluación.

A.17 evaluación de riesgos. Proceso de comparación del **riesgo** estimado contra **criterios de riesgo** dados para asistir en la decisión de tolerar o tratar un riesgo.

NOTA: Para la evaluación de riesgos en el contexto de seguridad, ver ISO/IEC Guide 51.

A.18 financiamiento de riesgos. Métodos aplicados para afrontar el tratamiento de riesgos (poner en vigencia estructuras e instrumentos) y las **consecuencias** económicas o financieras negativas.

A.19 identificación de riesgos. Proceso para determinar qué puede suceder, dónde, cuándo, por qué y cómo.

A.20 gestión de riesgos. Cultura, procesos y estructuras que están dirigidos hacia la gestión eficaz de oportunidades y efectos adversos potenciales.

A.21 proceso de gestión de riesgos. Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las tareas de, establecer el contexto, identificar, analizar, estimar, evaluar, tratar, supervisar y comunicar el **riesgo**.

A.22 sistema de gestión de riesgos. Conjunto de elementos del sistema de gestión de una **organización** concerniente a la gestión de **riesgos**.

NOTA 1: Los elementos del sistema de gestión pueden incluir planeamiento estratégico, toma de decisiones y otros procesos para tratar los riesgos.

NOTA 2: La cultura de una organización se ve reflejada en su sistema de gestión de riesgos.

A.23 reducción de riesgos. Aplicación selectiva de técnicas apropiadas y principios de gestión aplicados para disminuir la **probabilidad**, las **consecuencias** negativas, o ambas, asociadas a un **riesgo**.

A.24 aceptación ó retención de riesgos. Aceptación de la carga de la pérdida, o del beneficio a ganar, de un **riesgo** en particular.

NOTA 1: Retención del riesgo incluye la aceptación de riesgos que no han sido identificados.

NOTA 2: Retención del riesgo no incluye tratamientos que involucran seguros, o transferencia por otros medios.

NOTA 3: Puede haber variabilidad en el grado de aceptación y dependencia de los **criterios de riesgo**.

A.25 transferencia de riesgos. Cambiar la responsabilidad o compartir con otra parte la carga de la pérdida o el beneficio de la ganancia relacionada a un **riesgo**.

NOTA 1: Requerimientos legales o estatutarios pueden limitar, prohibir u obligar a la transferencia de algunos riesgos.

NOTA 2: La transferencia de riesgos puede llevarse a cabo mediante seguros u otros acuerdos.

NOTA 3: La transferencia de riesgos puede crear nuevos riesgos o modificar un riesgo existente.

A.26 tratamiento de riesgos. Proceso de selección e implementación de medidas para modificar el **riesgo**.

NOTA 1: El término *tratamiento del riesgo* es utilizado a veces para las medidas en sí mismas.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

NOTA 2: Las medidas de tratamiento de los riesgos pueden incluir evitar, modificar, transferir o retener el riesgo.

A.27 análisis de sensibilidad. Examinar cómo varían los resultados de un cálculo o modelo cuando se cambian las hipótesis o suposiciones individuales.

A.28 interesados. Personas y **organizaciones** que pueden afectar, ser afectados, o percibir ser afectados por la decisión o actividad.

NOTA: El término *interesados* ('stakeholders') puede también incluir *partes interesadas* tal como son definidas en IRAM/ISO 14050 e IRAM/ISO 14004.

ANEXO V

PLAN DE CONTINGENCIAS

ANEXO V

Plan de Contingencias

Un plan de contingencias es un conjunto de procedimientos alternativos a la operación normal, que le permitirá a su Organización seguir operando, aún cuando alguna de sus funciones deje de hacerlo por una falla.

Las causas pueden ser un problema informático de la Organización, la falla en la entrega de información o insumo básico por parte de terceros o la falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones y cualquier situación derivada de problemas climáticos o sociales.

La contingencia es en general atendida con alguna degradación en el nivel de servicio prestado y por un período limitado.

El hecho de que su Organización tenga un plan de contingencias no implica que se trabaje inadecuadamente. Por el contrario indica que su Organización es previsor y que está cubriendo las eventualidades tanto internas como externas, que puedan inhibir su normal operación con la consecuente pérdida que esto implica.

La preparación de un plan de contingencias, por ejemplo para la gestión de la informática y las comunicaciones, constituye una fuerte inversión, tanto de recursos humanos como de costos de servicios vinculados, sin embargo adecuada, ya que gran parte o la totalidad del mismo, así como la experiencia adquirida en su elaboración, serán aplicables a diversos escenarios de contingencias.

El objetivo principal de un plan de contingencias es la continuidad de operaciones de la Organización, no sólo de sus sistemas de información sino de todas las actividades humanas y de producción vinculadas.

La siguiente guía le orienta en las fases, actividades y tareas necesarias para elaborar un plan de contingencias.

Un plan de contingencias consiste en por lo menos las etapas de evaluación, planificación, pruebas, ejecución y recuperación. Las primeras tres etapas constituyen la fase de prevención y las dos últimas representan fase de reacción ante los eventos que afecten la operación.

Las etapas y actividades son las siguientes:

Evaluación

1. Constitución del grupo de desarrollo del plan de implementación:

Este grupo deberá estar formado por un líder a cargo del plan de contingencias, los responsables de las áreas afectadas, un representante de auditoría interna y el apoyo legal de la Organización. Esta última deberá intervenir para certificar que la adopción de las alternativas no colisione con los plazos convenidos y la calidad legalmente comprometida.

La decisión de desarrollar el plan deberá estar en el más alto nivel de dirección, ya que constituye un tema de continuidad de operaciones.

No deberá estar integrado por gente de informática exclusivamente. La designación de los miembros debiera ser avalada por la más alta dirección dado que deberán comprometerse recursos y aprobarse procesos especiales.

2. Identificación de las funciones críticas:

Identifique todas las funciones críticas y los sistemas y equipos automatizados de su Organización. Es importante detectar los equipos que contengan circuitos ocultos o embebidos y que afecten a funciones críticas y procesos de negocio críticos.

Si existe un inventario de activos de información (equipos, sistemas, base de datos, procedimientos, etc.,) utilícelo.

Evalúe las prioridades en el plan de contingencias.

3. Identificación de las interfases externas de los procesos críticos:

Identifique las relaciones con proveedores y clientes que intervengan en sus procesos críticos. Recuerde que sus objetivos pueden estar afectados fuertemente por la información o insumos externos a su Organización y viceversa.

4. Definición y documentación de los posibles escenarios de fallas, esto es las posibles fallas que pueden presentarse para cada función crítica, la caracterización de las fallas puede verse a continuación:

4.1 Internas: en este caso la falla está restringida a la empresa u Organización. Puede tratarse de problemas informáticos (hardware, software de base, de telecomunicaciones, software de aplicación propio o provisto por terceros) o equipos o sistemas automáticos dependientes de algoritmos o métodos como sistemas de acceso, circuitos de ascensores, sensores diversos, etc.).

También deberán incluirse en esta categoría los siniestros que podrían producir incendios, utilización indebida de medios magnéticos de resguardo o back up, o cualquier otro daño de origen físico que pudiera provocar la destrucción o pérdida masiva de información.

4.2 De interfases: se trata de problemas en la información recibida o enviada hacia otras empresas u Organismos. Considere que lo que es crítico para su organización. Incluya las interfases que pueden ser triviales para los proveedores de la información.

4.3 Infraestructura básica: se trata de problemas asociados con la carencia de fuentes de energía, de comunicaciones, abastecimiento de insumos, transporte, Internet, etc.

5. Análisis del impacto de la falla en cada función crítica:

Realice un análisis de impacto de cada falla, (ya sea interna, de interfases o de infraestructura básica) sobre cada una de las funciones críticas de la Organización, teniendo en cuenta las siguientes prioridades:

- Evitar pérdidas de vida.
- Satisfacer las necesidades básicas de ejecución de los procesos.
- Reanudar las operaciones lo antes posible.
- Proteger el medio ambiente.
- Lograr las conexiones con los principales clientes y proveedores.
- Mantener la confianza de terceros en su Organización.

Cuantifique, de ser posible, el impacto económico de cada falla; le servirá para la correcta selección de la solución alternativa.

6. Definición de los niveles mínimos de servicio:

Defina los mínimos niveles de servicio aceptables para cada falla. Es importante que dicho nivel sea aceptado por las áreas afectadas y cuente con el aval de auditoría interna y la intervención de su asesoría legal.

7. Identificación de las alternativas de solución (procesos de contingencia):

Identifique las soluciones alternativas para cada una de las fallas eventuales o previsibles. Para ello puede considerar:

- Implementar procesos manuales.
- Contratar las tareas de proceso críticas con terceros.

- Diferir la tarea crítica por un tiempo determinado.
- Otro que permita continuar las operaciones.

8. Evaluación de la relación costo/beneficio de cada alternativa:

De cada alternativa de proceso de contingencia, identificada en el punto anterior y sobre la base del impacto económico de cada falla, determine la mejor solución desde el punto de vista costo/beneficio para cada proceso crítico y su tiempo de elaboración con un nivel de servicio que satisfaga el mínimo nivel.

Elevar para su aprobación y obtener el compromiso de la máxima autoridad. Poner en conocimiento los pros y contras, ventajas y desventajas para cada alternativa.

5.2 Planificación

9. Documentación del plan de contingencias:

Es necesario documentar el plan, cuyo contenido mínimo será:

Nota: en algunos casos puede requerirse especificar estos contenidos para distintas funciones y tipos de fallas

- Objetivo del plan: definir el plan que permitirá continuar la operación de tareas críticas, por ejemplo: continuar las actividades en forma normal, continuar las actividades con un deterioro aceptable de la calidad y productividad o diferir las actividades por razones económicas o de seguridad.
- Modo de ejecución: indica si la solución alternativa es de tipo manual, semiautomática o automática.
- Tiempo máximo sin servicio: si es posible cuantificar, el tiempo que la Organización puede sobrevivir sin prestar ningún servicio.
- Tiempo máximo de duración de la contingencias: deberá estar claramente especificado el tiempo que la Organización admite trabajar según el nivel mínimo de servicio.
- Costos estimados: se refiere a los costos asociados a la solución alternativa.
- Recursos necesarios: para indicar qué tipo de recursos se necesitan para la solución alternativa: personal, formularios, máquinas, proveedor externo, grupo electrógeno, etc.
- Criterio disparador: cuál será el evento que comenzará la operatoria Alternativa contingente y quién es responsable de su activación.

- Autoridades: quiénes serán las autoridades a cargo de los distintos aspectos del plan.
- Roles y responsabilidades: definir qué hará cada persona afectada al plan y cuál es su responsabilidad.
- Capacitación del personal: según la tarea que cada persona cumpla en el plan deberá ser capacitada para esta nueva tarea. Si la solución es de tipo manual, hay que recordar que será necesario entrenar y capacitar.
- Retorno a la operación normal: deberá ser programada la entrada a la operación normal y, especialmente la recuperación de información dañada o corrupta.
- Comunicaciones: será necesario informar del servicio que se prestará tanto al personal de la Organización como al público usuario.

Es importante consignar aquí que se deben contemplar las interfases con otras Organizaciones que reciben información de la nuestra o que envían datos. Como ya se mencionó anteriormente lo que es trivial para una Organización puede ser muy importante para la otra.

10. Validar el plan de contingencias:

Es necesario validar el plan de contingencias con las áreas involucradas y también dar intervención a auditoría interna para asegurar que los procedimientos alternativos adoptados tienen la seguridad que corresponde. Asimismo, como en general la solución es degradada con respecto a la velocidad de respuesta, será necesario que personal de la asesoría legal verifique si la Organización puede tener problemas legales por su implementación.

5.3 Pruebas

11. Definir y documentar las pruebas del plan:

Es necesario definir las pruebas del plan y el personal y recursos necesarios para su realización. Una correcta documentación ayudará a la hora de realizar las pruebas.

12. Obtener los recursos necesarios para las pruebas:

Deben obtenerse los recursos para las pruebas, ya sean recursos físicos o mano de obra para realizarlas.

13. Capacitar al personal que intervendrá en las pruebas:

Será necesario en esta actividad capacitar a todos los participantes en las pruebas. Serán de utilidad los seminarios y talleres que se puedan implementar.

14. Ejecutar las pruebas y documentarlas:

Realice las pruebas o simulacros. Mientras mayores sean los ensayos de su plan, aumentará la certidumbre de que las tareas fundamentales de su Organización sobrevivan a las contingencias que se susciten.

La capacitación del equipo de contingencias y su participación en pruebas son fundamentales para poner en evidencia posibles fallas del plan.

Es necesario documentar las pruebas para su aprobación por parte de las áreas afectadas.

15. Ejecutar y documentar las pruebas de reiniciación del proceso normal:

La reiniciación del proceso normal no sólo deberá ser ensayado, sino también documentado.

Coordine las pruebas, en su caso, con el equipo encargado de los distintos proyectos en curso en la organización.

Deben establecerse los procedimientos para recuperar los datos desactualizados o que puedan haber quedado dañados.

16. Actualizar el plan de contingencias de acuerdo a los resultados obtenidos en las pruebas:

Será necesario realimentar el plan de acuerdo a los resultados obtenidos en las pruebas.

Tenga en cuenta que el plan de contingencias general o de continuidad de operaciones de la empresa contiene los planes de contingencias específicos para cada falla definida. Los distintos planes deben integrarse en un todo, considerando las posibles relaciones mutuas.

17. Designar el equipo ejecutor del plan, incluyendo el grupo de Recuperación de la información. El equipo ejecutor debería ser el de pruebas, ampliado. Definir autoridades y responsabilidades. Capacitar al equipo ejecutor.

5.4 Ejecución

18. Notificar a los involucrados la ocurrencia del evento disparador.

19. Ejecutar el plan de contingencias:

Recuerde que el plan no busca resolver la causa de la falla, sino asegurar la continuidad de las tareas críticas de la Organización a pesar de la falla en los medios normales de operación.

Tenga presente que la contingencias es un trabajo de equipo, en una situación de emergencia y por un tiempo corto.

Asegúrese de que haya una buena comunicación con sus empleados, sus proveedores y sus clientes.

5.5 Recuperación

20. Recuperar los datos:

Los datos de sus archivos o bases de datos pueden haber quedado desactualizados o corruptos. Deben corregirse usando los procedimientos ya definidos.

21. Iniciar el proceso normal en paralelo con el proceso alternativo:

En general la reiniciación del proceso normal no implica la cancelación del alternativo, salvo que deban utilizarse los mismos recursos. Si esto no es así, durante cierto tiempo, los procesos deberían ejecutarse en paralelo para asegurar que la reiniciación de la operación normal es correcta y, ante cualquier defecto, continuar con el de contingencias.

22. Notificar la reiniciación de la operación normal:

Su Organización deberá ser notificada de que la operación normal ha sido reiniciada.

23. Finalizar las operaciones de contingencias:

Una vez asegurados de que la operación normal se está ejecutando normalmente con sus datos correctos, se finalizarán las tareas de contingencias.

Elaborar un informe final sobre los resultados del plan de contingencias y actualizarlo de ser necesario.

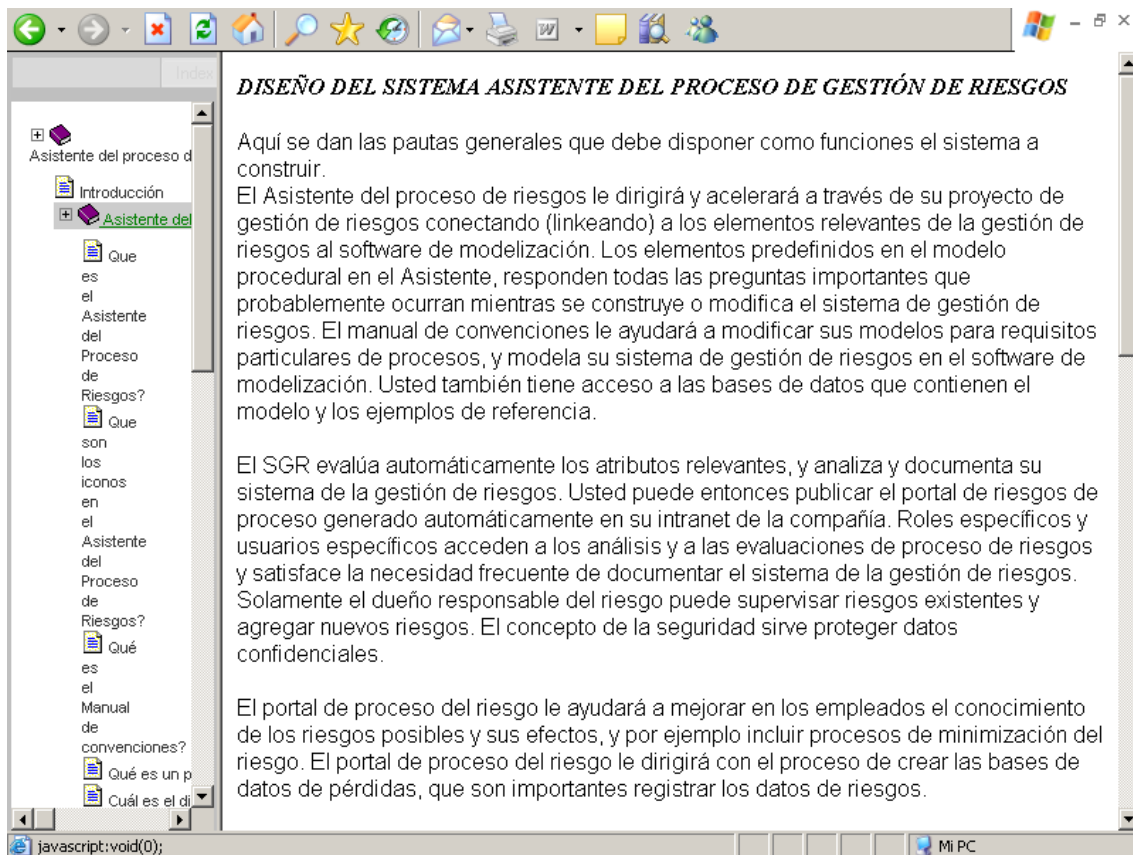
ANEXO VI

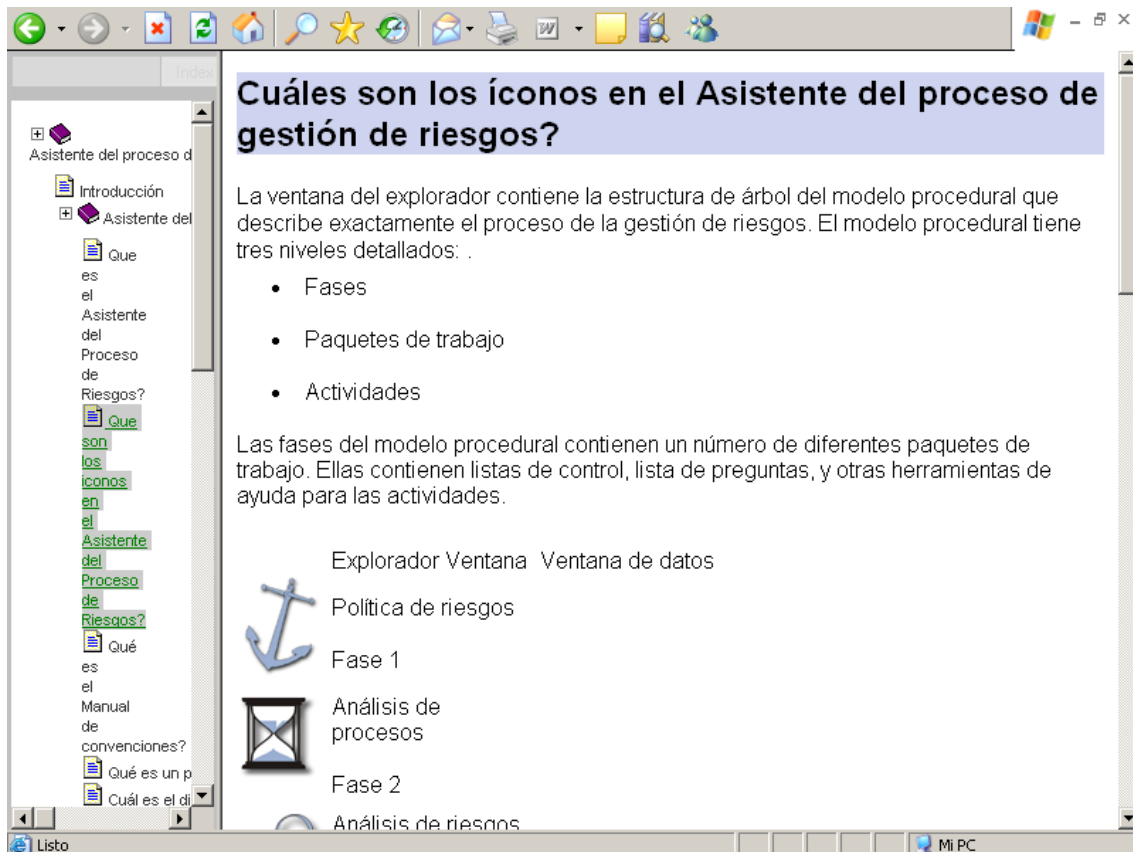
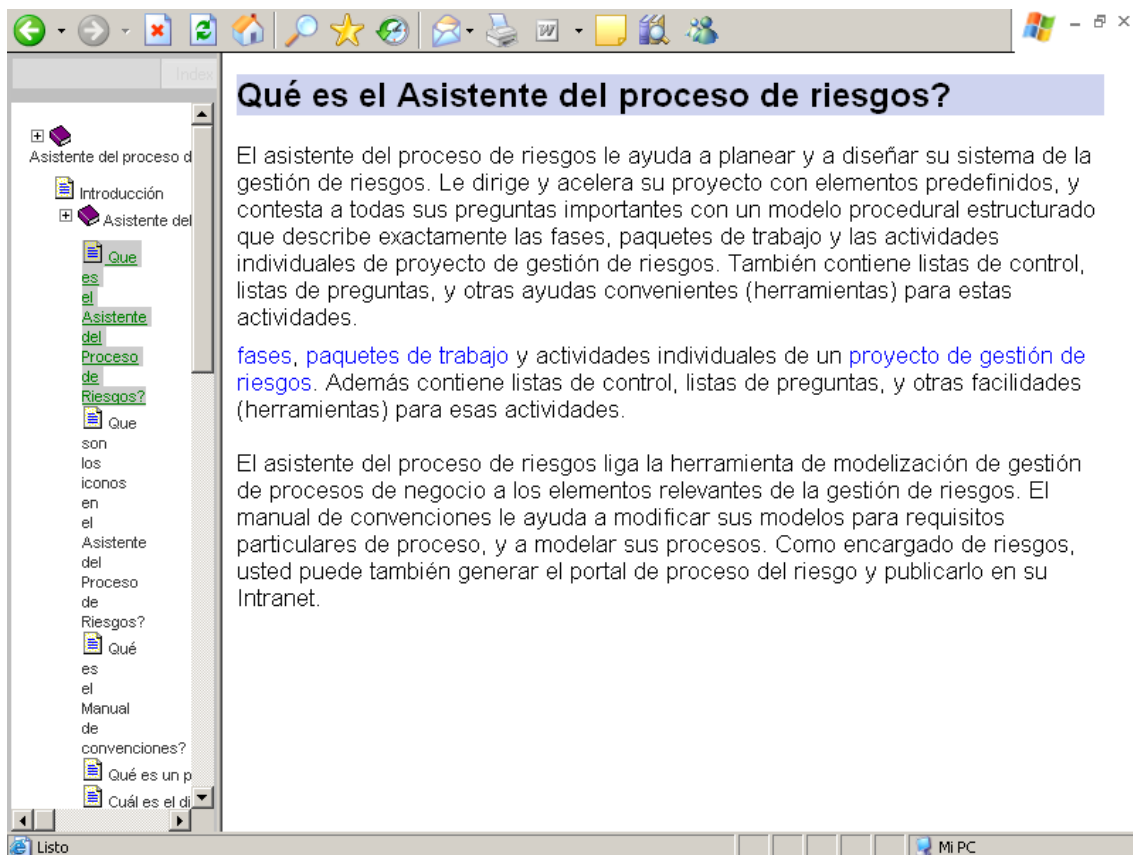
NAVEGADOR DEL PORTAL DE RIESGOS

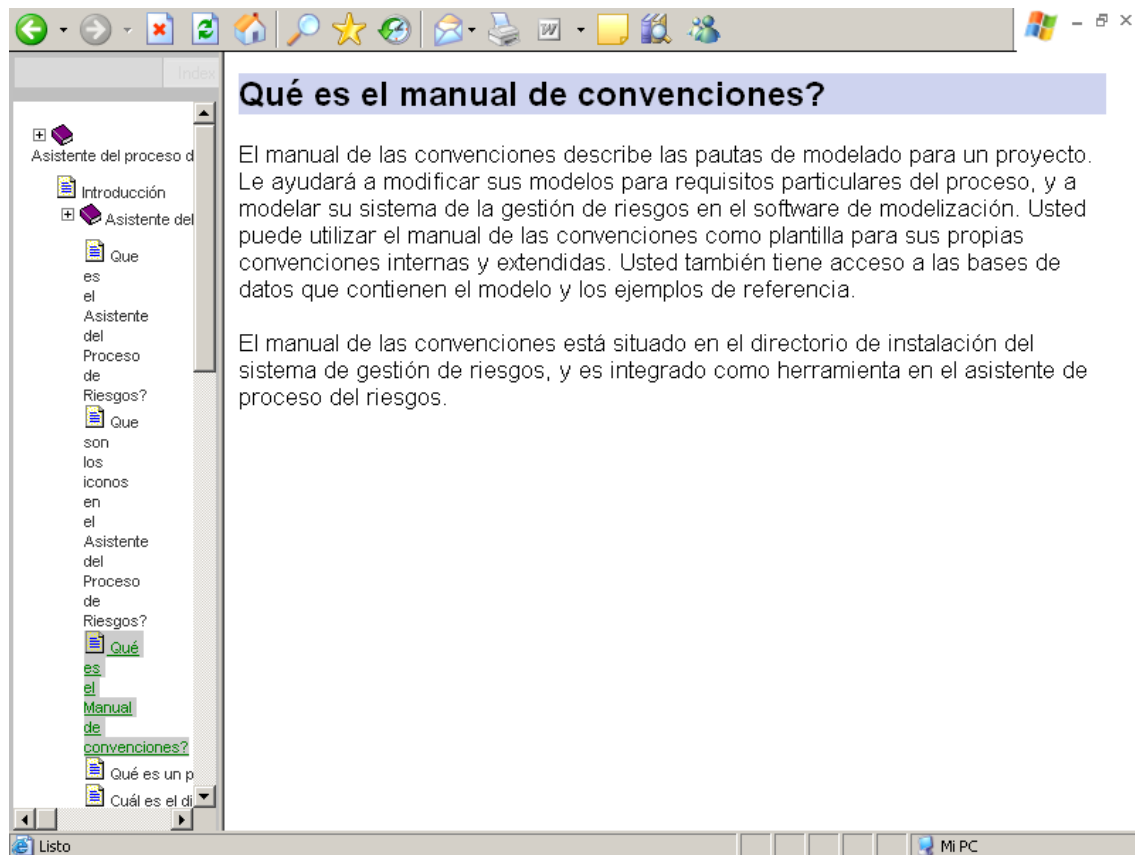
Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

ANEXO VI - NAVEGADOR PORTAL DE PROCESOS DE RIESGOS

PORTAL DE PROCESO DE RIESGOS







¿Qué es un proceso de gestión de riesgos?

Clique en un objeto para más información sobre ese objeto.

¿Qué es un proceso de gestión de riesgos?
Clique en un objeto para más información sobre ese objeto.

The diagram illustrates a risk management process cycle with the following components:

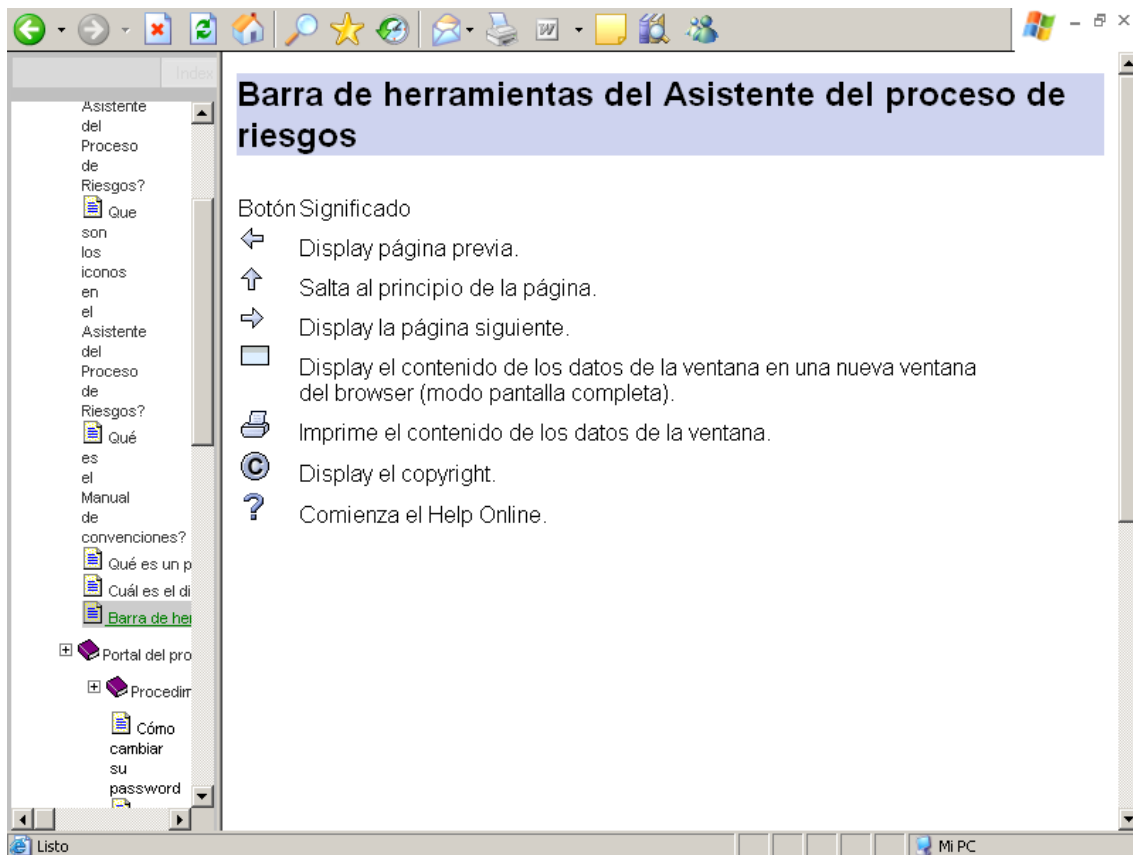
- risk policy
- process analysis
- Software de modelización
- risk analysis
- target definition
- Asistente de Proceso de gestión de riesgos
- risk reporting
- Sistema de performance de procesos
- risk control

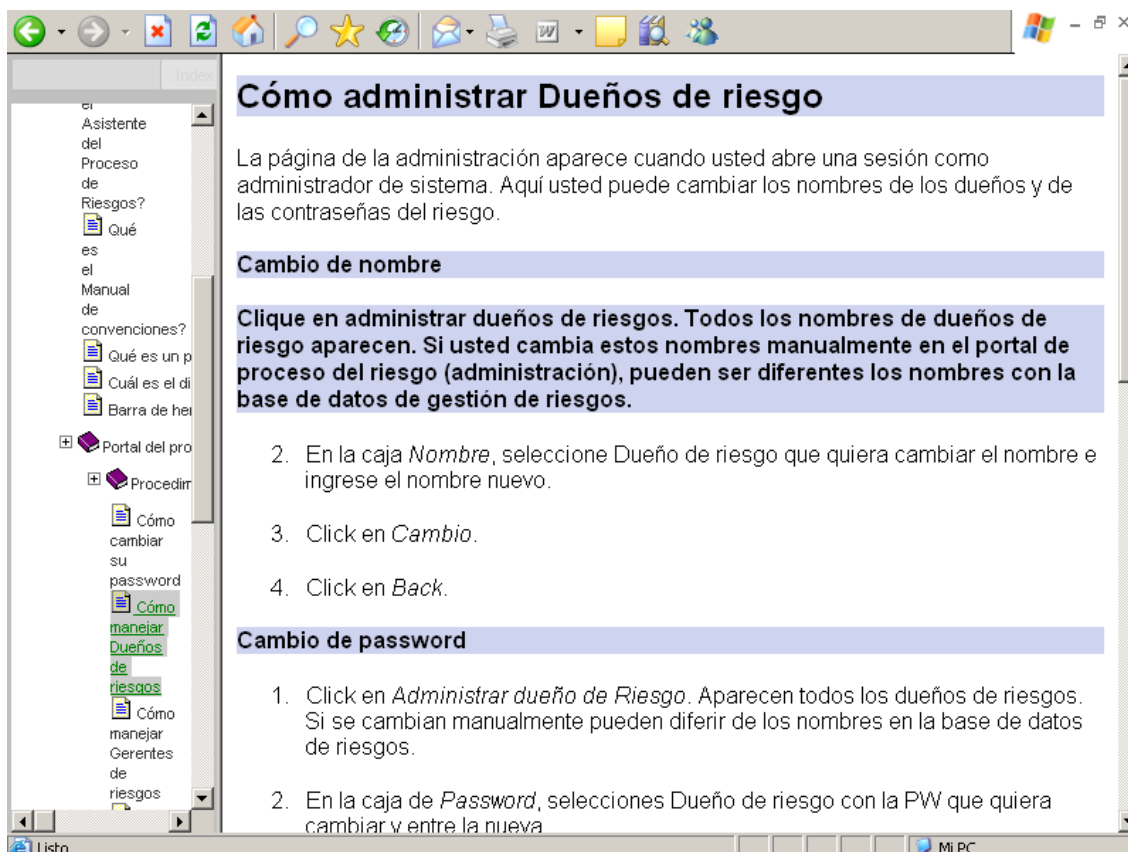
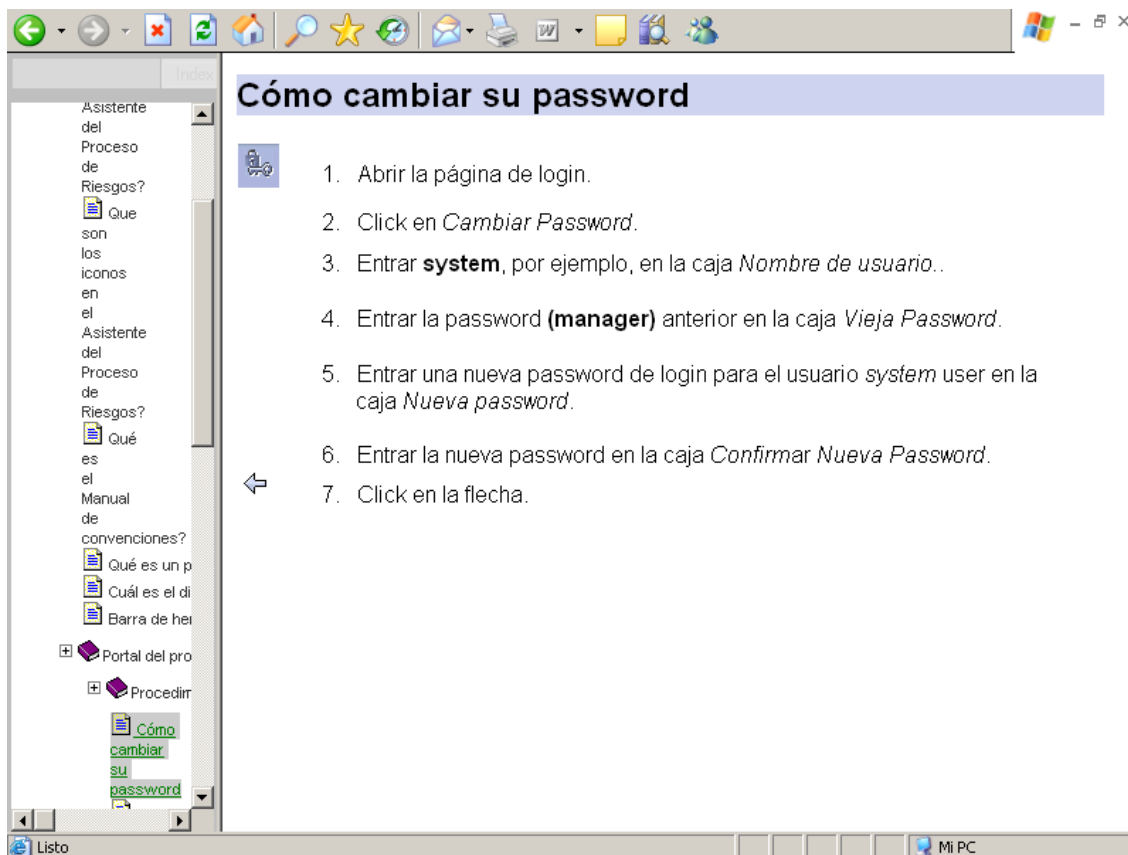
¿Cuáles son las arquitecturas de sistema y concepto de seguridad?

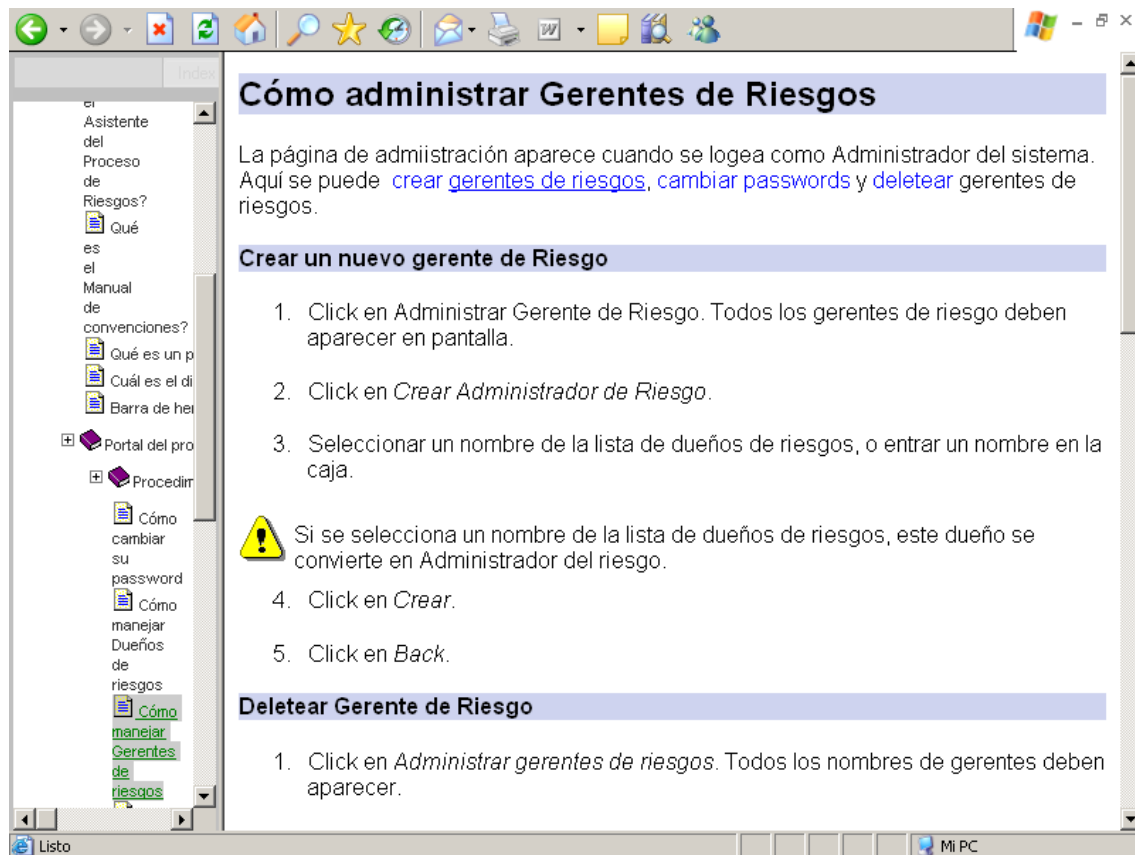
The diagram illustrates the system architecture for the Risk Management Portal:

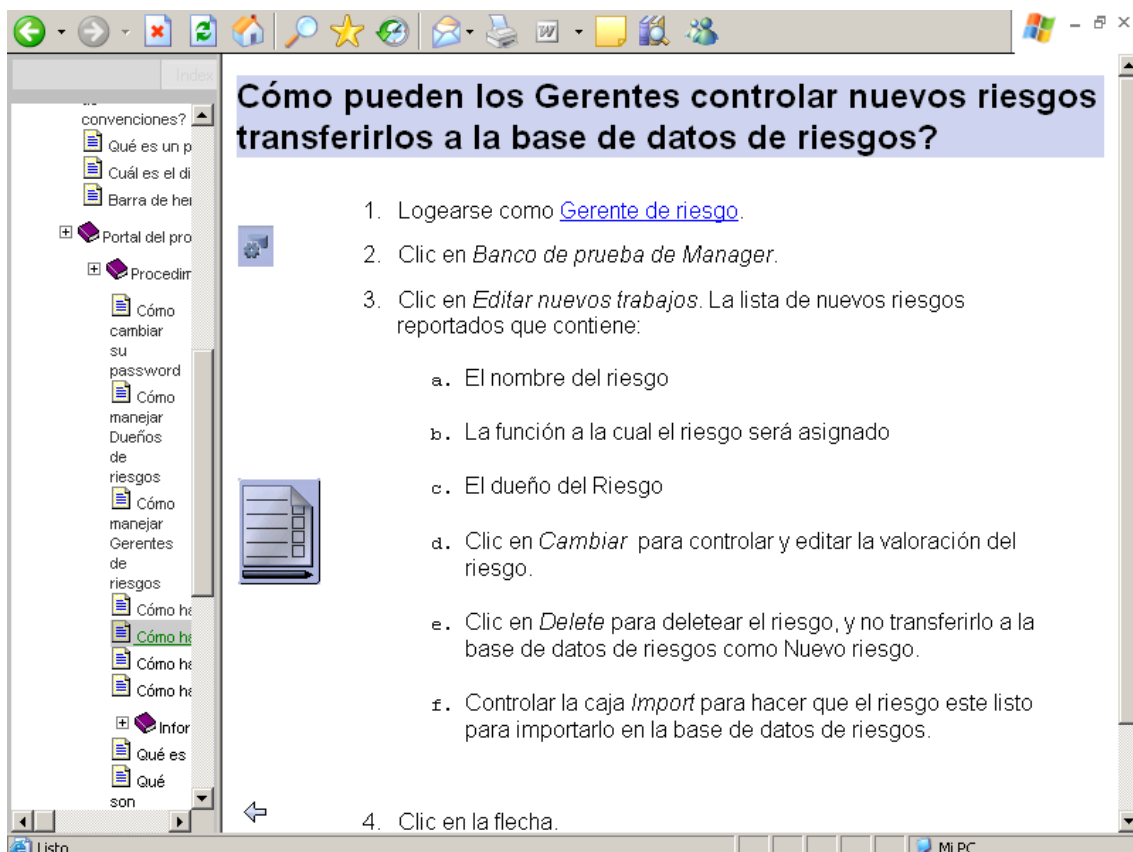
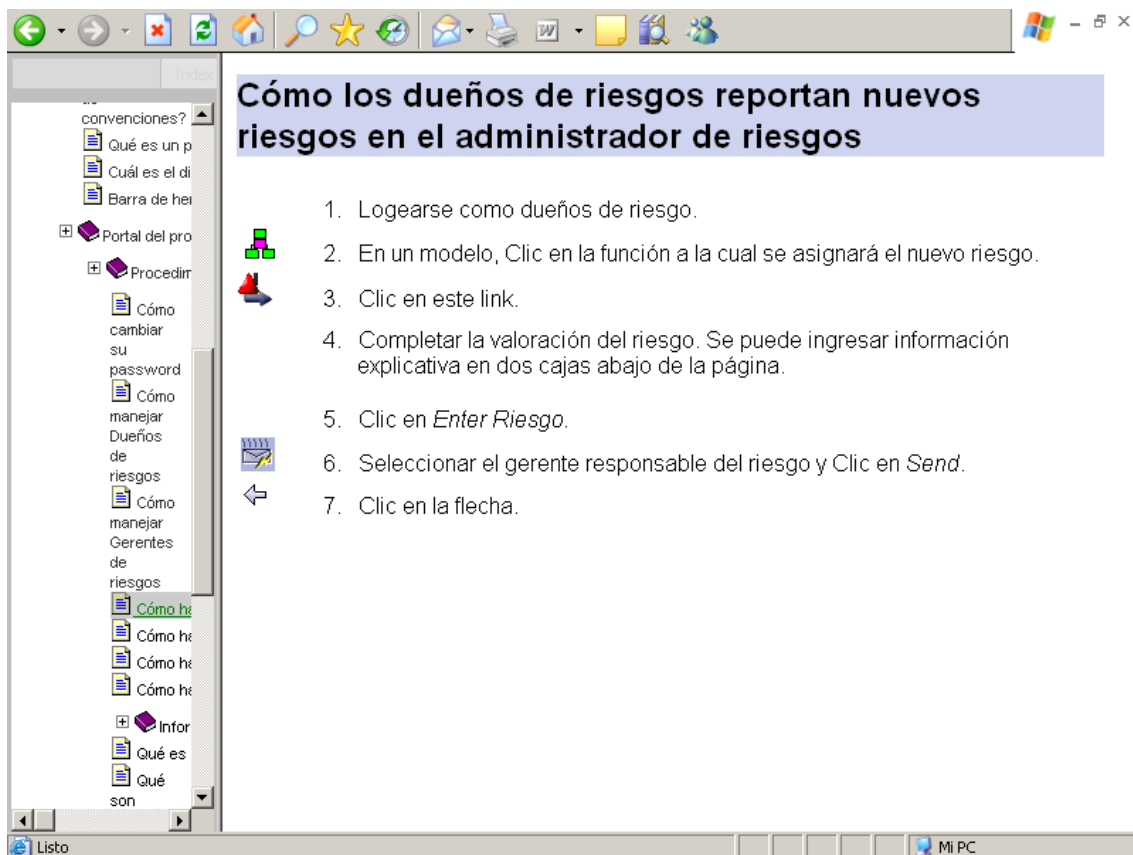
- Client Side:** PHP WEB, Banco de Pruebas de riesgos, Administrador De dueños de riesgos, Portal de proceso de riesgos.
- Server Side:** PHP Engine, Web Server, DB Server.
- Database Layer:** Base de Modelización (GUID), Base de datos De pérdidas de procesos, Tabla de pérdidas, Tabla de Eventos de riesgos.
- Interactions:** PHP connects to Base de Modelización and Base de datos De pérdidas de procesos. ARIS Format connects to Base de Modelización. SQL connects to Base de Modelización and Base de datos De pérdidas de procesos.

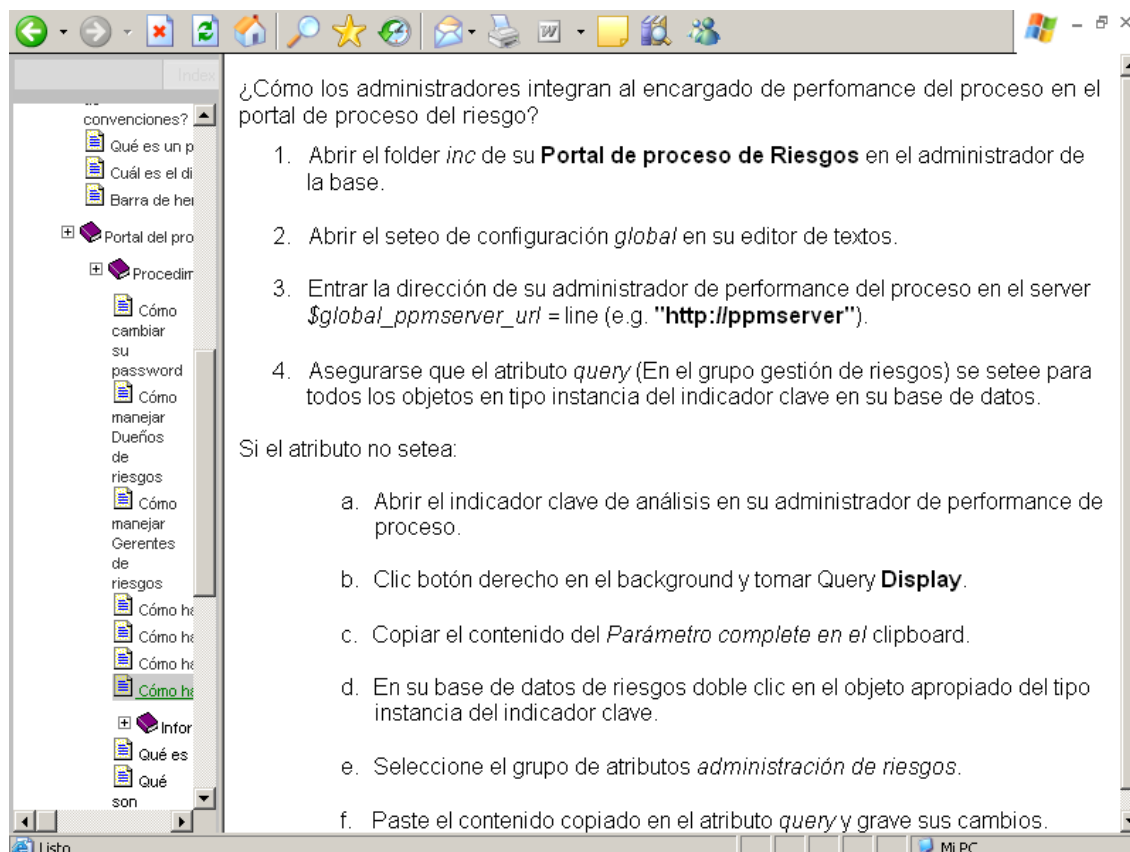
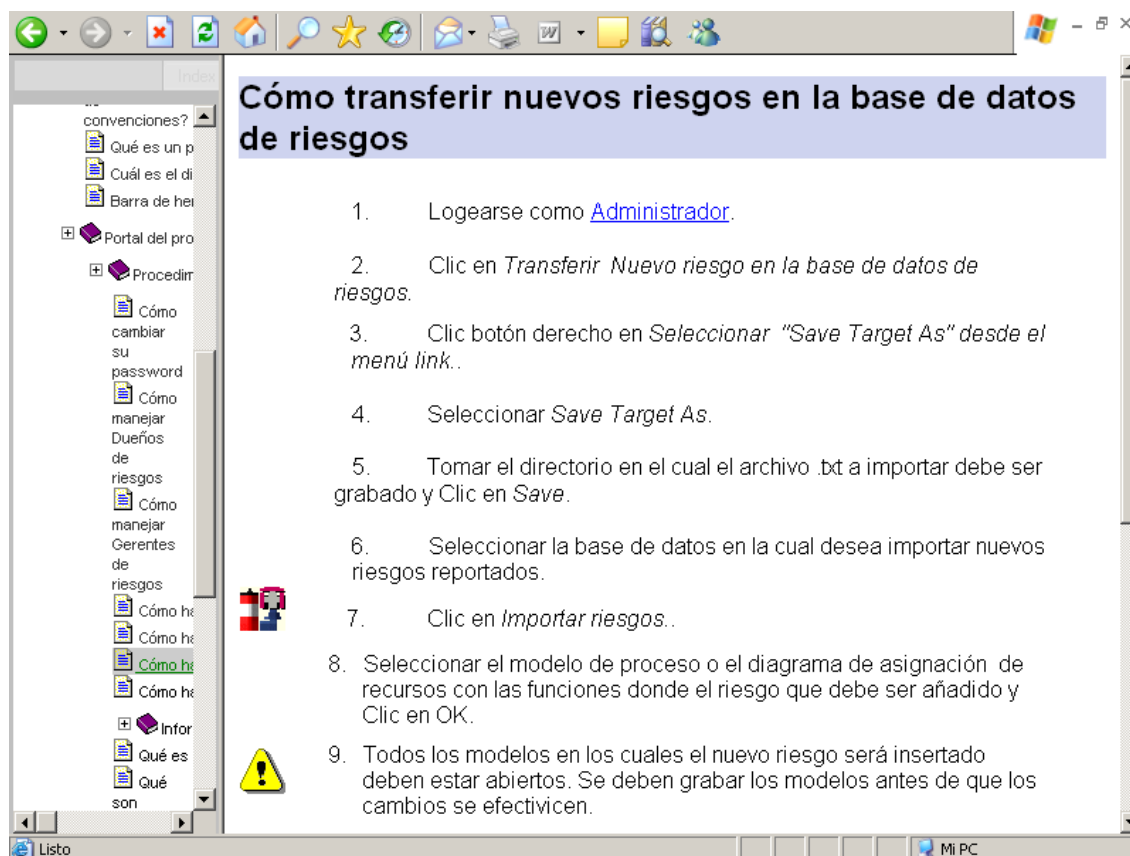
La arquitectura del portal del Proceso de Riesgos se basa en las páginas web dinámicas. Estas son generadas por roles y usuarios específicos utilizando un motor PHP. Sólo ciertos tipos de páginas son dinámicamente protegidas por mecanismos de acceso. Este escenario de arquitectura requiere el uso de un servidor web a partir de PHP que

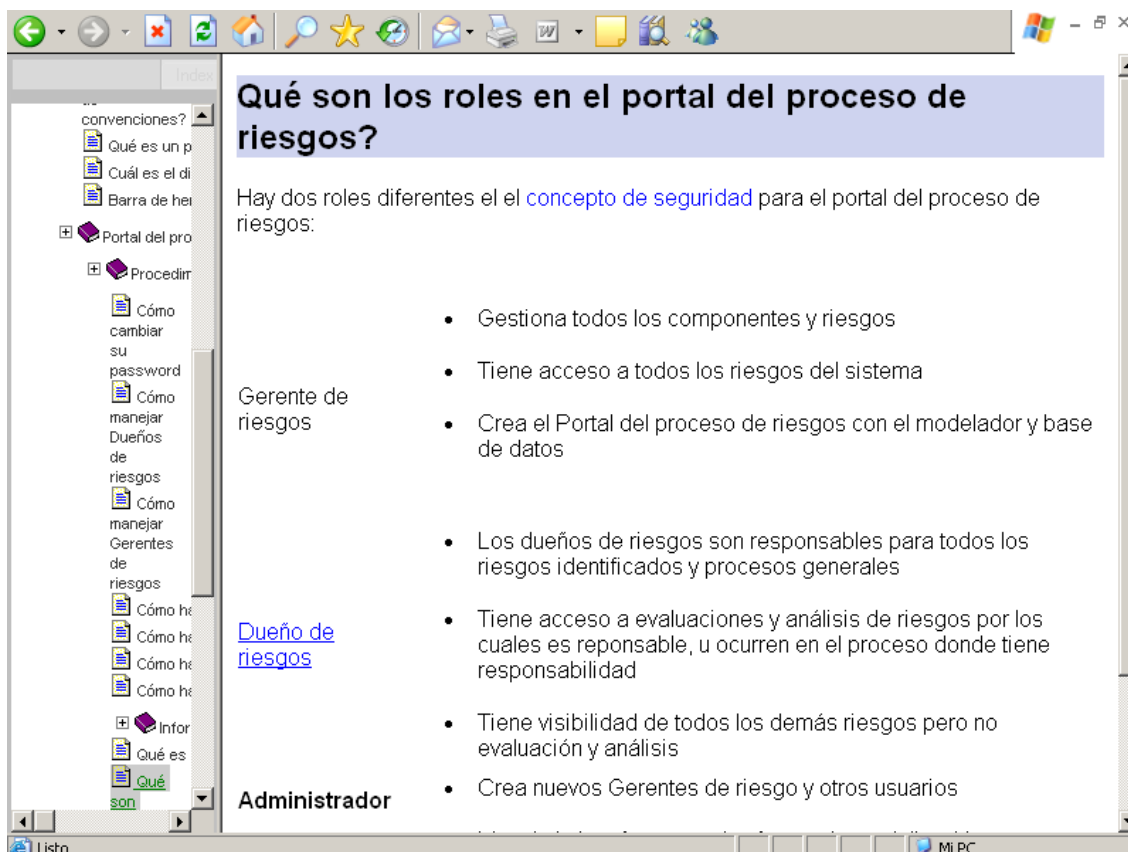
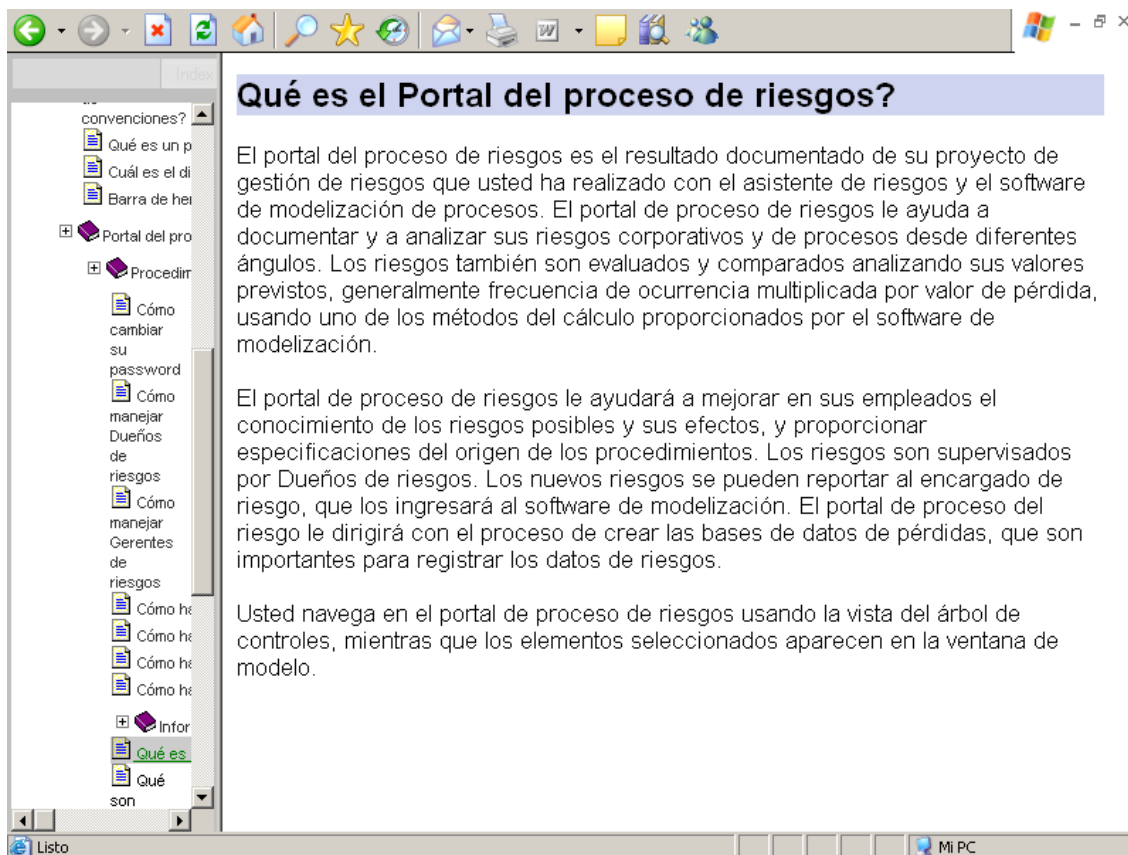


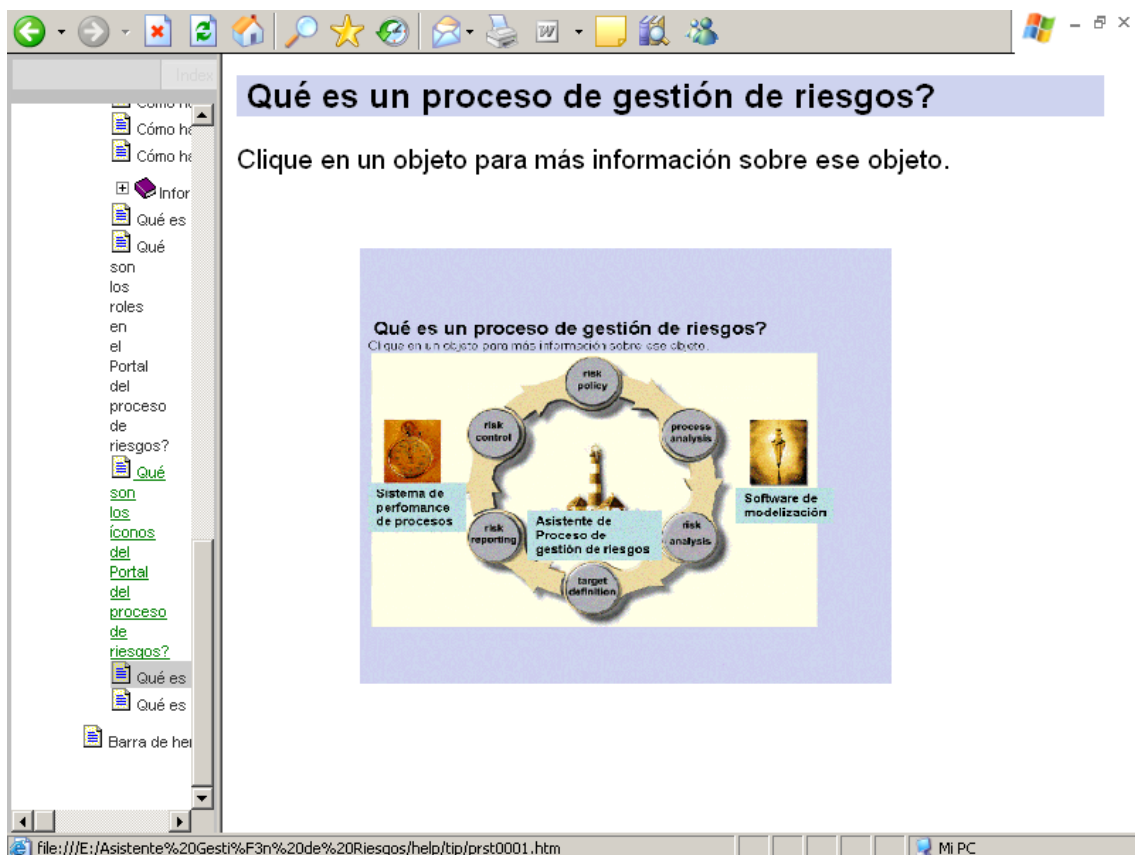
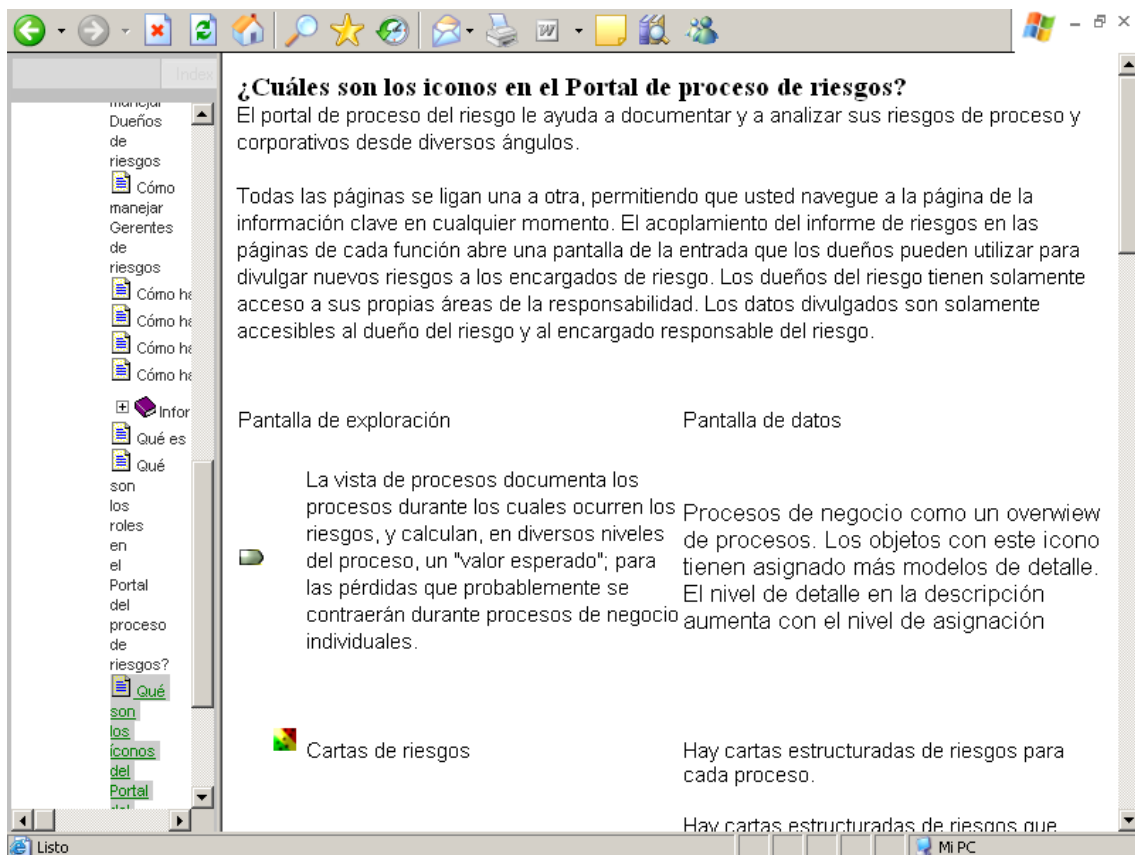












¿Cuáles son las arquitecturas de sistema y concepto de seguridad?

La arquitectura del portal del Proceso de Riesgos se basa en las páginas web dinámicas. Estas son generadas por roles y usuarios específicos utilizando un motor PHP. Sólo ciertos tipos de páginas son dinámicamente protegidas por mecanismos de acceso. Este escenario de arquitectura requiere el uso de un servidor web a partir de PHP que

Barra de herramientas del Portal del proceso de riesgos

Botón Significado

La página de la administración se abre cuando usted abre una sesión como administrador de sistema. Aquí usted puede

- [Gestionar Gerentes de Riesgo](#)
- [Gestionar Dueños de Riesgo](#)
- Actualizar datos de usuarios
- [Transferir nuevos riesgos a la base de datos de riesgos](#)

Una vez que usted ha abierto una sesión como Gerente de riesgo, sus nuevos y viejos trabajos aparecen en el banco de trabajo del gerente de riesgo. Usted verá:

- todos los nuevos riesgos que arriesgan a dueños han divulgado del portal de proceso del riesgo
- todos los riesgos que usted ya ha procesado

Abrir el diálogo de conexión. Usted puede abrir una sesión con un diferente nombre de usuario. El usuario anterior se logonea.

← Exhíbe la página anterior.

↑ Saltos a la tapa de la página.

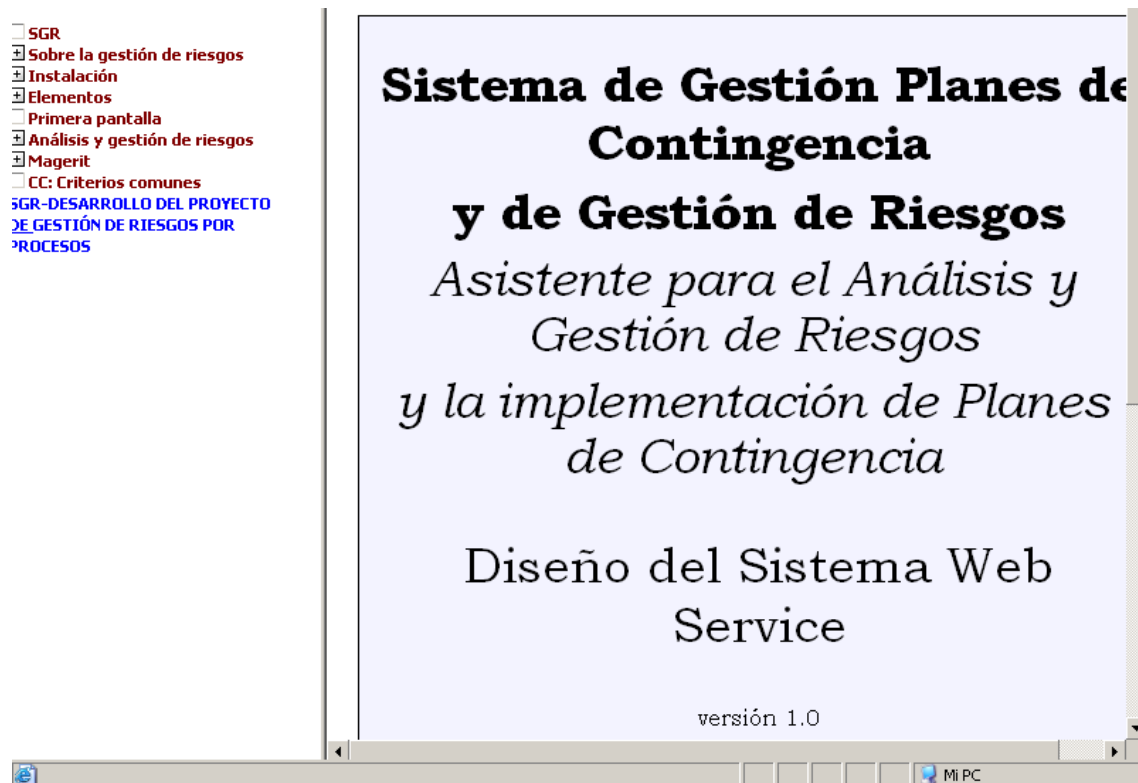
Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

ANEXO VII

**SE PRESENTA LA ESTRUCTURA DE PANTALLAS DE NAVEGACIÓN
DE LA APLICACIÓN DISEÑADA.**

ANEXO VII SE PRESENTA LA ESTRUCTURA DE PANTALLAS DE NAVEGACIÓN DE LA APLICACIÓN DISEÑADA.



Sobre la gestión de riesgos

Para conocer el estado de seguridad de un sistema de información, es necesario modelarlo, identificando y valorando sus activos, e identificando las amenazas sobre dichos activos, determinando los riesgos que representan dichas amenazas y valorando los mismos. Así pues, podemos estimar el riesgo a que el sistema está sujeto.

El riesgo se puede mitigar o eliminar, por medio de las salvaguardas o contramedidas desplegadas para proteger el sistema. Es inusual que las salvaguardas reduzcan el riesgo a cero, es decir los eliminen; es más frecuente que siga existiendo un riesgo residual, luego de aplicar las salvaguardas establecidas, que la organización o bien lo pueda aceptar, o bien intente reducirlo aún más, estableciendo un plan de seguridad orientado a llevar el riesgo a niveles aceptables.

El análisis de riesgos proporciona información para las actividades de tratamiento de los riesgos. Estas actividades se ejercen una vez y otra vez, incorporando nuevos activos, nuevas amenazas, nuevas vulnerabilidades, y nuevas salvaguardas.

Es decir que un sistema de gestión de la seguridad de la información (SGSI), será cada vez más completo cuando se incluyan nuevos riesgos y nuevas salvaguardas.

El SGR es un conjunto de herramientas

- para realizar un análisis general, sobre las diversas dimensiones de seguridad (confidencialidad, integridad, disponibilidad,...)
- o un análisis de la continuidad, centrado en la disponibilidad del sistema, buscando reducir los tiempos de interrupción del servicio cuando sobrevienen desastres.

En cualquier caso, el análisis puede ser cualitativo o cuantitativo.

El SGR se implementa en base a la metodología Magerit y considerando las normas [ISO 27001 y 27002](#).

Vea:

Análisis cualitativo

El SGR permite realizar un análisis cualitativo, usando una serie de niveles de valores discretos para la valoración de los activos.

Un análisis cualitativo es recomendable siempre en primer lugar, antes de que se intente un análisis cuantitativo detallado. Un análisis cualitativo permite:

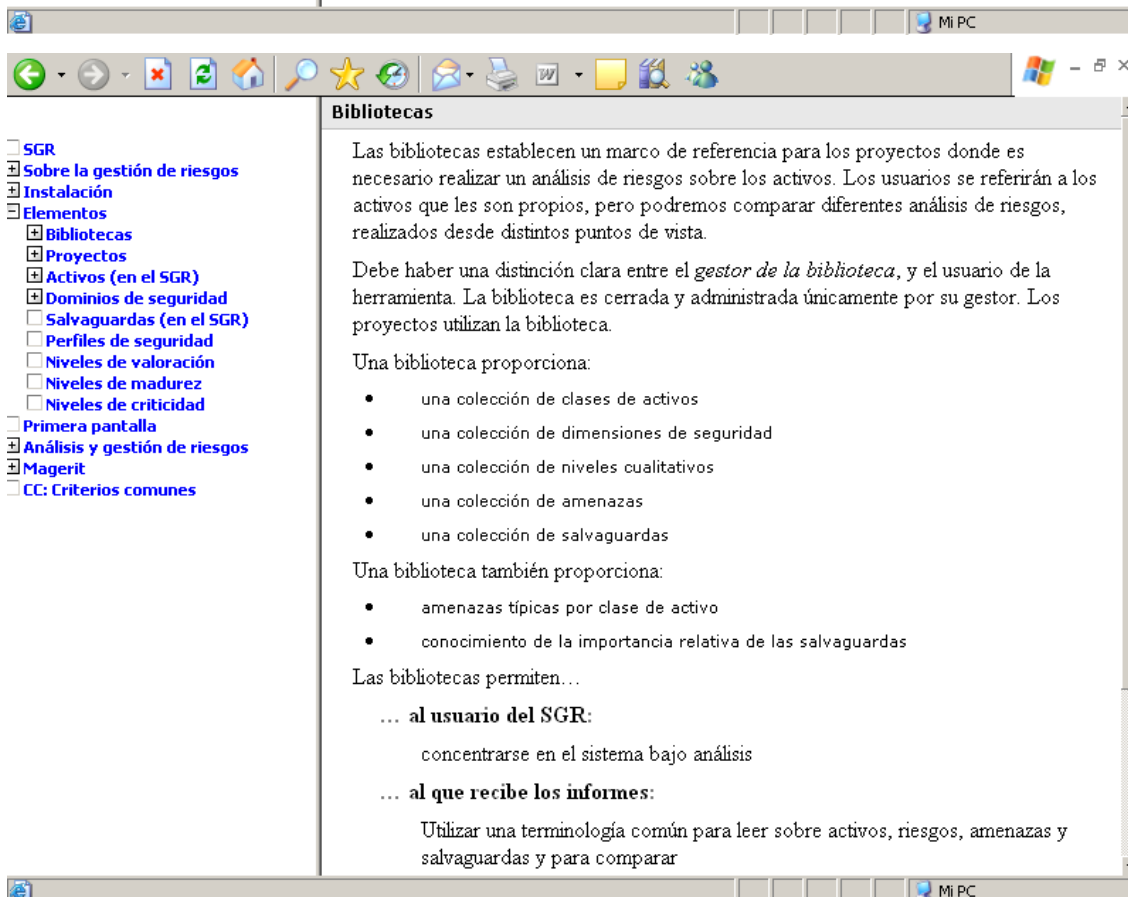
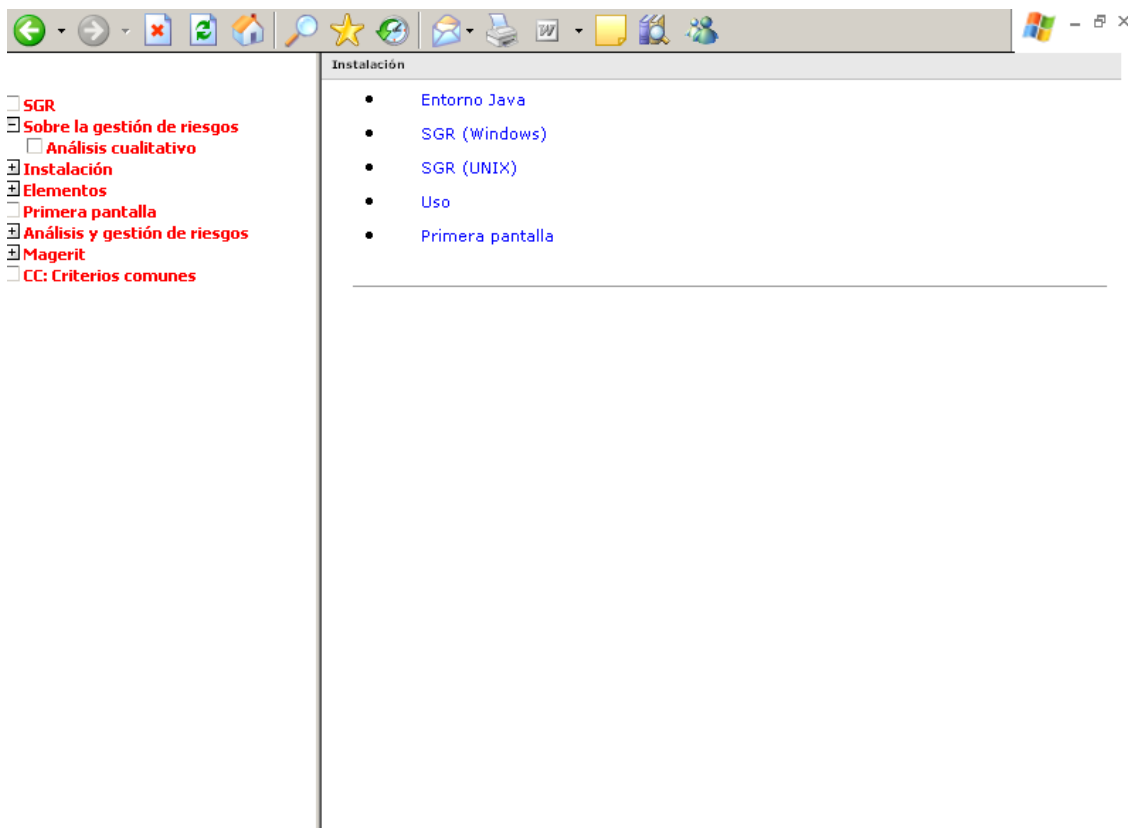
- identificar los activos más significativos
- identificar el valor relativo de los activos
- identificar las amenazas más relevantes
- identificar las salvaguardas presentes en el sistema
- establecer claramente los activos **críticos** (los que están sujetos a un riesgo máximo)

Un análisis cualitativo permite centrarse en esos aspectos que sean difíciles de cuantificar exactamente, o no sea fácil de explicar con medidas cuantitativas (es decir, para esas cosas que *“no tienen precio”* como por ejemplo *la imagen de la organización, el segmento de mercado de los productos, el nivel de conocimiento y experiencia del personal, etc.*). Además, proporciona un primer acercamiento a esas cosas que sí tienen un precio, pero no estamos interesados ni podemos indicar en este momento. Un análisis cuantitativo posterior entrará en más profundidad y detalle.

Ver [niveles de valoración](#).

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello



The image shows two screenshots of a web application interface. The top screenshot displays the 'Perfiles de seguridad (extensión de la biblioteca)' page. The left sidebar contains a navigation menu with items like 'SGR', 'Sobre la gestión de riesgos', 'Instalación', 'Elementos', 'Bibliotecas', 'Proyectos', 'Activos', 'Dominios de seguridad', 'Primera pantalla', 'Análisis y gestión de riesgos', 'Magerit', and 'CC: Criterios comunes'. The main content area explains that security profiles are sets of safeguards and lists typical profiles: ISO/IEC 27002, national laws on personal data protection, and other security concepts.

The bottom screenshot displays the 'Perfiles de amenazas' page. The sidebar is identical. The main content area defines threats and lists typical questions for the SGR system, such as '¿cuáles son las amenazas típicas sobre este activo?' and '¿cuál es la probabilidad típica?'. It also mentions the use of ISO/IEC 13335-4 for deducing typical threats.

Proyectos de gestión de riesgos

Los proyectos de gestión de riesgos se construyen mediante:

- una colección de activos, que son propios del sistema bajo análisis
- una colección de amenazas, a elegir de una biblioteca, y valoradas para el sistema bajo análisis
- una colección de salvaguardas, a elegir de una biblioteca, y valoradas para el sistema bajo análisis

Usando estos elementos, es posible estimar el impacto y el riesgo para el sistema bajo análisis.

El Reporte técnico [ISO / IEC 13335-2](#) Administración y planificación de la Seguridad de la información y en el Reporte técnico [ISO / IEC 13335-3](#) Técnicas para la administración de la seguridad de la información, brindan un panorama completo de conceptos, métodos y técnicas a implementar en un sistema de gestión de la seguridad de la información y por ende de aquéllos temas a incluir en el proyecto de gestión de contingencias y riesgos.

Para caracterizar un proyecto de gestión de riesgos:

- se necesitan determinar una serie de datos administrativos y de personal
- determinar las posibles fuentes de información
- restringir el análisis a un subconjunto de dimensiones, dentro de los previstos en la biblioteca
- restringir el análisis a un subconjunto de amenazas, dentro de las previstas en la biblioteca
- Para desarrollar en su organización un proyecto de gestión de riesgos orientado a procesos de negocio
- Utilice el siguiente link: [SGR-DESARROLLO DEL PROYECTO DE GESTIÓN DE RIESGOS POR](#)

Fases del proyecto

El tratamiento del riesgo se puede afrontar por etapas o fases.

El siguiente documento muestra las [fases de un proyecto de implementación de un SGSI](#) que incluye las fases del proyecto de gestión de riesgos

Estas fases son fotografías de la evolución del sistema de protección, mientras que se ponen en ejecución las nuevas salvaguardas, o se mejora su madurez, el SGR puede estimar el impacto y el riesgo residuales.

Las fases se utilizan para establecer objetivos de seguridad a medio y largo plazo.

Según surge de la norma IRAM 17551 – Sistemas de gestión de riesgos se muestra el cuadro adjunto:

Proceso de Gestión de Riesgos detallado

```
graph TD
    A[Yellow Bar] --> B[Establecer el Contexto  
• Contexto estratégico  
• Contexto organizacional  
• Contexto gestión de riesgos  
• Desarrollar criterios  
• Decidir la estructura]
    B --> C[Identificar los Riesgos  
¿Qué puede suceder?]
    C --> B
    C --> A
```

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Activos Disponibles

Los elementos básicos para el análisis de riesgos son los activos, sometidos a amenazas, y protegidos por salvaguadas. Sin embargo, es conveniente organizar los activos en una estructura decente para una mejor presentación que permita entender del sistema bajo análisis.

Vea [activos en Magerit](#).

Los activos se organizan en

- [capas](#),
- [grupos de activos](#) y
- activos propiamente dichos

Los activos pueden ser calificados indicando las [clases](#) que sean relevantes para describirlo.

La gestión de activos se detalla a continuación en el [Capítulo 7 de la norma IRAM – ISO / IEC 17799](#) (Actual ISO 27002)

Capas

Los activos se organizan siempre en capas, y se pueden agrupar opcionalmente en grupos. Puede establecerse la similitud con un sistema de ficheros: las capas son como discos, y los grupos son como carpetas, mientras los activos corresponden a ficheros.

Es habitual utilizar un patrón estándar de capas como el siguiente:

- capa de negocio
- equipamiento
 - servicios internos
 - aplicaciones (software)
 - equipos (hardware)
 - comunicaciones
 - elementos auxiliares
 - servicios subcontratados
- instalaciones
- personal

Una instalación de SGR puede tener su capa estándar fijada según lo descrito en el ejemplo siguiente:

capas activos dominios estadísticas

ACTIVOS

- [FS] Funciones del sistema de información
 - [S_T_presencial] Tramitación presencial
 - [S_T_remota] Tramitación remota
 - [D_exp] Expedientes en curso

por capas

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Grupos de activos

Los activos dentro de una capa se pueden organizar en grupos.

Los grupos trabajan como carpetas que contienen activos.

La clasificación facilita la presentación a las partes afectadas relevantes (durante actividades de la comunicación de riesgos), pero no tiene ningún impacto en el análisis.

A continuación se muestra un ejemplo de lo planteado:

capas activos dominios estadísticas

ACTIVOS

- [FS] Funciones del sistema de información
 - [S_T_presencial] Tramitación presencial
 - [S_T_remota] Tramitación remota
 - [D_exp] Expedientes en curso
- [SI] Servicios internos
 - [email] Mensajería electrónica
 - [archivo] Archivo histórico central
- [E] Equipamiento
 - [sw] [SW_exp] Tramitación de expedientes
 - [hw] [PC] Puestos de trabajo
 - [SRV] Servidor
 - [network] [firewall] Cortafuegos
 - [LAN] Red local
 - [ADSL] Conexión a Internet
- [L] Instalaciones
 - [oficinas] Oficinas
 - [cpd] Sala de equipos

activo: [network.ADSL] Conexión a Internet - sin licencia

Clases de activos

Los activos se pueden clasificar como pertenecientes a una o más clases.

Las clases disponibles de activos están fijadas en la biblioteca de la organización.

Las clases de los activos proporcionan:

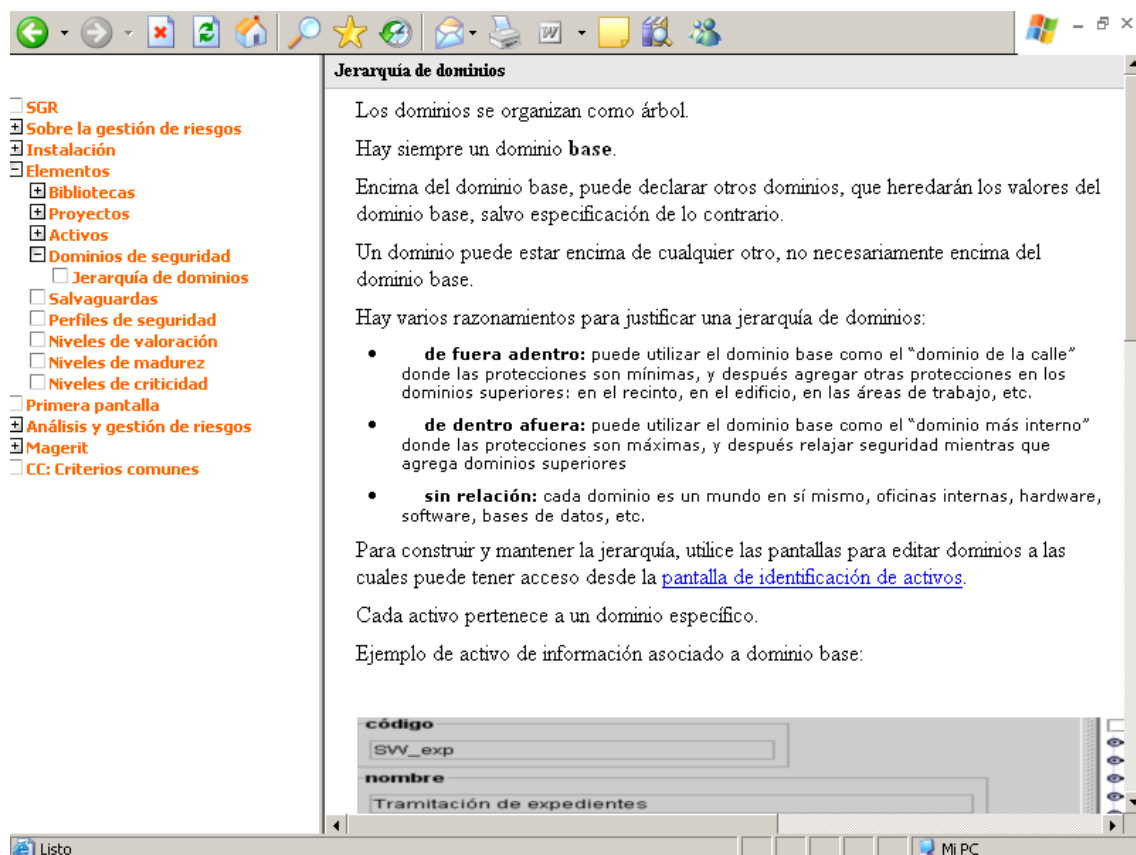
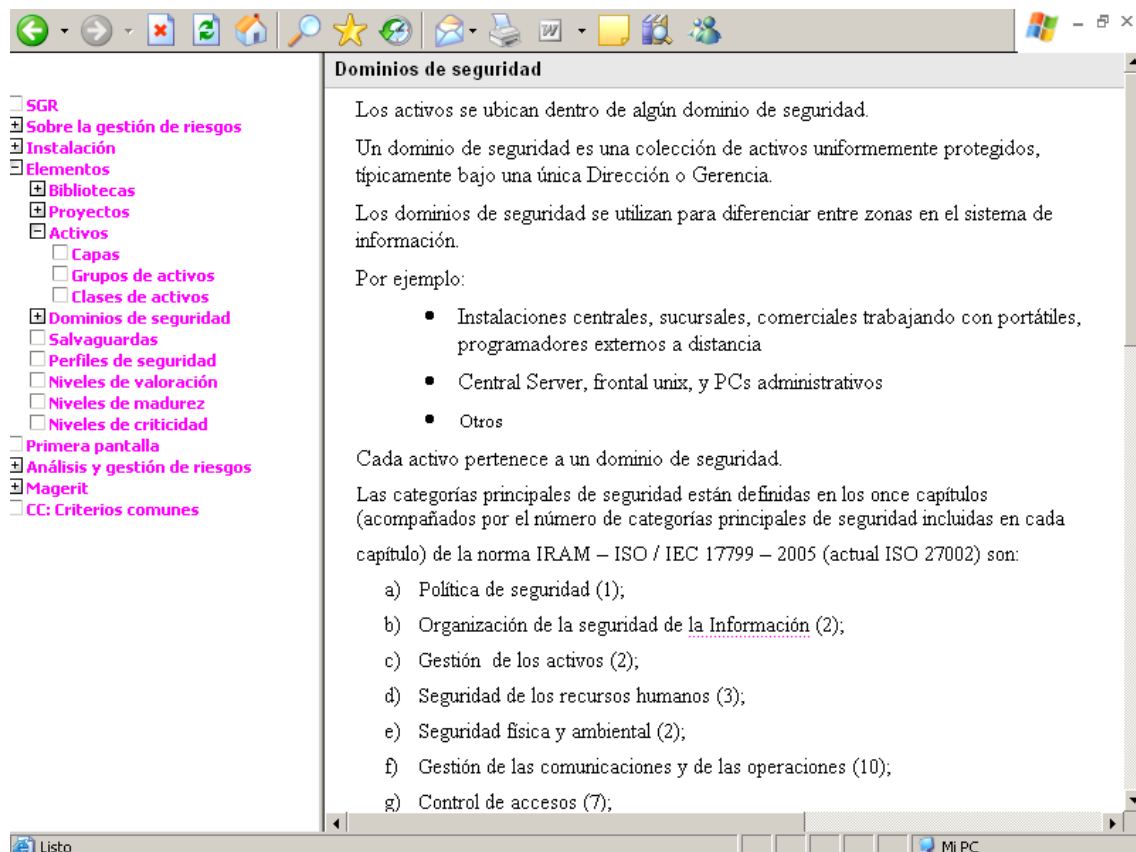
- una mejor descripción del activo
- pistas para sugerir amenazas típicas
- pistas para sugerir salvaguardas típicas
- pistas para remitir a protecciones adicionales

Ejemplos:

capas activos dominios estadísticas

ACTIVOS

- [FS] Funciones del sistema de información
 - [S_T_presencial] Tramitación presencial
 - [S_T_remota] Tramitación remota
 - [D_exp] Expedientes en curso
- [SI] Servicios internos
 - [email] Mensajería electrónica
 - [archivo] Archivo histórico central
- [E] Equipamiento
 - [sw] [SW_exp] Tramitación de expedientes
 - [hw] [PC] Puestos de trabajo
 - [SRV] Servidor
 - [network] [firewall] Cortafuegos
 - [LAN] Red local
 - [ADSL] Conexión a Internet
- [L] Instalaciones
 - [oficinas] Oficinas



The image displays two screenshots of a web application interface, likely a help or documentation system. Both screenshots feature a left sidebar with a tree view and a main content area.

Top Screenshot: Salvaguadas (en el SGR)

- Sidebar:**
 - SGR
 - Sobre la gestión de riesgos
 - Instalación
 - Elementos
 - Bibliotecas
 - Proyectos
 - Activos
 - Dominios de seguridad
 - Jerarquía de dominios
 - Salvaguadas
 - Perfiles de seguridad
 - Niveles de valoración
 - Niveles de madurez
 - Niveles de criticidad
 - Primera pantalla
 - Análisis y gestión de riesgos
 - Magerit
 - CC: Criterios comunes

- Main Content:**
- Las salvaguadas son medios para combatir y luchar contra las amenazas. Pueden tratar aspectos organizativos, técnicos, físicos o relativos a la gestión del personal.
- Las salvaguadas adecuadas de un Sistema de gestión de la información están planteadas en el siguiente documento [anexo de la norma ISO / IEC 27001](#)
- Otras salvaguadas están planteadas en:
 - Vea [salvaguadas en Magerit](#).
- En el SGR, las salvaguadas se pueden evaluar por dominio o por activo. La evaluación consiste en asignar un nivel de madurez [al proceso asociado] a la salvaguarda.
- Las salvaguadas se evalúan típicamente una vez para todos los activos en cada dominio de seguridad; pero cuando los activos no disfrutan de una protección homogénea, hay una opción para especificar valores específicos para activos específicos.
- Vea [niveles de madurez](#).
- Evaluación por dominio**
 - Se aplica un mismo valor común a todos los activos en el dominio. Si no se especifica ningún valor, se aplica el del dominio inferior. Si no se proporciona ningún valor en este dominio o en un dominio inferior, se aplica el valor en la fase previa.
- Vea [dominios de seguridad](#).

Bottom Screenshot: Perfiles de seguridad

- Sidebar:** (Identical to the top screenshot)
- Main Content:**
 - Los perfiles de seguridad son estándares o guías que se centran en uno o más aspectos de seguridad, y proporcionan un criterio de la conformidad que a veces se solicita previamente a la acreditación para funcionar en ciertos entornos o instituciones.
 - Algunos perfiles están internacionalmente reconocidos.
 - El SGR evalúa la satisfacción de estos perfiles estableciendo una correspondencia entre los requisitos contemplados por el perfil y el conocimiento de las [salvaguadas](#) alcanzado durante el análisis.
 - Vea [extensiones de la biblioteca](#).

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

nivel	significado
A - alto	el valor más alto, el daño más alto
M - medio	cuando las consecuencias no afectan a otras organizaciones externas
B - bajo	consecuencias limitadas, de carácter interno
insignificante	puede ser obviado a todos los efectos prácticos

Si existe necesidad de aplicar otras medidas y valores el cuadro siguiente muestra una metodología aplicable, que se presenta en la [ISO / IEC 27004](#).

SGR utiliza niveles de madurez para evaluar salvaguardas según el modelo de madurez (CMM) usado para calificar la madurez de procesos.

Inexistente	Inicial	Repetible	Definido	Gestionado
0	1	2	3	4
LEYENDA DE SÍMBOLOS EMPLEADOS		LEYENDA DE RANGOS EMPLEADOS		
	Estado actual	0 Inexistente	- No se aplican p	
	Referencia de la industria	1 Inicial	- Procesos ad	
	El mejor de la clase	2 Repetible	- Procesos sig	
	Estrategia de mejora	3 Definido	- Procesos doc	
		4 Gestionado	- Procesos sup	
		5 Optimizado	- Se siguen bu	

Niveles de criticidad

El SGR estima los riesgos según una escala simple de seis valores:

{5}	crítico
{4}	muy alto
{3}	alto
{2}	medio
{1}	bajo
{0}	insignificante

Ejemplo de valoración de riesgos por activo:

potencial	current	target	activo	
			[A] [email] mensajera electronica	{0}
			[A] [archivo] Archivo histórico central	{4}
			[E] Equipamiento	{5}
			[sw]	
			[A] [SW_exp] Tramitación de expedientes	{5}
			[hw]	
			[A] [PC] Puestos de trabajo	{5}
			[A] [SRV] Servidor	{5}
			[network]	
			[A] [firewall] Cortafuegos	{4}
			[A] [LAN] Red local	{4}

Primera pantalla

Para empezar rápidamente

Para ver un análisis de riesgos (sólo lectura):

- **modo** → **presentación**
- **análisis cualitativo**

Para trabajar en un proyecto nuevo o ya existente:

- **modo** → **trabajo**
- vaya al directorio donde guardó la licencia (fichero .lic) y selecciónela
- **análisis cualitativo**

Esta primera pantalla determina el modo de trabajo.

configuración

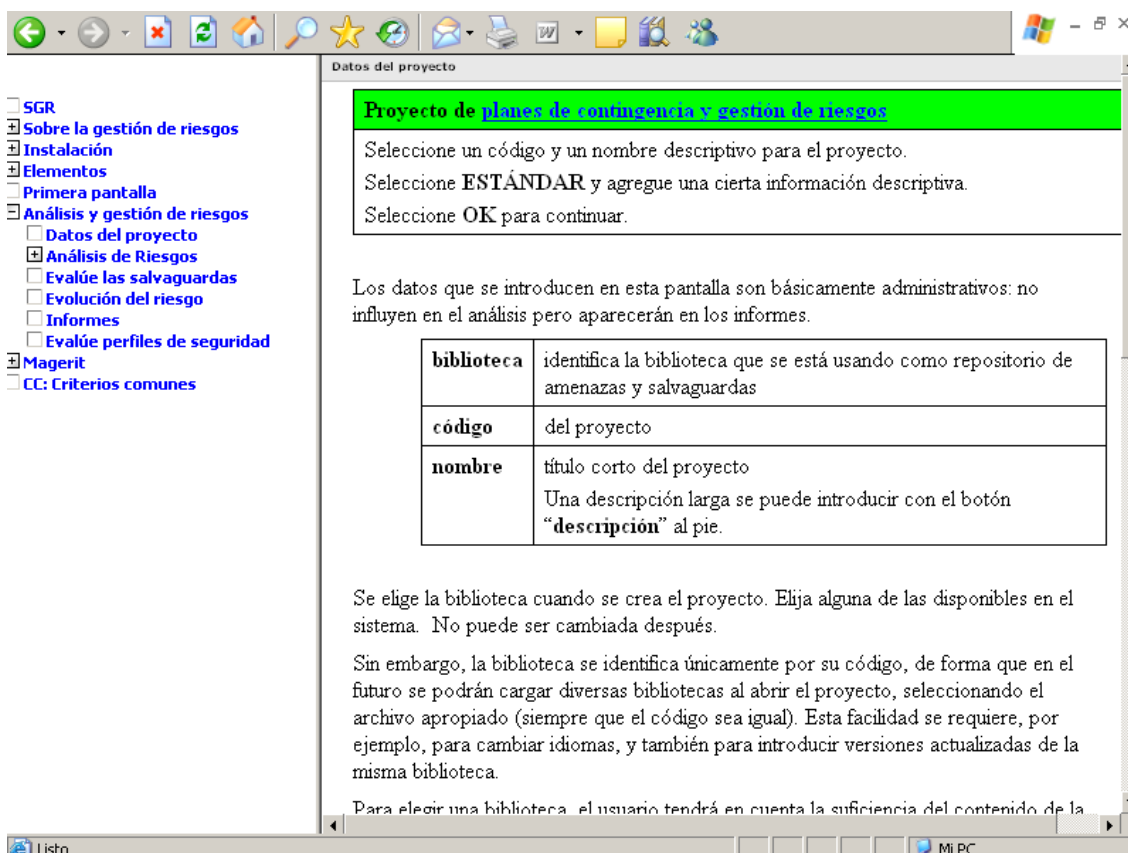
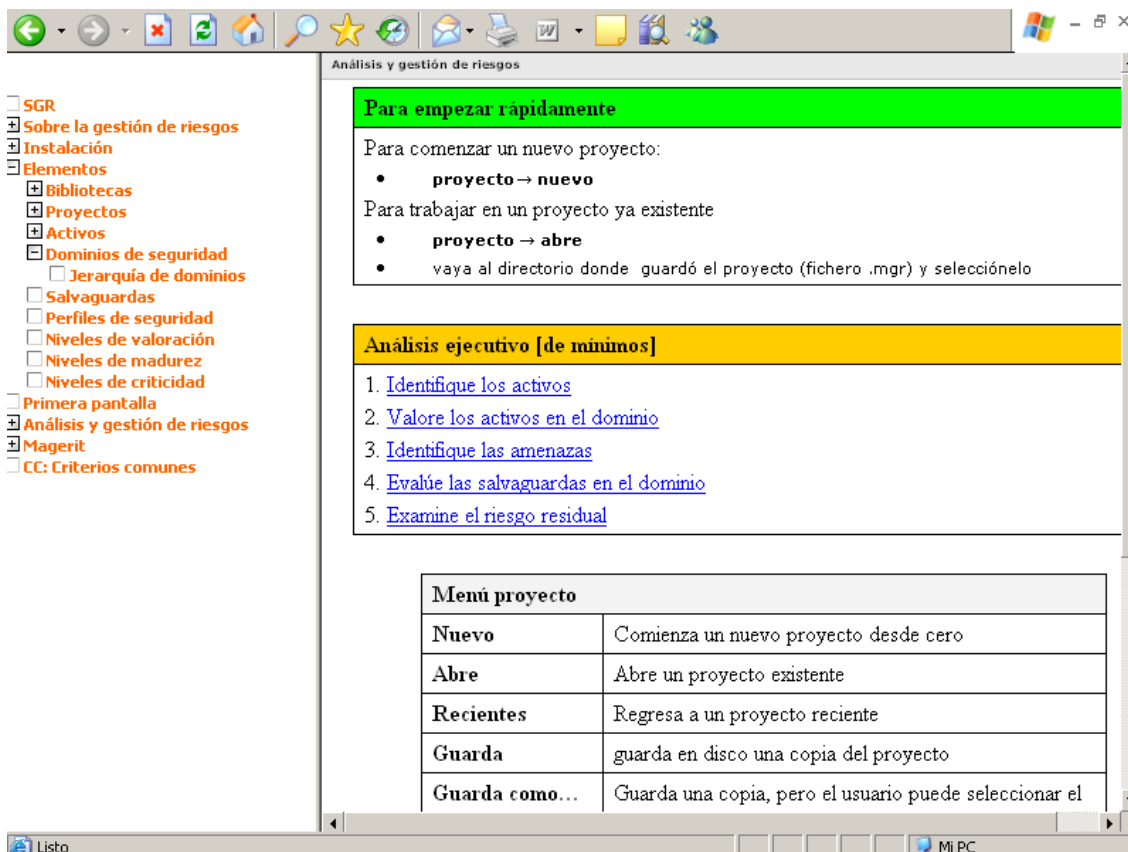
Elija una configuración de trabajo para las herramientas; es decir, idioma y biblioteca de funcionamiento.

Generalmente, elegirá STIC_es.car en el directorio de la instalación.

modo

Hay dos modos de usar el SGR:

- **presentación:**
Se puede visualizar los resultados, pero no se puede corregir datos.
- **trabajo:**
Se puede utilizar el sistema completo con todas sus posibilidades.



El análisis de riesgos es el conjunto de actividades que proporciona información para el tratamiento de los riesgos. A continuación se sintetiza lo establecido en la norma IRAM – ISO / IEC 17799 – capítulo 4 - **Evaluación y tratamiento de riesgos:**

4.1 Evaluación de los riesgos de seguridad

Se recomienda que la evaluación de riesgos identifique, cuantifique, y priorice los riesgos, en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para la organización. Se recomienda que los resultados guíen y determinen la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos. Puede ser necesario ejecutar más de una vez el proceso de evaluación de riesgos y la selección de los controles para cubrir diferentes partes de la organización o sistemas de información particulares.

Es conveniente que dicha evaluación incluya el enfoque sistemático de estimación de la magnitud de los riesgos (análisis de riesgos) y el proceso de comparación de los riesgos estimados contra los criterios de riesgo a fin de determinar la importancia de éstos (valoración de riesgos).

A su vez se recomienda efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. También debiera efectuarse la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

Se recomienda que la evaluación de riesgos de seguridad de la información tenga un alcance definido para ser efectiva y que incluya relaciones con las

Los activos del sistema necesitan ser identificados y después ser valorados.

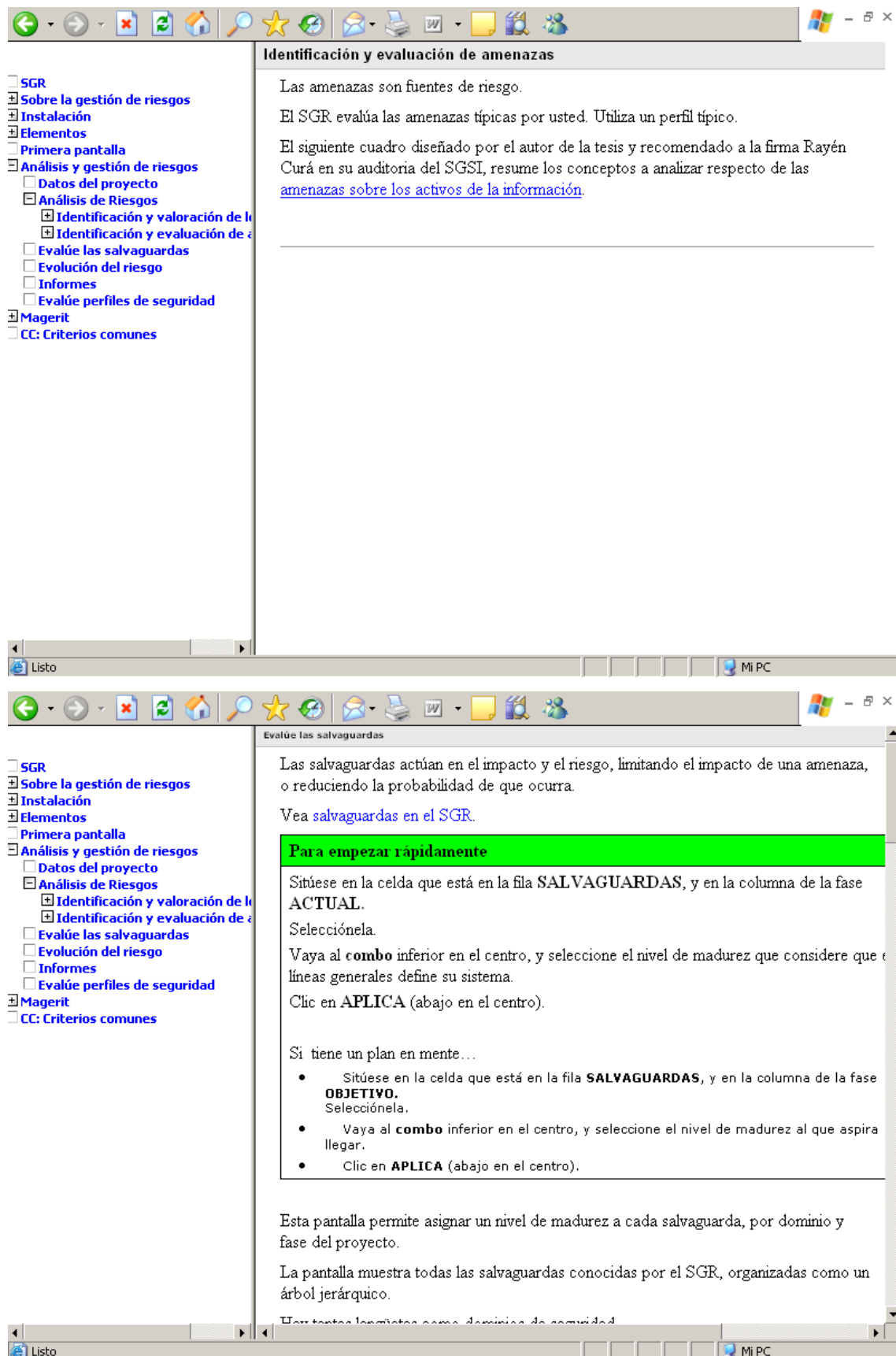
Para la identificación vaya a la [identificación del activo](#).

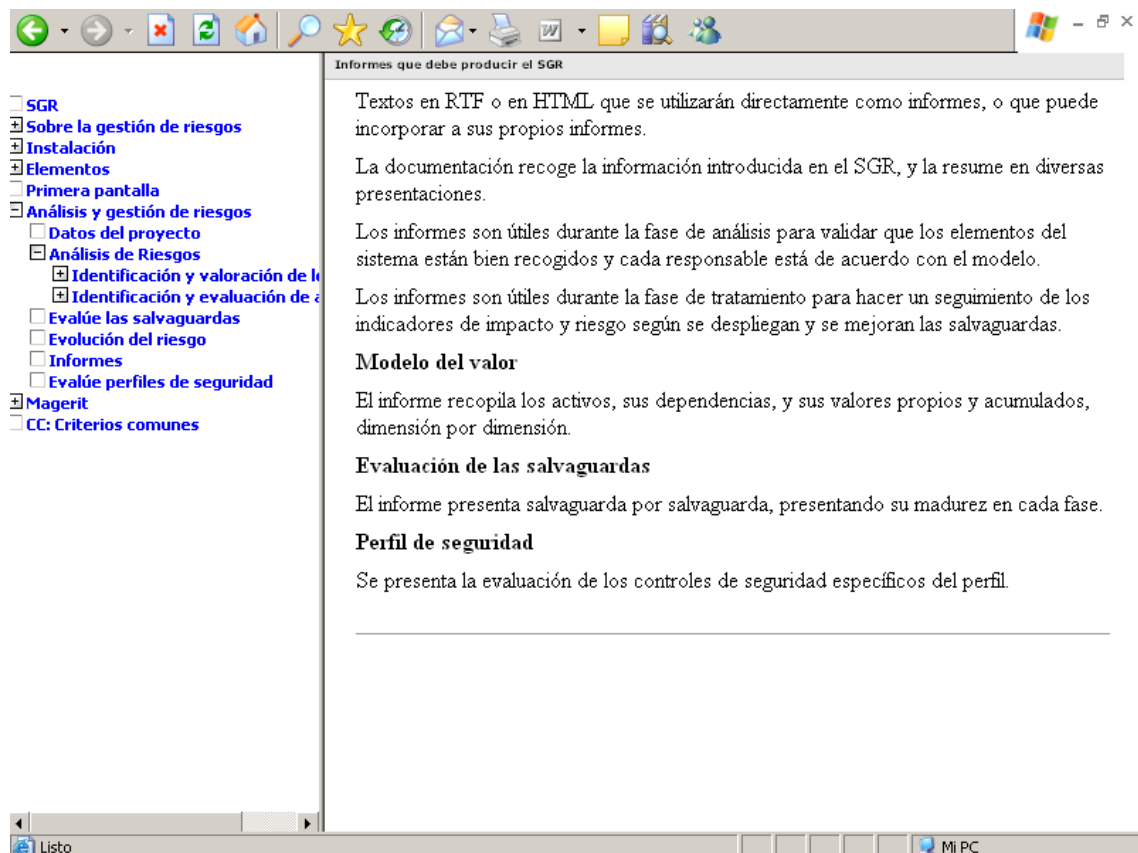
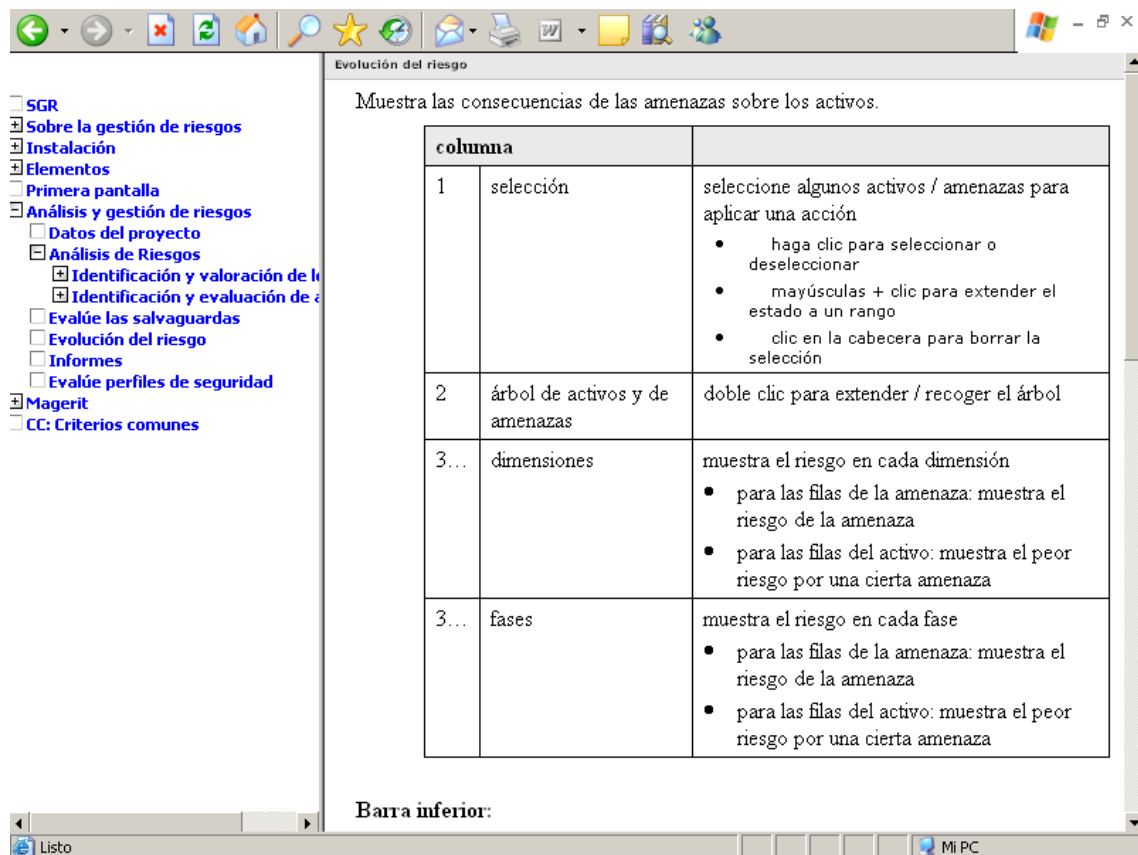
Para la valoración vaya a la [valoración del dominio](#)

Las Dimensiones de la Disponibilidad de los activos de información (Availability)

Fuente: Sungard Whitepaper: The evolution of contingency planning, www.sungard.com

The diagram illustrates the relationship between Business Availability, Data Availability, and Infrastructure Availability. It features three main vertical columns of boxes. The left column, labeled 'Disponibilidad del Negocio' at the top, includes 'Instalaciones de trabajo de emergencia redundantes' and 'Instalaciones de trabajo de emergencia'. The middle column, labeled 'Disponibilidad de Infraestructura' at the bottom, includes 'Con centros de proceso de emergencia', 'Con un centro de proceso de emergencia', and 'Sin centro de proceso de emergencia'. The right column, labeled 'Disponibilidad de datos' at the bottom, includes 'No hay copias de los datos', 'Respaldo de datos por lotes', and 'Respaldo de datos en forma continua'. A central stack of boxes represents different levels of availability: 'Negocio ininterrumpido', 'Negocio redundante', 'Negocio con alta disponibilidad', 'Procesamiento ininterrumpido', 'Recuperación con alta disponibilidad', and 'Imagen de datos en línea'. Arrows indicate dependencies and relationships between these elements.





Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Podemos ver la posición de seguridad del sistema desde el punto de vista de un perfil dado.

Hay tantas lengüetas como **dominios de seguridad**.

Se hace una presentación [parcial] de las salvaguardas evaluadas, y un resumen de la cobertura de los objetivos o de los controles de seguridad en el perfil seleccionado.

selección	para seleccionar algunas filas
recomendación	En cuanto a salvaguardas. Vea identificación de salvaguardas .
semáforos	Valoración de la salvaguarda / de la pregunta / del control en la referencia. Para seleccionar la fase de la referencia, haga clic en la cabecera de la fase
árbol	controles en el perfil + preguntas explícitas + referencias a las SGR.
comentario	a efectos de documentación, en particular si algún control es documentarse las razones que llevan a la exclusión es frecuente introducir comentarios relativos a planes de implementación de la situación actual
aplica	sí o no: el usuario decide. Este preparado para explicar sus decisiones a auditores e inspectores.
fases	tantas columnas como fases, recogiendo los valores en cada fila

El SGR utiliza la metodología Magerit,

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
"Ministerio de Administraciones Públicas"
<http://www.csi.map.es/csi/pg5m20.htm>

Magerit cubre las actividades de análisis y tratamiento de riesgos facilitando una gestión de riesgos informada.

1. El análisis de riesgos le permite conocer su sistema: sus activos, su valor, y las amenazas a las que está expuesto.
2. El tratamiento de riesgos se centra en seleccionar medidas de seguridad para conjurar las amenazas.
3. La gestión de riesgos es el proceso integral de tratamiento de los riesgos descubiertos durante el análisis.

El sistema se modela por medio de la identificación de los **activos** que lo componen. Los activos están expuestos a una serie de **amenazas** que, cuando ocurren, **degradan** el [valor del] activo, causando un cierto **impacto**.

Si estimamos la **probabilidad** de la amenaza, podemos concluir el **riesgo** en el sistema, o la pérdida a la cual está expuesto.

La degradación y la probabilidad califican la vulnerabilidad del sistema frente a una amenaza.

El responsable de seguridad tiene la oportunidad de desplegar **salvaguardas** para hacer frente a las amenazas.

Las salvaguardas mitigan los valores de impacto y riesgo dejándolos reducidos a unos valores **residuales**.

Vea también:

- [análisis de riesgos](#)

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Análisis de Riesgos

El análisis de riesgos es la parte del proceso de gestión de riesgos en la que se calculan los indicadores de impacto y riesgo que se utilizarán para tomar decisiones de tratamiento.

Uso sistemático de la información de identificar los orígenes y estimar el valor de riesgo.
Definición según la norma Reporte Técnico [ISO Guide73: 2002]

```
graph TD; A[amenazas] -- "están expuestos a" --> B[activos]; A -- "causan una cierta" --> C((degradación)); A -- "con una cierta" --> D((probabilidad)); B -- "Interesan por su" --> E((valor)); C --> F((impacto)); D --> F; E --> F; F --> G((riesgo));
```

El diagrama de flujo ilustra el proceso de análisis de riesgos. Comienza con 'amenazas' que 'están expuestos a' 'activos'. Las amenazas 'causan una cierta' 'degradación' y 'con una cierta' 'probabilidad'. Los activos 'Interesan por su' 'valor'. Tanto la degradación como la probabilidad contribuyen al 'impacto', que a su vez contribuye al 'riesgo'. El valor de los activos también contribuye al 'riesgo'.

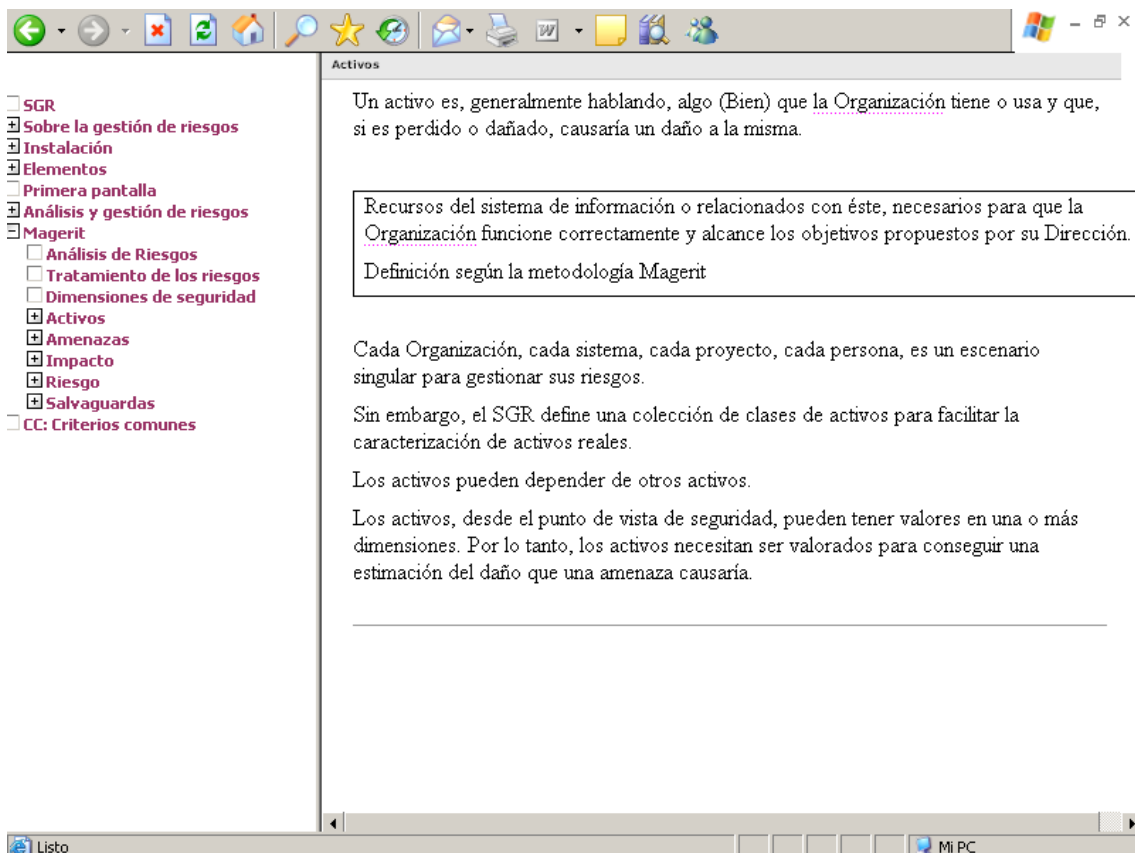
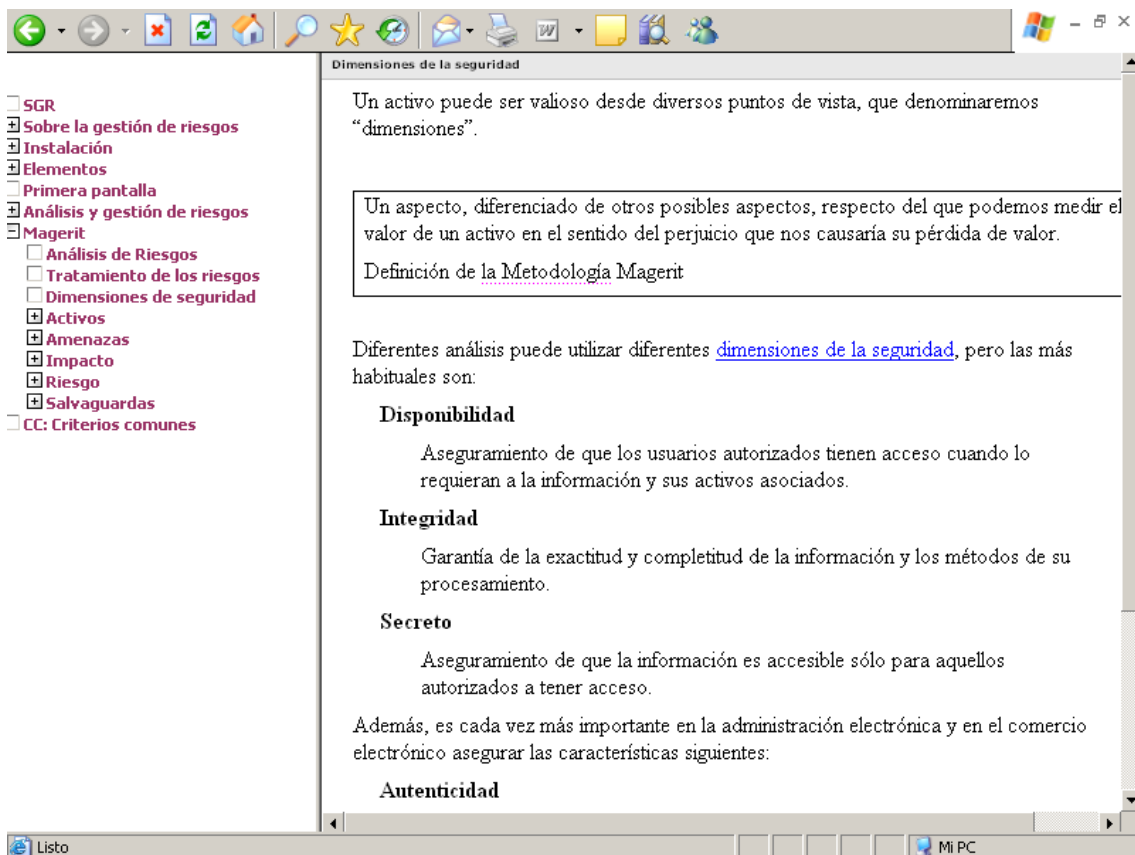
Tratamiento de los riesgos

Los resultados del análisis de riesgos proporcionan información que, comparada con los criterios de clasificación aprobados por la Organización, permiten tomar decisiones de tratamiento de los riesgos identificados.

Proceso de selección e implantación de medidas para modificar el riesgo.
Definición según la norma Reporte Técnico [ISO Guide73: 2002]

```
graph TD; A[amenazas] -- "están expuestos a" --> B[activos]; A -- "causan una cierta" --> C((degradación residual)); A -- "con una cierta" --> D((probabilidad residual)); B -- "Interesan por su" --> E((valor)); C --> F((impacto residual)); D --> F; E --> F; F --> G((riesgo residual)); S[salvaguardas] --> C; S --> D;
```

El diagrama de flujo ilustra el proceso de tratamiento de riesgos. Comienza con 'amenazas' que 'están expuestos a' 'activos'. Las amenazas 'causan una cierta' 'degradación residual' y 'con una cierta' 'probabilidad residual'. Los activos 'Interesan por su' 'valor'. Tanto la degradación residual como la probabilidad residual contribuyen al 'impacto residual', que a su vez contribuye al 'riesgo residual'. El valor de los activos también contribuye al 'riesgo residual'. Las 'salvaguardas' (definidas por tipo de activo, dimensión, amenaza y nivel de riesgo) actúan sobre la degradación residual y la probabilidad residual.



Amenazas

Una amenaza es cualquier evento que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de los activos de la organización.

Causa potencial de un incidente que puede causar daño a un sistema o a una organización

Definición tomada de la norma internacional [\[ISO/IEC 27002:2005\]](#)

Los activos son más o menos vulnerables a las amenazas que pueden ocurrir sobre ellos.

La vulnerabilidad de un activo a una amenaza se mide por medio de dos informaciones:

- la probabilidad de ocurrencia
- la degradación potencial del valor del activo

El daño potencialmente causado por las amenazas se puede mitigar por medio de salvaguardas.

Ejemplo de amenazas sobre los activos

	amenazas	activos
ACTIVOS		
[FS] Funciones del sistema de información		▲ [I] D
[SI] Servicios internos		▲
[E] Equipamiento		▲
[L] Instalaciones		▲

Impacto

El impacto es la medida del daño causado por una amenaza sobre un activo, cuando se materializa la misma.

Impacto

Consecuencias para la Organización cuando se materializa una amenaza.

Definición según [EBIOS: 2005]

El siguiente es un [ejemplo de análisis de impacto](#)

Sabiendo el valor de los activos, y la degradación causada por las amenazas, se estima el impacto como:

$$\text{impacto} = \text{valor} * \text{degradación}$$

El impacto, en conjunto con la probabilidad de la amenaza, nos da la medida del riesgo:

$$\text{riesgo} = \text{impacto} * \text{probabilidad}$$

Vea también:

- [impacto residual](#)
- [impacto acumulado](#)

Riesgo

Las amenazas sobre los activos son una fuente de daño que, si no es protegido, ocurre una y otra vez.

Si el impacto es el daño causado por cada incidente, el riesgo es el daño que se repite causado por incidentes que se repiten.

Riesgo

Combinación de la probabilidad de un acontecimiento y de sus consecuencias.

Definición según la norma Reporte Técnico [ISO Guide73: 2002] – [ISO / IEC 27005 – Gestión de Riesgos de los SGSI](#)

Sabiendo el impacto de una amenaza y su probabilidad, se estima el riesgo como:

$$\text{riesgo} = \text{impacto} * \text{probabilidad}$$

Salvuardas

Una salvaguarda o contramedida es cualquier cosa que ayuda a controlar y contener las amenazas existentes sobre nuestros activos.

Procedimiento o mecanismo tecnológico que reduce el riesgo.

Definición según la norma Reporte Técnico [ISO/IEC 13335-1: 2004]

El siguiente es un ejemplo de [salvuardas](#) un sistema de detección de intrusiones en la red.

Otro mecanismo importante cada día mas utilizado es la utilización de [criptografía y firma digital](#).

Hay muchos tipos de salvuardas. Podemos clasificarlas

- según el aspecto de seguridad en el que se centran
- según la estrategia que utilizan para detener las amenazas.

Las salvuardas actúan sobre amenazas...

- limitando el impacto
- reduciendo la probabilidad
- atenuando, en último extremo, el riesgo

Aunque algunas salvuardas no conllevan gastos significativos, otras veces sí tienen un coste que no puede ignorarse.

El costo es un factor importante a tomar en consideración cuando vayamos a seleccionar salvuardas para atenuar un riesgo.

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Eficacia de las salvaguardas

Es la medida de cuán eficaz es una salvaguarda.

Las salvaguardas perfectas son eficaces al 100%.

En la práctica, la eficacia es menor:

- porque la salvaguarda no está completamente desplegada
- porque la salvaguarda no está completamente operacional
- porque la salvaguarda no está perfectamente gestionada

La eficacia de las salvaguardas se utiliza para estimar el impacto y el riesgo residuales sobre los activos.

La eficacia de las salvaguardas se mide en términos de madurez.

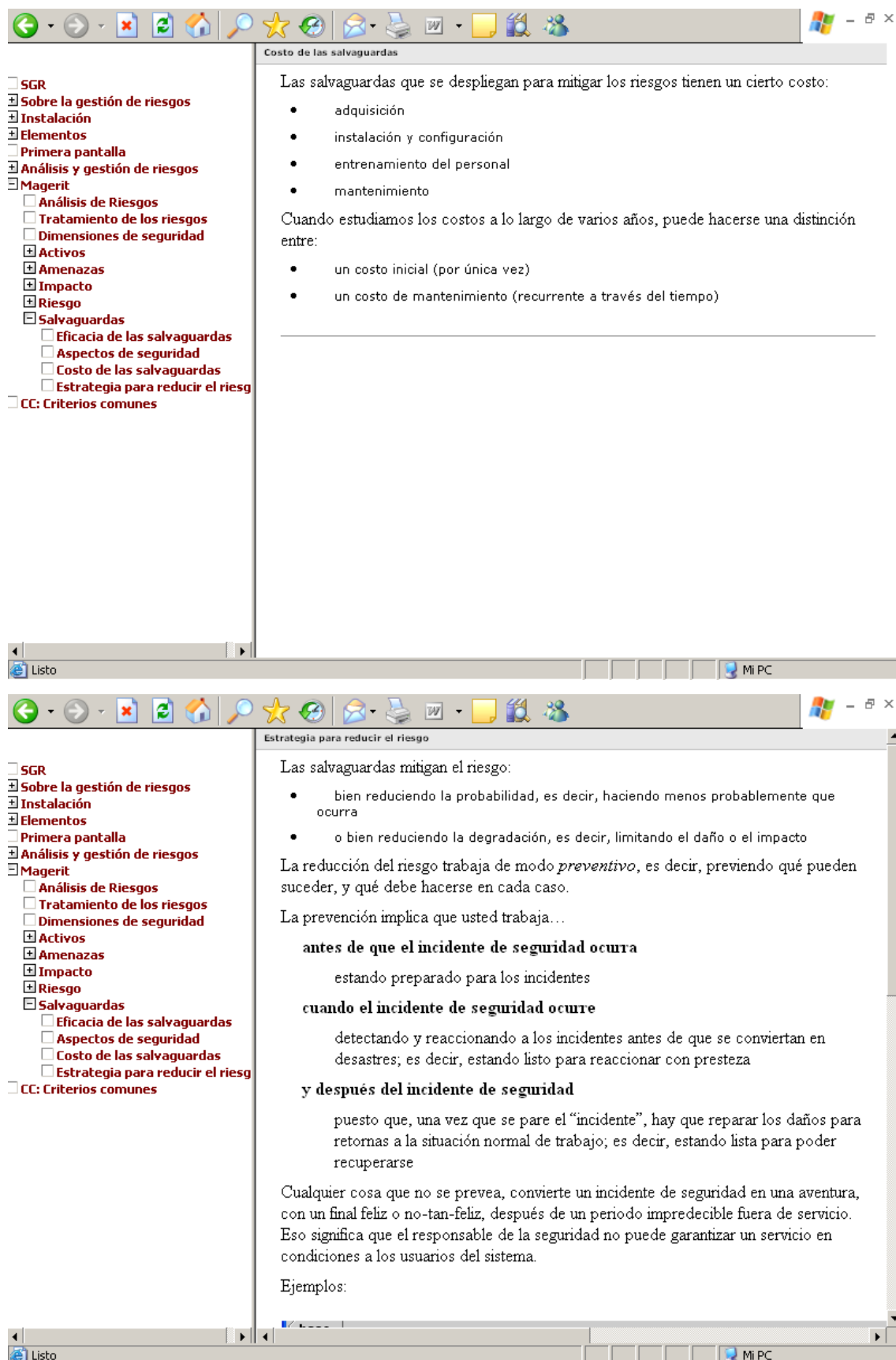
Cuando los niveles de madurez se traducen a porcentajes de la eficacia, el SGR utiliza la tabla siguiente:

nivel	significado	eficacia
L0	inexistente	0%
L1	inicial / ad hoc	10%
L2	reproducibile pero intuitivo	50%
L3	proceso definido	90%
L4	gestionado y medible	95%
L5	optimizado	100%

Aspectos de seguridad

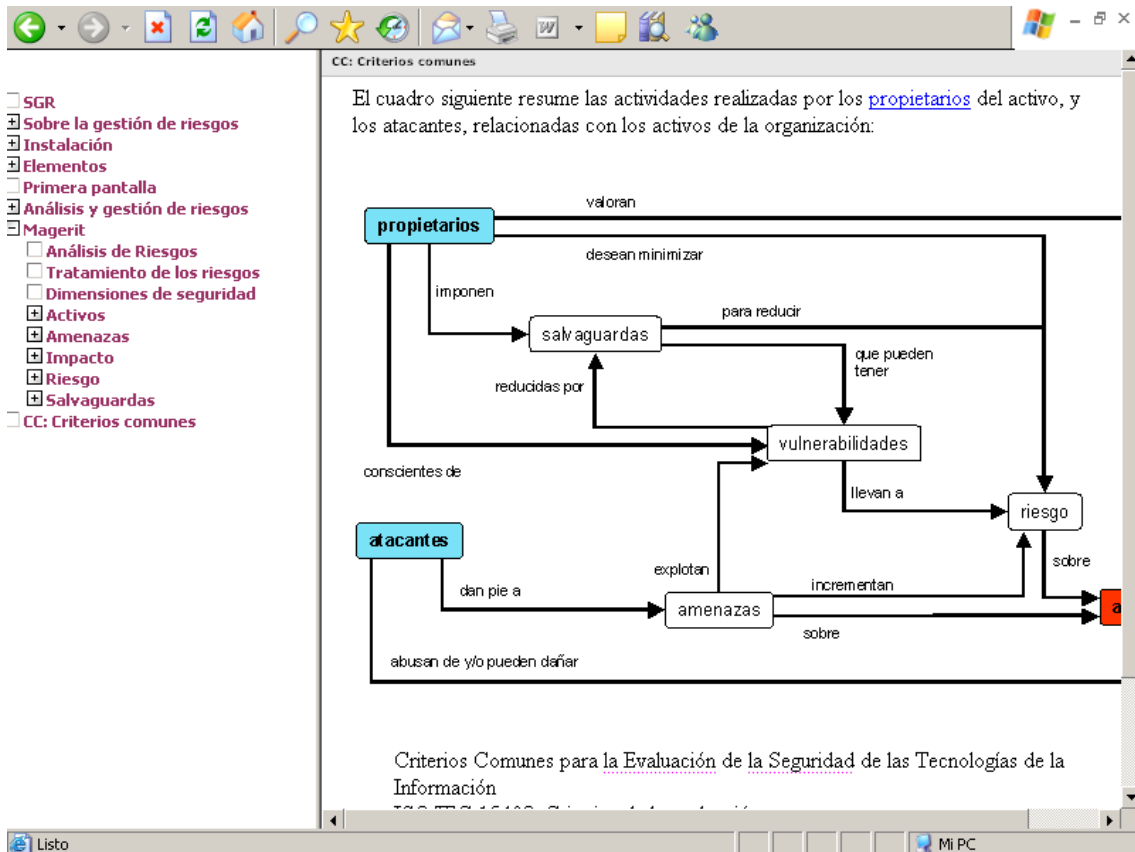
Cada salvaguarda se centra en cierto aspecto de seguridad. El SGR distingue los siguientes:

[G]	Gestión de la seguridad
[P]	Normativa del personal
[T]	Soluciones técnicas: software, hardware, comunicaciones, ...
[F]	Seguridad física y seguridad en redes



Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello



ANEXO VIII

PRESENTACIÓN DE LA AYUDA DEL SISTEMA AUDIT MANAGER DE LA FIRMA IDS SCHEER AG, PRINCIPALES FUNCIONES DEL SISTEMA

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio
Autor: Lic. Domingo Donadello

ANEXO VIII - PRESENTACIÓN DE LA AYUDA DEL SISTEMA AUDIT MANAGER DE LA FIRMA IDS SCHEER AG, PRINCIPALES FUNCIONES DEL SISTEMA:

Introducción

Cuáles son los requerimientos técnicos para el ARIS Audit Manager

Cómo está estructurada la ayuda del ARIS Audit Manager

Cómo está estructurada la interfase de usuario del ARIS Audit Manager

Cómo está estructurada la interfase de usuario del ARIS Audit Manager

La interfase del usuario se estructura como sigue:

The screenshot shows the ARIS Audit Manager interface. On the left is a tree view with categories like SOX, Testcases, SOA relevances, and Administration. The top bar displays the ARIS logo and user status. A toolbar contains 'Refresh' and 'Export' buttons. A filter area has dropdowns for 'Responsible' (set to 'My') and 'Result' (set to 'Open'). Below this is a table with columns: Testcase, Responsible, Performed by, Testing date, Testing period, Result, Type, Process, and Funkti. The table lists three testcases (100, 101, 107) with their respective responsible user groups and testing periods. A status bar at the bottom indicates 'Entry 1 to 3 selected'.

Testcase	Responsible	Performed by	Testing date	Testing period	Result	Type	Process	Funkti
100	User group 1	-	-	22/7/04-26/7/04	?	Correct value		
101	User group 3	-	-	22/7/04-26/7/04	?	Correct value		
107	User group 7	-	-	22/7/04-22/7/04	?	Correct value		

Cómo está organizado el árbol de vistas del ARIS Audit Manager Procedimiento

General

Cómo lanzar el ARIS Audit Manager

Cómo realizar Log in

Cómo enviar mensaje anónimo al administrador del sistema

Cómo cambiar su passwords

Cómo abrir un caso de test

Cómo enviar mensaje anónimo al administrador del sistema

Cómo cambiar el estado de un caso de test

Cómo crear un documento final en Microsoft Excel

Cómo navegar desde una SOA relevance al modelo de proceso

Cómo imprimir el contenido de la pantalla

Cómo imprimir tópicos individuales

Administración

Cómo crear un archivo de usuario de importación

Cómo importar usuarios / grupos de usuarios

Cómo importar SOA relevances

Cómo crear una nueva responsabilidad

Cómo cambiar la autorización de una SOA relevances

Cómo crear un nuevo usuario

Cómo especificar un usuario como sustituto

Cómo crear un nuevo grupo de usuario

Cómo asignar un padre al grupo de usuarios

Cómo asignar responsabilidades a grupos de usuarios

Cómo asignar un usuario a un grupo de usuarios

Cómo deletar la asignación de un usuario de un grupo de usuarios

Cómo cambiar la autorización de un grupo de usuarios

Cómo asignar password a usuarios

Cómo crear un nuevo cliente

Cómo crear una nueva SOA relevance

Cómo crear una nueva especificación de test

Cómo controlar un test case completo

Cómo cambiar el seguimiento para un test case

Cómo crear un seguimiento

Cómo limpiar completamente un test case

Cómo crear un proceso de integración a la Web

Información útil

General

Cuál es el propósito del workflow de un test SOA y Cómo él trabaja

Cómo es el modelo estructurado del workflow del test SOA

Qué se necesita tener en cuenta para modelar en ARIS

Cómo se realiza el concepto de delegado

Cuáles test cases está incluido en el proceso de follow-up

Qué status pueden tener los test cases

Qué evaluación está disponible para un test de control no efectivo

Qué períodos de testing deben ser definidos como parte de una responsabilidad

Qué probabilidad de ocurrencia está disponible para un riesgo

Qué efectos están disponibles para una SOA relevances

Cómo se crean versiones de SOA relevances

Qué es logearse en el sistema

Administración

Qué tareas tiene un administrador

Cuál es la estructura de un grupo de usuarios / usuarios en el archivo de importación

Cómo se manejan usuarios

Cómo se estructuran los usuarios / grupos de usuarios

Qué es el concepto básico de privilegio

Cuál es la estructura del archivo de importación de una SOA relevance

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Cómo se gestiona el seguimiento de una responsabilidad

Cómo se automatiza la notificación a los testers

Qué opciones se ofrecen por el proceso de integración Web

Glosario

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en
Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

ANEXO IX

TECNOLOGIA DE SALAS COFRES. 2006-2007 – NORMA ICREA STD-131-2007- ANTECEDENTES

ANEXO IX

TECNOLOGIA DE SALAS COFRES. 2006-2007 – NORMA ICREA STD-131-2007- ANTECEDENTES

Introducción:

Una de las primeras necesidades que dieron nacimiento a la Seguridad Física para Informática fue la preservación de los datos de respaldo, más conocidos como Back-Up.

Nos remontamos a la década de los años setenta, en la cual se comprobó que los límites de supervivencia de los medios magnéticos, eran diferentes a los del papel, y en caso de exposición a temperaturas superiores a los 75 grados Celsius y más de 85% de humedad relativa ambiente, los datos pierden su integridad. Luego se comprobó también que frecuentes problemas para lograr la restauración de las aplicaciones a partir de respaldos en cintas, eran causados por el hollín y el polvo sedimentado en la superficie de las cintas.

Para resolver esta necesidad, se rediseñaron las antiguas cajas de seguridad, se investigaron nuevos materiales a partir de los que entonces se utilizaban, y surgieron los primeros Cofres para Datos.

Debido a que la Integridad de los datos debía estar garantizada, se desarrollaron procedimientos de test para Cofres simulando las reales y verdaderas condiciones experimentadas durante incendios.

Se ensayaban los primeros prototipos sometiéndolos a la acción del fuego y del impacto, midiendo por un tiempo determinado en la norma cuál era la elevación de la temperatura y humedad relativa en el interior del Cofre testado.

El Objeto de esta norma fue y lo es aún, garantizar que no se superen los límites de temperatura y humedad necesarios para la supervivencia de los datos almacenados en cintas para garantizar su Integridad en caso de incendios e impactos severos.

En los Estados Unidos de América, para ensayar armarios y cofres para datos, la norma desarrollada hace varias décadas es la UL 72, y la equivalente desarrollada en Europa, original de Alemania es la VDMA 24.991, y ambas tienen objeto y alcance equivalente. La norma alemana luego fue tomada como base para convertirla en euro norma EN-1047 parte 1.

Estas normas y los ensayos descritos en ellas, no tienen previsto en su objeto de teste (cofre), que exista vinculación alguna entre el interior del cofre y el medio ambiente, dado que los back-up off line, son cintas o discos ópticos que no están almacenados en ningún dispositivo de lectura o procesamiento conectado a las redes de lógica y potencia.

Ya en la década de los ochenta, algunas empresas acumulaban una gran cantidad de cintas de back-up, lo que las obligaría a adquirir decenas de Cofres para Datos. Ante la necesidad de comprar una gran cantidad de cofres para datos una empresa alemana, hoy global, preguntó si no era posible concebir "un ambiente tipo cofre, para datos" creándose así la necesidad de concebir un recinto que tuviera las propiedades de un Cofre, al cual se lo denominaría, más tarde "Data Room" o "Sala Cofre".

La primer Sala Cofre se desarrolló en Alemania, y para que ésta pudiera ofrecer garantías de protección como las de un cofre fue preciso crear un método formal y neutral, mediante la conformidad de una norma Certificable específica, que fue denominada VDMA 24.991 parte 2.

Esta norma dio nacimiento a una nueva modalidad de ensayo que tenía en consideración que el objeto de test ya no sería un pequeño cofre, monobloque y transportable, sino que sería un ambiente de grandes dimensiones, que debía ofrecer las mismas garantías de protección físico-ambiental.

A partir de esta norma alemana, la actual norma mundialmente reconocida que fue desarrollada especialmente la EN-1047/2 (euronorma), y su equivalente BS-1047-2 (British Standard), que son tomadas como base de la única norma regional que es la NBR/ABNT 15.247, siendo ésta última la más moderna en la actualidad.

Ver información oficial en:

http://www.fup-gut.de/english/resistancegrade_e.htm

O simplemente en Google colocando "Data Room" + EN 1047/2

Mientras en Europa se desarrolló este estándar, en los Estados Unidos, no se desarrolló uno equivalente, debido a que los agentes de riesgo del territorio americano priorizan la recuperación luego de desastres naturales y no la preservación ante incidentes o desastres de origen humano, ambientales o físicos, y que en la actualidad

constituyen el mapa de riesgos más preocupantes. En EEUU las políticas de recuperación de desastres están priorizadas por sobre la protección y es por esto el gran desarrollo de las duplicaciones, redundancias y espejamiento.

Dado esto, no existe equivalencia entre normas europeas y americanas para Salas Cofre, lo cual ya ha sido comprobado y documentado en varias instancias licitatorias e informes técnicos, por ejemplo del INTI, en Argentina, en la ABNT en Brasil, para mencionar los países más próximos. Asimismo contamos con comunicaciones de UL manifestando oficialmente esto, y que es parte de los documentos utilizados por el B.I.D en el proceso de evaluación de ofertas del proyecto AFIP/Argentina-LPI 47-02. (Tenemos copia)

A partir de estos antecedentes y documentos, hemos incorporado al glosario de términos, y a los niveles de categorización 4 y 5 de Centros de Datos conforme la norma I.C.R.E.A Std 131-2007, la tecnología de Salas Cofre y su correcta aplicación dentro de los proyectos y auditorías a realizarse a partir de 2007.

El Underwriters Laboratory (UL-EEUU) sólo lista materiales que hayan sido sometidos a pruebas de resistencia al fuego (ASTM E 119), que luego pueden ser usados como barreras corta fuego en perímetros externos, pero UL no tuvo la inquietud de invertir en nuevas instalaciones para ensayar ambientes completos (Salas Cofre) de grandes dimensiones, situación que no ha variado hasta el presente, conforme consta en declaraciones oficiales de los ingenieros de UL.

Entonces, más adelante podremos ver un cuadro resumen donde se detallan los niveles de protección que son garantizados para cada una de las normas mencionadas de tal manera de dar certeza sobre las responsabilidades que pueden asumirse en materia de protección para ambientes de Datos y Hardware.

UNA INDUSTRIA MUY ESPECIALIZADA EN DESARROLLO

Cientos de Salas Cofre fueron instaladas en todo el mundo para las primeras Cintotecas de Respaldo de grandes empresas, y en 1987, en la ciudad de Mestre, Italia, Telecom Italia sufrió el incendio total de un edificio, del cuál sólo pudieron sobrevivir los back-up protegidos en una Sala Cofre Certificada conforme la norma VDMA 24.991 parte 2 (actualmente EN.1047-2), y esta "prueba de fuego" sirvió para que ésta misma empresa decida utilizar este estándar a nivel mundial para las áreas críticas de TICs.

Algunos años después el volumen de datos seguía creciendo por el aumento de performance de los "Mainframe", y aparecieron los primeros robots para almacenamiento de datos "en operación" y para esto hubo que desarrollar una nueva tecnología de Salas Cofres, que pudiera mantener estables y confiables las demandas de potencia y climatización de grandes computadores, lo que incluía una gran dinámica para el ambiente (cambios de computadores, replanteo de lay-out, ampliaciones de la Sala Cofre), y todo esto manteniendo los niveles de protección Certificados originales.

Entonces, las Salas Cofres pasaban a ser no sólo un ambiente de protección sino un ambiente con infraestructura eléctrica y mecánica con demandas crecientes, lo cual se ha acentuado en la actualidad.

Luego de los robots y mainframes, surgieron, en los '90, los primeros servidores que fueron distribuidos en diferentes departamentos internos de las empresas, lo cual generó un procesamiento distribuido.

El procesamiento distribuido fue creciendo hasta generar problemas para el control y la integración de los sistemas y empezó la era de la concentración en Pool de Servidores.

Nacen así la segunda generación de Centros de Cómputos, hoy llamados Data Centers, donde convivían sistemas de almacenamiento robotizados, mainframes para las aplicaciones core y los servidores para aplicaciones departamentales que debían ser integrados, y para proteger semejante concentración de valor es que la tecnología de Salas Cofre tuvo que evolucionar para ser un Sistema Prefabricado "Modular", que mantenga las características de protección de la norma EN-1047-2.

En este salto tecnológico, las Salas Cofre ya definitivamente dejan de tener cualquier punto de comparación con las Bóvedas refractarias, los encofrados o los Vaults norteamericanos.

Las primeras Salas Cofre IT Modulares fueron utilizadas para securitizar un área del Centro de Datos existente, donde se protegían todos los equipos de cómputo crítico, alguno de los cuales ya estaban en operación y debían seguir funcionando mientras eran recibidos servidores de diferentes áreas, y de manera incipiente nos aproximábamos a la era del Internet y de las comunicaciones.

De más está decir que el impacto económico de parada de un Centro de Cómputos ya era grande en aquella época, y ahora es difícil de calcular, aunque es sabido que el resultado tiende a ser insoportable para la continuidad del negocio.

Por este motivo, la responsabilidad para las empresas que proyectan, proveen e instalan Sala Cofre IT Modular, tiene un riesgo contingente incalculable en caso de error en cualquiera de las fases de proyecto, producción y ejecución de cada proyecto.

Este es el principal motivo que existan muy pocas industrias a nivel mundial que asuman semejante responsabilidad.

Veamos una de las etapas previas al ensayo conforme la norma EN-1047-2:



Preparativos del Ensayo de una Sala Cofre IT Modular conforme EN-1047-2

Este prototipo, tiene dimensiones especificadas en la norma, y será sometido al fuego en todos las paredes y techos, y luego será ensayado contra impacto.

A los ensayos realizados por la norma EN-1047-2, que son condición necesaria para avanzar en una Certificación conforme dicha norma, sabemos que se le están agregando otros ensayos complementarios, que agregan valor a la tecnología de protección, y cuyos detalles pueden encontrarse en la norma NBR-ABNT- 15.247, sobre la cual haremos mención más adelante.

Conforme hemos estudiado la evolución de esta tecnología, primero vemos que las Normas se actualizan para acompañar la dinámica de los riesgos y necesidades operacionales en la aplicación dentro de Centros de Datos, y luego los fabricantes investigan, ensayan y presentan para la Certificación nuevos modelos de Salas Cofre.

Existen tres fabricantes de Salas Cofres Certificados en el mundo, que son: Lampertz AG (Europa,EEUU,ASIA), Priorit (Alemania), y Sismetel-Aceco TI (America

Latina-Alemania) En la actualidad, los Data Centers son el Cerebro operacional de las organizaciones y los computadores centrales precisan sobrevivir a las emergencias, para poder garantizar una vuelta a la normalidad luego de contingencias de manera rápida y previsible. Sin esta capacidad, la continuidad del negocio puede colapsar rápidamente.

Es por esto que en la actualidad las Salas Cofre IT Modulares son una excelente solución para crear dentro del Centro de Datos un área segura y Certificada, que proteja de todos los riesgos (1) del medio ambiente (Fuego, calor, humo, gases corrosivos, impacto de escombros, explosiones, sabotajes, intrusiones, agua, inundaciones, humedad, polvo y radiofrecuencias).

En resumen, las Salas Cofre IT Modulares son la única tecnología que garantiza, conforme normas internacionales (ya reconocidas en la argentina), la protección efectiva multifuncional contra todos los agentes de riesgos antes mencionados (1), y que, además, puede implantarse en Centros de Datos nuevos o existentes, sin obra húmeda, y en muy poco tiempo de ejecución, protegiendo los datos y equipos críticos para garantizar su supervivencia en caso de contingencias.

(1) LISTADO DE RIESGOS DESCRITO EN LA NORMA ISO-IEC 17799

La tecnología más avanzada de Salas Cofre para garantizar la protección de Data Centers es mediante el procedimiento de certificación conforme la norma NBR 15.247 bajo la metodología aprobada por la ABNT/INMETRO PE047.01. Esta norma incluye a la EN-1047-2 como ensayo de resistencia al fuego y al impacto, pero agrega otros ensayos que completan la cobertura de riesgos físicos conforme el siguiente cuadro resumen:

Salas Cofre Certificadas vs Contrucción Tradicional

Modelo	Test Fuego Elementos	Test Fuego Sala Completa Confinada	Test Completo Piso y Estructura Auxiliar	Test Agua y Polvo Presur. IP 67	Test Agua Sprinkler NBR 10849	Teste Estanq. ASTM E 779
ABNT 15247	✓	✓	✓	✓	✓	✓
ECB-S 1047-2	✓	✓	✗	✗	✗	✗
CERTIFICABLES						
Bóvedas tipo ASTM E 119 simulando UL 72	✓	✗	✗	✗	✗	✗
Construcción tradicional	✓	✗	✗	✗	✗	✗
NO CERTIFICABLES						

Salas Cofre Certificadas vs Contrucción Tradicional Organismo de Certificación:

<http://www.inmetro.gov.br/prodcert/certificados/busca.asp>

Buscar en el listado de productos certificados ordenados por orden alfabético hasta encontrar Salas Cofre y Cofres para hardware

CONCLUSIONES ABC:

A. La Sala Cofre es una tecnología de Seguridad embebida en una modalidad constructiva, que ya tiene varias décadas evolucionando y son mas de 2.500 las Salas Cofre instaladas en el mundo.

B. Se basa en normas especialmente desarrolladas para la protección de datos y hardware que deben ser Certificadas.

C. Aún existe la necesidad de esclarecer y difundir conocimiento sobre estas normas, y la legalidad del procedimiento de Certificación a nivel mundial, dado que en este proceso no sólo se garantiza el cumplimiento de los niveles de protección necesarios, sino que garantiza además, una garantía de corresponsabilidad entre el oferente y el Organismo de Certificación.

SUSTENTABILIDAD DE LA SALA COFRE COMO AMBIENTE DE MAXIMA SEGURIDAD DE UN CENTRO DE DATOS RIESGOS:

Al riesgo propio del edificio, tanto en el piso del Centro de Datos como los del piso inferior y superior, deben sumarse los del entorno del edificio.

Riesgo es, conforme el Sistemas de Gestión de la Seguridad de la Información (SGSI-ISO 27.001) aquellos agentes(2) cuya presencia no puede descartarse, independientemente de la frecuencia o intensidad con que podrían generar un incidente o un desastre.

El gerenciamiento de riesgos debe ser constante porque el mapa de riesgos es dinámico, siendo hoy de gran preocupación para el mundo de la informática, riesgos como la contaminación del ambiente por humo, gases corrosivos, agentes químicos, polvo y hollín. También preocupan los efectos colaterales de disturbios sociales, actos de vandalismo, explosiones y ataques con radiofrecuencias.

La protección contra el fuego es la más difundida, pero esto resulta una visión muy simplista del contexto de amenazas y vulnerabilidades que hay que prevenir.

Los agentes de riesgo que hay que evaluar individualmente y luego en conjunto son:

AMBIENTALES tales como el Fuego y sus consecuencias: calor, humo, contaminación por gases y líquidos, explosiones, humedad relativa superior el 85%, vapor; inundación, granizo, rayos y otros producidos por la naturaleza

HUMANOS tales como acceso indebido, intrusiones violentas, sabotaje, disturbios sociales, o fallas por uso inapropiado o accidentes.

TECNICOS tales como los generados por el mal uso o desgaste de los dispositivos de infraestructura, generación de campos magnéticos o de radiofrecuencias, ya sea por proximidad de agentes contaminantes o por actos criminales.

(2) Vulnerabilidades + Amenazas = Riesgo

Del análisis de incidentes y desastres producidos sobre equipamiento electrónico, y tomando como base las estadísticas de compañías reaseguradoras especializadas en la materia, se han llegado a varias conclusiones interesantes:

-- La construcción corporativa tradicional y la seguridad física y contra-incendios diseñadas para ambientes de trabajo, no ofrecen respuesta a los agentes de riesgos que pueden afectar la integridad de datos y equipamiento electrónico.

-- Las tecnologías utilizadas para la seguridad corporativa no permiten lograr una solución de gerenciamiento y control de riesgos multifuncional, que no sólo controle un riesgo de manera individual, sino en su interacción y concatenación con otros agentes de riesgos presentes en el entorno al Data Center.

-- Dado esto, las compañías de seguro especializadas en "seguros técnicos" para TICs, exigen Salas Cofre Certificadas, como condición necesaria para cubrir no sólo el valor del equipo asegurado, sino el "loss profit" por no operación del/los equipos cuya disponibilidad o pérdida haya sido generada por un incidente o desastre de origen físico-ambiental.

¿POR QUÉ ES NECESARIA UNA SALA COFRE CERTIFICADA AÚN EN CASO DE TENER CENTROS DE CÓMPUTOS PARALELOS O DE CONTINGENCIA?

En un análisis preliminar, al momento de evaluar si es necesario contar con el nivel de protección de una Sala Cofre, es habitual que se crea que contando con redundancia de dos Centros de Cómputos, no sería necesario proteger uno o ambos.

En la actualidad esta pregunta tiene cada vez una respuesta más cercana a la necesidad de proteger el sitio primario con Sala Cofre, lo cual es considerado un complemento inteligente para la inversión en redundancia, y en caso en que la arquitectura de TICs muestre que la redundancia es parcial, no caben dudas sobre la necesidad de preservar los activos críticos del Sitio Primario.

El espejamiento parcial o total es necesario y no siempre es posible de lograr de manera sostenible, y uno de los máximos desafíos puede ser la implantación de Soluciones como el Sysplex paralelo, que realiza la recuperación de errores desde un sólo punto de control, es decir, es una Solución donde no se prioriza un Centro de Cómputos sobre otro sino que funcionan como "un par" coordinados desde un punto de control, que administra el procesamiento geográficamente dividido.

La implantación de sistemas que funcionan en "paralelo" plantean un escenario donde el interés a proteger es la sustentabilidad del "procesamiento en Paralelo" para garantizar así la continuidad del servicio, utilizando la capacidad residual de cada procesador paralelo para soportar la operación aún en caso de las frecuentes fallas

técnicas o humanas, además de los problemas de comunicaciones que afecten a uno de los paralelos.

En condición normal, ciertas aplicaciones serán divididas y por lo tanto una parte del banco será soportado por un sitio, y otra parte del banco será soportado por el otro.

Esta tecnología es excelente y probada en grandes bancos a nivel mundial, porque los incidentes técnicos menores, que son muy frecuentes, no son percibidos por el usuario o por el cliente.

Pero, ¿qué pasaría si un incidente de origen físicoambiental como: fuego, calor, humedad, contaminación, etc, que impactan de manera concurrente a todos los equipos de cómputo del Centro de Datos, terminara con la integridad de los computadores críticos de uno de los paralelos?

La sustentabilidad del "paralelismo" quedará sin capacidad de ser restaurada por tanta cantidad de meses como puedan ser comprados, configurados y puestos en marcha los nuevos computadores.

Dentro de la Estrategia de Continuidad de los Sistemas de Información regulada por el BCRA, conforme la reciente circular 4609, es necesario no sólo gerenciar las contingencias durante las mismas, sino demostrar que la Vuelta a la Normalidad es en un plazo compatible para no entrar en un conocido "loop" conocido como "contingencia de la contingencia".

En LATINOAMÉRICA y en particular para empresas estatales, volver a comprar todos los computadores, aún con autorizaciones de emergencia, puede demandar muchos meses, y esto no es compatible con los tiempos de la Informática.

Salas de cómputo construidas con materiales tradicionales no pueden ser Certificadas porque no ofrecen garantías ni están diseñadas conforme a ninguna norma que integre todos los materiales utilizados como parte de un conjunto que pueda ser ensayado.

Las Salas Cofres garantizan esto, y sirven al propósito de garantizar una vuelta a la normalidad de la "redundancia" en horas o pocos días.

Diferentes análisis de riesgo y análisis de impacto realizados con herramientas como el BIA (Análisis de Impacto sobre el Negocio) por parada del Data Center, y

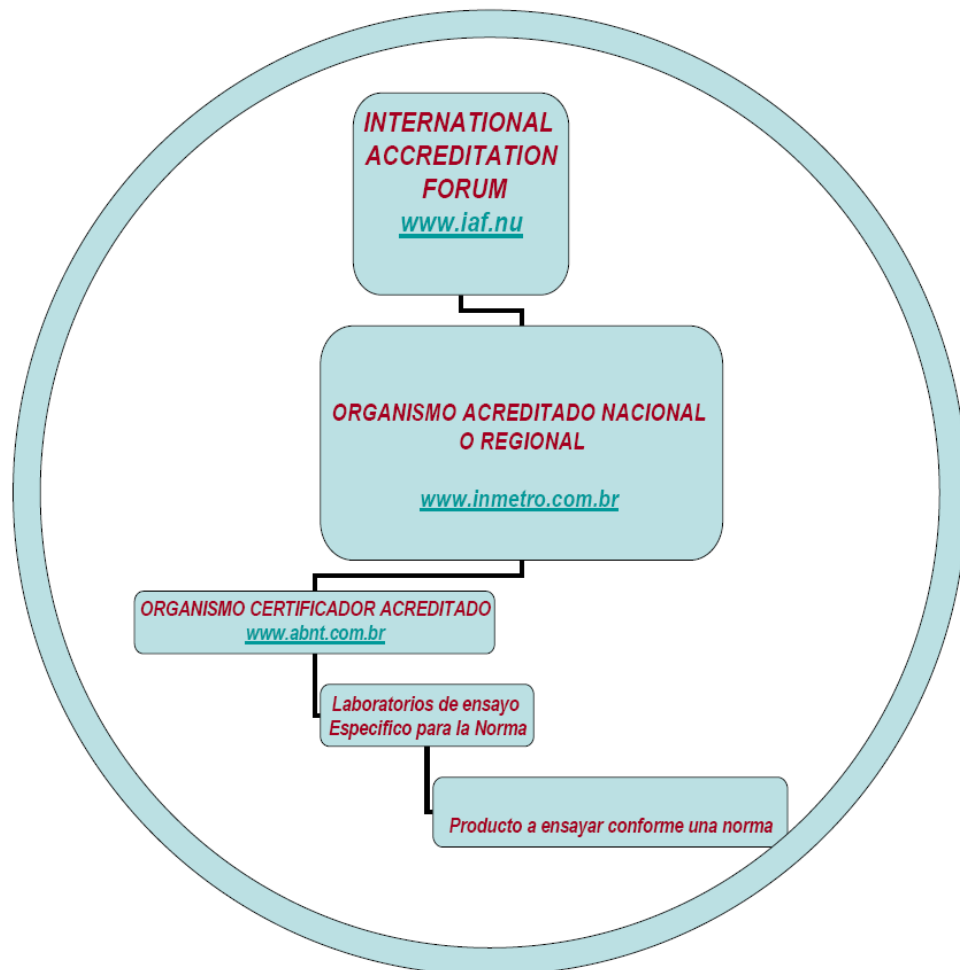
otras auditorías conforme el SGSI ISO 27.001, comprueban que el impacto de un incidente o desastre de origen físico-ambiental sobre un Data Center determina de manera concurrente una pérdida sobre todos los activos críticos, lo cual se acentúa por la mayor concentración de mips, y Gbytes por m3 de Data Center.

En éstos análisis, y sobre casos evaluados sólo en América Latina, la ventana de recuperación completa (Plan de Contingencia + Vuelta a la Normalidad) se ha medido en no menos de 150 días, cuando se ha perdido hardware del Data Center Primario.

El retorno de la inversión en proteger con Sala Cofre los activos críticos del Data Center se puede determinar mediante diferentes tipos de análisis. Por ejemplo, al medir el valor económico de la reducción del "loss profit" al minimizar el tiempo de Vuelta a la Normalidad (unos pocos días con Sala Cofre, en lugar de varios meses, sin Sala cofre)

La complementación de un Data Center con Sala Cofre, y un Cold Site o hot site con espejamiento parcial es la ecuación más costo-efectiva en estrategias continuidad.

Proceso de certificación de Salas cofre en Mercosur:



CÓMO ES EL PROCEDIMIENTO PARA CERTIFICAR:

Para que un producto "x" pueda ser Certificable, debe existir una NORMA para ensayarlo y un PROCEDIMIENTO REGISTRADO en un ORGANISMO CERTIFICADOR ACREDITADO que debe ser parte del INTERNACIONAL ACCREDITATION FORUM (www.iaf.nu) PARA EL "SCOPE SALA COFRE".(ES IMPORTANTE QUE SEA ACREDITADO PARA EL SCOPE SALA COFRE PORQUE QUE SEA ACREDITADO PARA UN PROGRAMA ISO 9000, POR EJEMPLO, GARANTIZA UN PROCEDIMIENTO DE CALIDAD PERO NO SE OCUPA DE LA PERFORMANCE DEL PRODUCTO, EN ESTE CASO UNA SALA COFRE)

Si este procedimiento no está registrado y aprobado no existe posibilidad de tener una Certificación reconocida mundialmente y de validez legal.

Para Iniciar un proceso de Certificación es preciso que el interesado presente un prototipo conforme el objeto de test de la norma para Salas Cofre (EN-1047-2 o

NBR/ABNT 15.247) Si el prototipo pasa con éxito los ensayos, el Organismo Certificante hace las comprobaciones y auditorías correspondientes para luego emitir la Certificación con su correspondiente vigencia.

En el Caso de la Certificación para Salas Cofres, la norma no sólo exige que el prototipo pase el ensayo sino que los procesos de fabricación sean normalizados conforme ISO 9001-2000, y que este programa de calidad incluya, proyecto, fabricación, montaje y mantenimiento de Salas Cofre e Infraestructura para Data Center.

A. En síntesis, la Certificación es el documento solicitado todas las licitaciones y también en este pliego, porque garantiza el nivel de protección necesario y porque representa la Garantía por la cual será responsable el oferente-proveedor

B. Para la construcción tradicional no existe Certificación posible.

C. Presentar cualquier otro documento que no sea emitido por un Organismo Certificador Acreditado para o scope sala cofre, y que no sea miembro del Internacional Accreditation Forum, le resta validez y llevará al usuario a no contar con el nivel de protección esperado de una Sala Cofre. Asimismo, transfiere al dador de ese "documento" la responsabilidad por los perjuicios ocasionados al Cliente, descritos en las Leyes de Defensa al Consumidor, en lo que respecta a Publicidad Engañosa, conforme legislación de cada país, y al impacto sobre el negocio por negligencia.

LISTADO DE ORGANISMOS DE ACREDITACION MIEMBROS DEL INTERNATIONAL ACCREDITATION FORUM, CON CAPACIDAD PARA RESPALDAR A ORGANISMOS CERTIFICANTES DE NORMAS:

International Accreditation Forum (IAF) Multilateral

Recognition Arrangement (MLA) Signatories

Diseño de un sistema de gestión de Planes de Contingencia y Gestión de Riesgos basado en Análisis de Procesos de Negocio

Autor: Lic. Domingo Donadello

Location	Signatory	MLA & Date Admitted
Argentina	Organismo Argentino de Accreditation (OAA)	QMS 17 Sep 2005 EMS 17 Sep 2005 Product 17 Sep 2005
Australia & New Zealand	Joint Accreditation System of Australia and New Zealand (JAS-ANZ)	QMS 22 Jan 1998 EMS 9 Oct 2004 Product 9 Oct 2004
Austria	Federal Ministry for Economic Affairs and Labor (BMWA)	QMS 25 Sep 2003 EMS 9 Oct 2004 Product 9 Oct 2004
Belgium	BELAC	QMS 29 Sep 1999 EMS 9 Oct 2004 Product 9 Oct 2004
Brazil	National Institute of Metrology, Standardization and Industrial Quality (INMETRO)	QMS 23 Aug 1999 EMS 8 Dec 2005
Canada	Standards Council of Canada (SCC)	QMS 22 Jan 1998 EMS 9 Oct 2004 Product 9 Oct 2004
China	China National Accreditation Service for Conformity Assessment (CNAS)	QMS 29 Oct 1999 EMS 9 Oct 2004
Czech Republic	Czech Accreditation Institute, (Český Institut pro Akreditaci, o.p.s.) (CAI)	QMS 29 Sep 1999 EMS 9 Oct 2004 Product 9 Oct 2004

Los Organismos Acreditantes miembros del International Accreditation Forum, con procedimientos y normas de ensayo para Salas Cofres son:

1) DAR (Alemania) bajo la Euronorma EN-1047-2 Certificada por el European Certification Board-Security y DAR;

2) en el MERCOSUR, es el INMETRO (con base en Brasil) conforme la norma NBR/ABNT 15.247 que incluye y agrega ensayos adicionales respecto de la EN-1047-2.

ANTECEDENTES LOCALES, REGIONALES E INTERNACIONALES

En los anexos entregamos más información detallada, pero a modo de resumen podemos mencionar que en el mundo existen más de dos mil Salas Cofre Certificadas conforme la norma EN-1047-2, y en América Latina existen ya más de doscientas, Certificadas conforme EN-1047-2 y NBR/ABNT 15.247, de las cuales seis ya están en Argentina.

La más reciente instalada fue para el ANSES, mediante licitación pública nacional, y la más grande pertenece a la AFIP mediante licitación pública Internacional (VER ANEXO ANALISIS DEL BID), en ambos casos certificadas por la EN-1047-2 y la ABNT 15.247.

El tamaño promedio de las Salas Cofre instaladas en América Latina varía según el país y el tamaño de las empresas.

Por ejemplo, en Brasil el promedio de superficie por Sala Cofre supera los 200m², en Argentina es de 120 m², en Venezuela 90m², en Chile 30m², entre otros.

Es importante destacar que las propiedades de modularidad de la Sala Cofre, más la ingeniería de proyecto normalizada para esta industria permite que las dimensiones y hasta la localización de la misma, no sea un problema durante el ciclo de vida del Data Center.

Tres de cada cinco salas cofre han sido ampliadas o modificadas con el Data Center en operación.



Características de la Salas Cofre IT Modulares-Especificación básica

Es un conjunto ambiental modular ignífugo y refractario, hermético con características específicas para protección de equipamientos electrónicos, data centers, medios magnéticos, papeles y demás portadores de datos, certificada conforme Euronorma EN 1047/2 y NBR- 15247 bajo el procedimiento ABNT/Inmetro pe047.01.

La Sala Cofre está Certificada para ser absolutamente estanca al agua exterior al cumplir con la norma NBR 10897, que es uno de los ensayos de teste incluidos dentro de la norma NBR 15.247 (Presentamos la Certificación correspondiente).

La Sala Cofre, incluidas su puerta, es absolutamente estanca a los gases, penetración de polvo y/o agua presurizada cumpliendo con la categoría mínima IP 66 de la norma EN 60529.

Presentamos la certificación correspondiente. Se deberá probar la estanqueidad del ambiente luego del montaje según procedimientos ASTM E779 y NFPA 2001 Anexo A. Estos ensayos están incluidos dentro de la Certificación ABNT 15.247

Las puertas de la Sala Cofre están diseñadas a prueba de vandalismo y cumplen con la norma DIN V 18103 categoría ET3 y/o norma EN 1627 categoría WK4.

La SalaCofre es inmune a impulsos electromagnéticos, radiofrecuencias y campos magnéticos por los materiales y su ingeniería de instalación, conformando una Jaula de Faraday.

Un fuego externo de 1.100 °C durante 60 minutos no generará una temperatura mayor a 75 °C y una humedad relativa mayor al 85% en el interior de las Salas Cofre, conforme se garantiza al presentar las Certificaciones conforme EN-1047-2 y NBR 15.247, que incluyen el ensayo de teste contra fuego.

La Sala Cofre es un conjunto ambiental certificado, compuesto por elementos modulares para piso, techo y laterales, que posee una puerta de acceso con cerramiento automático, un sistema de blindaje que permite el pasaje de cables y tuberías blindados, y un sistema de sellado de juntas para proporcionar flexibilidad sin perder estanqueidad, en caso de presión extrema.

Los perímetros y muros tradicionales son construcciones compuestas por materiales individualmente testeados, cuya garantía como ambiente no es posible determinar, y que tienen comportamiento HIGROFUGO, lo cual en caso de contacto con el agua aumentan su peso, y modifican sus propiedades.

Los paneles que componen la Sala Cofre no absorberán los líquidos y flujos de aguas provenientes de roturas de caños o sistemas de combate de incendio del edificio. La tecnología Aceco – Lampertz, es totalmente NO HIGROFUGA.

Además de ser presentada la documentación original que acredita el cumplimiento de las certificaciones exigidas, presentaremos al finalizar la ejecución del proyecto el Sello de Seguridad emitido por la Asociación Brasileira de Normas Técnicas y por el inmetro que garantiza el cumplimiento de todos los ensayos listados en la norma NBR 15.247 y el procedimiento pe047.01, con las normas de calidad para proyecto y manutención de infraestructura de Salas Cofre.

La modularidad de la Sala Cofre ofrecida admite alteraciones en sus dimensiones iniciales y el traslado de lugar sin pérdida de material, caracterizando así la completa flexibilidad y preservación de la inversión, con bajos costos y riesgos en caso de modificaciones del CPD.

Puerta de Acceso a la Sala-Cofre

El acceso es único a través de la puerta compuesta por capas de acero y aislantes. El cerramiento posee traba automática, con accionamiento electromecánico para control de acceso, pero totalmente libre para la salida, (función anti-pánico que permita a las personas salir de la sala aunque se encuentre la puerta trancada). Para acceso en caso de contingencia deberá tener "by-pass" mecánico por llave.

La puerta posee sellados herméticos de elastómero y burletes intumescentes para altas temperaturas, impidiendo la entrada de calor, agua y gases corrosivos. La puerta de entrada está certificada como parte del conjunto ambiental "Sala Cofre Certificado", anteriormente especificado.

La puerta será operada normalmente cerrada, y cuando estuviese abierta, se accionará su cierre sin intervención humana a través de la señal de alarma recibida en el panel de control. El espacio de luz de la puerta es de un mínimo 2000 mm x 950 mm.

Blindaje para pasaje de cables y cañerías:

Se entregarán la cantidad estimada de blindajes necesarios para gerenciar los cables entrantes y salientes de la Sala Cofre de acuerdo a la tabla de equipos informada en el diseño del lay-out, que incluye los dispositivos de infraestructura dentro de la sala cofre, admitiendo una tasa de crecimiento del 30%. El detalle de ubicación de los mismos, será funcional a la aprobación del lay-out definitivo.

El sistema es modular, permitiendo el reacomodamiento de cables siempre que fuese necesario, sin interferencia en la operación y manteniendo el nivel de protección del ambiente de la sala.

El blindaje es parte del ensayo de teste del conjunto y está certificado como parte del mismo.

Iluminación de la Sala

La iluminación interna de la Sala Cofre está provista de fuentes electrónicas de alta frecuencia y seguridad. El nivel de iluminación será de, aproximadamente, QUINIENTOS (500) lux.

El proyecto incluye una unidad autónoma para luz de emergencia, que deberá garantizar su funcionamiento por un período mínimo de SESENTA (60) minutos.

Una vez instalada la Sala Cofre, por fases, en una fase completa, se procederá a ejecutar el Test de Estanqueidad final que se realiza "on site"

La infraestructura Termomecánica, de Potencia, Cableado, Mobiliario Técnico y sistemas de control ambiental y de seguridad física, junto con las tareas civiles complementarias, serán especificadas conforme el proyecto a diseñar para cada caso, aplicando políticas de seguridad, y normas de infraestructura, controladas mediante los procedimientos de calidad ISO 9001-2000 para Proyecto, Instalación y mantenimiento de Salas Cofre e Infraestructura de Data Centers exigida al proveedor de la Sala Cofre.