PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERIA

MAESTRÍA EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN

CONSTRUCCIÓN DE UN PLAN DE CONTINUIDAD DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN PARA UNA EMPRESA DE SEGUROS

CADENA ANDRADE INGRID KATIUSKA

TESIS PRESENTADA PREVIO A LA OBTENCIÓN DEL TITULO DE

MAGISTER EN GERENCIA DE TECNOLOGÍAS DE

INFORMACION

QUITO, 2012

AGRADECIMIENTOS

A mi familia que es el pilar que me apoya y me ayuda a seguir adelante luchando por mis objetivos, por su paciencia y compresión para poder finalizar con mi maestría.

A mi director el Ing. Alberto Pazmiño por todo su tiempo y guía para poder desarrollar este tema y a mis revisores por su aporte para la mejora del proyecto.

Y la lista interminable de amigos y profesores que contribuyeron para que pueda alcanzar un objetivo más.

INDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

Introducción

Son varias las causas por las que los servicios de tecnología de información de una empresa pueden quedar fuera de línea, estas causas pueden ser tanto internas como externas a la empresa. Entre las causas internas podemos tener errores en la administración de los sistemas de información, errores en la configuración de equipos, difusión de software dañino, caída de sistemas por agotamiento de recursos, etc. y entre las causas externas podemos mencionar desastres naturales, ataques terroristas, ataques desde el exterior de software dañino, etc. Cada una de estas causas puede afectar de manera total o parcial un servicio de tecnología de información y con la falta de estos servicios los procesos de la empresa que dependen de estos servicios pueden detenerse por un corto o largo tiempo dependiendo de la magnitud del daño en el servicio de tecnología.

Cualquiera sea la causa de la suspensión de un servicio de tecnología, genera pérdida de recursos así como malestar entre los clientes internos y proveedores por falta de herramientas y servicios para la ejecución normal de sus actividades, así como el malestar que puede generar en los clientes externos los cuales verán un deterioro en el servicio entregado al no funcionar adecuadamente el proceso de atención al cliente por la falta de una de las herramientas tecnológicas necesarias, si no existe un adecuado plan de continuidad de los servicios.

En nuestro país la construcción de un plan de continuidad de negocio puede ser un proceso muy difícil debido a varios factores como falta de conocimiento y experiencia sobre todo en las pequeñas y medianas empresas en las cuales los recursos de TI son limitados, siendo estas las razones por las cuales son escasas las empresas que tienen la visión de trabajar en un plan de continuidad. La mayoría de compañías trabaja en una cultura de reacción antes que prevención, con la concepción que un plan de continuidad es solamente para empresas grandes, pero las fallas y amenazas en los servicios de TI son un riesgo latente para todas las empresas y las consecuencias de estas depende de los mecanismos de prevención y recuperación con los que cuente la empresa.

1. Capítulo I: Marco Teórico

En el primer capítulo se revisarán temas generales de concepto que son necesarios conocer para el desarrollo del proyecto, los temas que se revisarán van desde tecnologías de información (TI), servicios basados en TI, pasando por infraestructura de TIC para una empresa de seguros y los riesgos asociados a los servicios de TI, finalizando con estándares de seguridad de información y la elaboración de planes de continuidad para servicios de TI.

1.1. Tecnologías de Información y comunicaciones

Las tecnologías de información y comunicación son un conjunto de recursos que permiten almacenar, manipular, administrar y transmitir información numérica, textual, audible, multimedia a través de computadores, programas informáticos, redes de comunicación y dispositivos que combinan la electrónica, computación y telecomunicaciones.

Las tecnologías de información y comunicaciones (TIC) pueden ser agrupadas en:

- Redes: en este grupo tenemos una variedad de equipos que permiten la comunicación como la telefonía fija y móvil, banda ancha, canales virtuales etc.
- Hardware: dispositivos que permiten el almacenamiento y procesamiento de datos, aplicaciones y servicios como servidores, teclados, computadores, etc.
- Software: son las aplicaciones informáticas que permiten manejar los datos.
- Equipamiento auxiliar: son equipos o dispositivos que apoyan la gestión de las tecnologías de información como fuentes de poder, equipos de climatización, etc.
- Servicios: estos han ido evolucionando según ha ido creciendo la tecnología, los servicios son aquellos que se pueden brindar y ayudan para la gestión de datos.

1.1.1. Características de las Tecnologías de Información

Entre las características de las tecnologías de información podemos decir que existen 5 generales que son:

1. Interactividad: Las tecnologías de información permiten la interacción de sus usuarios, lo que los permite pasar de un papel pasivo para tener un rol activo.

2. Instantaneidad: Esta característica se refiere a la posibilidad de poder recibir información casi de manera instantánea.

3. Interconexión: Esta característica permite que podamos comunicarnos con personas que se encuentran al otro lado del mundo, además que podamos acceder a información que se encuentra almacenada a kilómetros de distancia sin tener que desplazarnos.

4. Digitalización: La característica de la digitalización hace referencia a la transformación de la información analógica en códigos numéricos, lo que favorece la transmisión de diversos tipos de información por un mismo canal, como son las redes digitales de servicios integrados. Esas redes permiten la transmisión de videoconferencias o programas de radio y televisión por una misma red.

5. Diversidad: Otra característica es la diversidad de esas tecnologías que permiten realizar un sinfín de funciones.

1.1.2. Ventajas y Desventajas de las Tecnologías de Información

Son varias las ventajas y desventajas que presentan las tecnologías de información, a continuación nombraremos algunas de ellas.

Ventajas:

- Apoyar a las empresas para presentar y vender sus productos a través de la Internet.
- Permitir el aprendizaje interactivo y la educación a distancia.
- Ofrecer nuevas formas de trabajo, como teletrabajo
- Permitir el acceso al flujo de conocimientos e información de forma ágil.

Desventajas:

- Los beneficios de las tecnologías de información no están distribuidos de manera equitativa, lo que genera un tipo de pobreza para los países con mayor acceso a las tecnologías de información de los países con menor acceso.
- Falta de privacidad
- Disminución de puestos de trabajo

1.2. Servicios basados en Tecnologías de Información

Actualmente existe un gran número de servicios basados en Tecnologías de Información, estos varían en cada organización dependiendo de varios factores como tamaño, presupuesto, etc.

Para poder contar con un mejor control sobre estos servicios es necesario tener un catálogo de servicios de tecnologías de información.

El catálogo de servicios es un listado de los servicios que el departamento de TI brinda a los usuarios y/o clientes y que incluye ciertas características de los mismos.

Los beneficios de un catálogo de servicios de TI son:

- Mejora el desarrollo de los servicios
- Ayuda a identificar riesgos de operación en un ambiente cada vez más regulado.
- Ayuda a construir una comunicación interna efectiva y a ilustrar las responsabilidades de cada persona.
- Permite identificar servicios adicionales que pueden ser de interés para el usuario.

Un catálogo de servicios debe tener cumplir con las siguientes directrices para su elaboración:

- El servicio debe estar detallado de forma clara de manera que las personas que no son técnicas puedan entenderlo.
- Agrupar los servicios en conjuntos que sean fáciles de identificar y entender.
- Debe indicar la disponibilidad de cada servicio (horarios especiales, feriados, etc.).

- Debe indicar el tiempo de entrega de cada servicio.
- Debe ser creado y debe ser actualizado periódicamente.

Bajo las directrices indicadas anteriormente se construyó el catálogo de servicios de tecnología de información para una empresa de seguros en Ecuador.

Grupo Servicio	Servicio	Definición	Disponibilidad	Tiempo Entrega	Tiempo Ejecución
Sistemas de información	Solicitud de información de los sistemas SIS y KREA	Generación y entrega de información de las aplicaciones de gestión SIS y KREA (reportes) que no se pueden generar a través de herramientas de usuario disponibles	8x5	4 dl	12h
Sistemas de información	Instalación, configuración y acceso a los sistemas de información SIS, KREA y Datamart	Instalación, configuración y acceso a software de gestión SIS, KREA y Datamart	8x5	1 dl	2h
Sistemas de información	Eventualidades con el sistema de información KREA	Eventualidades con el software de gestión KREA	8x5	2 dl	2h
Sistemas de información	Eventualidades con el sistema de información SIS	Eventualidades con el software de gestión SIS	8x5	2 dl	4h
Sistemas de información	Eventualidades con el sistema de información Datamart	Eventualidades con el software de gestión Datamart	8x5	15 dl	30h
Servicios de apoyo	Creación y configuración de cuentas de correo electrónico	Creación y configuración de cuentas de correo electrónico	8x5	1 dl	2h

Grupo Servicio	Servicio	Definición	Disponibilidad	Tiempo Entrega	Tiempo Ejecución
Servicios de apoyo	Eventualidades de correo electrónico	Eventualidades con el servicio de correo electrónico	24x7	1 dc	24h
Servicios de apoyo	Servidor de archivos	Acceso y configuración al servidor de archivos de la organización (carpetas compartidas N, M y T)	8x5	30 min	30 min
Servicios de apoyo	Conexión a impresora	Instalación y configuración de impresoras	8x5	2 h	2 horas
Servicios de apoyo a las aplicaciones de gestión	Instalación, configuración y acceso a aplicaciones externas	Instalación, configuración y acceso a aplicaciones de entidades externas (gubernamentales, proveedores, aliados estratégicos, entidades financieras)	8x5	2 dl	2h
Servicios de apoyo a las aplicaciones de gestión	Eventualidades con aplicaciones externas	Eventualidades con aplicaciones de entidades externas (Dim formularios, file laboral, software para envío de archivos a bancos, etc)	8x5	8 dl	1h
Servicios de apoyo a las aplicaciones de gestión	Instalación, configuración y acceso a aplicaciones de gestión	Instalación y configuración de aplicaciones de gestión como herramientas de ofimática, audio y video, etc.	8x5	2 dl	3h
Servicios de apoyo a las aplicaciones de gestión	Eventualidades con aplicaciones de gestión	Eventualidades con aplicaciones de gestión como herramientas de	8x5	3 dl	3h

Grupo Servicio	Servicio	Definición	Disponibilidad	Tiempo Entrega	Tiempo Ejecución
		ofimática, audio y video, etc.			
Servicios de proveeduría de herramientas de TI	Proveeduría de Periféricos	Adquisición de periféricos permanentes y temporales como mouse, teclado, monitor, pen drive, impresoras.	8x5	3 dl	4h
Servicios de proveeduría de herramientas de TI	Proveeduría de equipos de computación*	Solicitud de equipos permanentes y temporales de computación como laptops, impresoras de alto rendimiento, PC's	8x5	8 dl	6h
Servicios de proveeduría de herramientas de TI	Proveeduría software*	Adquisición de software de aplicaciones (herramientas de ofimática, audio y video, etc)	8x5	8 dl	4h
Servicios de apoyo al puesto de trabajo	Instalación de un puesto de trabajo nuevo**	Instalación de un puesto de trabajo nuevo con equipos de computación y/o red.	8x5	15 dc	50h
Servicios de apoyo al puesto de trabajo	Instalación o reubicación en un puesto de trabajo existente	Instalación, reubicación o adecuación en un puesto de trabajo existente con equipos de computación y/o red.	8x5	2 dl	4h
Servicios de apoyo al puesto de trabajo	Eventualidad de pérdida de conexión	Cuando el equipo ha dejado de estar conectado a la red de cable o inalámbrica	8x5	1 dl	3h

Grupo Servicio	Servicio	Definición	Disponibilidad	Tiempo Entrega	Tiempo Ejecución
Servicios de apoyo al puesto de trabajo	Eventualidad con equipos de computación o periféricos*	Cuando el equipo de computación o periféricos (PC de escritorio, laptop, impresora, mouse, teclado, etc.) ha dejado de funcionar	8x5	2 dl	3h
Servicio de información y comunicación	Acceso a la red corporativa	Altas, bajas y modificaciones para la red (cable o inalámbrica) de la organización	8x5	1 dl	1h
Servicio de información y comunicación	Servicios Web	Acceso a la página Web corporativa (intranet)	8x5	1 dl	1h
Servicio de información y comunicación	Acceso a Internet	Acceso a Internet por primera vez o solicitud de un acceso especial a una página de Internet	8x5	1 dl	1h
Servicio de información y comunicación	Eventualidades con Internet	Eventualidades con el servicio de Internet	24x7	1 dc	12h
Servicio de información y comunicación	VPN	Instalación, configuración, acceso y eventualidades con la VPN	8x5	1 dl	2h
Desarrollo de proyectos con uso de las TIC	Consultoría para levantamiento de EF	Guía, revisión y aprobación en el levantamiento de Especificaciones Funcionales (EF)	8x5	1 dl	2h
Capacitación	Capacitación	Capacitación a usuarios en el manejo de los sistemas de información SIS y KREA	8X5	2 dl	1h30

Grupo Servicio	Servicio	Definición	Disponibilidad	Tiempo Entrega	Tiempo Ejecución
Servicios de construcción e implementación de sistemas de información	Desarrollo de sistemas de información (mejoras y/o adecuaciones)	Adaptación de mejoras y/o adecuaciones a los sistemas de información SIS y KREA.	8x5	30 dl	120h
Servicios de construcción e implementación de sistemas de información	Desarrollo de sistemas de información (funcionalidades nuevas)	Construcción de nuevas funcionalidades en los sistemas de información SIS y KREA.	8x5	3 m	240h
Servicios de construcción e implementación de sistemas de información	Implementación de cambios en los sistemas de información en el ambiente de pruebas	Implementación y configuración de cambios en los sistemas de información en un ambiente de QA.	8x5	2 dl	6h
Servicios de construcción e implementación de sistemas de información	Pruebas de Funcionalidad en sistemas de información	Realización de pruebas de funcionamiento y adaptabilidad de sistemas de información según un plan de pruebas	8x5	3 dl	8h
Servicios de construcción e implementación de sistemas de información	Implementación y versionamiento de sistemas de información en producción	Instalación y versionamiento de sistemas de información en el ambiente de producción	8x5	5 dl	4h
Servicios de construcción e implementación de sistemas de información	Creación de ambientes de desarrollo, pruebas y producción de sistemas de información	Creación de ambientes (repositorio de componentes de software y base de datos) de desarrollo, pruebas y producción de sistemas de información	8x5	8 dl (con hardware disponible)	8 dl

Grupo Servicio	Servicio	Definición	Disponibilidad	Tiempo Entrega	Tiempo Ejecución
Servicios de construcción e implementación de sistemas de información	Actualización de ambientes	Actualización de base de datos y ambientes de desarrollo de software y pruebas de calidad.	8x5	10 dc	10h

Tabla 1 – 01: Catálogo de Servicios de Tecnología de Información para una Empresa de Seguros en Ecuador [A]

Leyenda del cuadro:

***** Si la solicitud es de una localidad, agregar 1 día laborable más al tiempo de entrega.

** Si la solicitud es de una localidad, agregar una semana adicional al tiempo de entrega.

abreviatura	Representación
M	Meses
Dc	días calendario
Dl	días laborables
H	Horas
Min	Minutos
8x5	8 horas al día, 5 días laborables a la semana
24x7	24 horas al día, 7 días a la semana

1.3. Infraestructura de TIC de una empresa de Seguros en Ecuador

La infraestructura tecnológica en una empresa varía de acuerdo a los servicios de TIC de los cuales dispone la organización, querer estandarizar dicha infraestructura resultaría casi imposible pero al enfocarnos en una empresa de Seguros en Ecuador podemos levantar la infraestructura según los servicios que maneja la organización.

La infraestructura de una empresa de Seguros en Ecuador podemos clasificarla en 5 grupos que son:

- **Hardware:** son el conjunto de componentes que conforman la parte física de la infraestructura de TI.
- **Software:** es un conjunto de programas que hacen funcionar el hardware.
- **Comunicaciones:** son todos los elementos que permiten conformar una red de comunicación por la cual se transmiten datos.
- **Datos:** es uno de los activos más valiosos de la organización y corresponde a la información resultado de la gestión de la empresa.
- **TTHH:** es el equipo humano que opera en el área de TIC.

En el anexo adjunto infraestructura.xls se puede observar la infraestructura que soporta los servicios de TIC tanto de forma general como de forma detallada, además de la clasificación de los servicios de TI en 3 categorías:

- **Críticos:** servicios que soportan algún proceso crítico de la organización y que puede influir en la rentabilidad (servicios resaltados en rojo).
- **Complementarios:** servicios que apoyan a la gestión de los procesos y que son necesarios para la consecución de los mismos (servicios resaltados en amarillo).
- **Suplementarios:** servicios que no tienen un impacto directo en los procesos críticos de la organización (servicios resaltados en verde).

1.4. Riesgos de los Servicios de Tecnologías de Información y Comunicaciones

Riesgo es la probabilidad de que un evento ocurra y genere consecuencias adversas; los servicios de tecnologías de información también están expuestos a riesgos por lo que es importante realizar un adecuado análisis y gestión riesgos.

El objetivo principal para el área de TI debe ser cuidar las características que definen la seguridad de la información:

- **Disponibilidad:** asegura que los usuarios autorizados tienen acceso a la información cuando lo requieran.

- **Integridad:** asegura que la información y sus métodos de procesamiento son exactos y completos

- **Confidencialidad:** consiste en asegurar que sólo quienes estén autorizados pueden acceder a la información.

- **Autenticidad:** asegura que el contenido de los datos y su fuente de origen son auténticos.

Por lo que se puede concluir que seguridad es la capacidad de las redes o de los sistemas de información de resistir con cierto grado de confianza las eventualidades que comprometan la disponibilidad, confiabilidad e integridad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen, tomando en cuento el establecimiento de métodos de autenticación.

1.4.1. Análisis de Riesgos

Los objetivos de un análisis de riesgos son:

- Reducir los riesgos para garantizar de manera razonable con un costo eficiente el alcance de los objetivos estratégicos de TI y por lo tanto del negocio.

- Identificación y amenazas de las vulnerabilidades.
- Identificación de probabilidades y consecuencias.
- Determinación de niveles aceptables de riesgo

En el análisis de riesgos debemos valorar 4 tipos de riegos:

- **Riesgo inherente:** referente a la valoración del riesgo sin ningún tipo de control.
- **Riesgo residual:** referente a la valoración del riesgo que persiste luego de haber establecido medidas de control.
- **Riesgo repercutido:** toma en cuenta el valor propio del activo combinándolo con la degradación causada por una amenaza y la frecuencia estimada de la misma.
- **Riesgo acumulado:** toma en cuenta el valor propio de un activo y el valor de los activos que dependen de él, combinándolo con la degradación causada por una amenaza y la frecuencia estimada de la misma.

La evaluación del riesgo resulta de la relación entre la probabilidad de que el riesgo ocurra con el impacto causado producto de la ocurrencia del riesgo.

Riesgo = TABLA **[Probabilidad**, **Impacto]**

En la matriz de riesgos se puede identificar la severidad del riesgo según la probabilidad de ocurrencia y el impacto del mismo, como se puede apreciar en la siguiente tabla:

Probabilidad		**Impacto**				
		Insignificante	**Menor**	**Moderada**	**Mayor**	**Catastrófica**
		1	2	3	4	5
Casi Cierto	5	Alto	Alto	Extremo	Extremo	Extremo
Probable	4	Moderado	Alto	Alto	Extremo	Extremo
Posible	3	Bajo	Moderado	Alto	Extremo	Extremo
Improbable	2	Bajo	Bajo	Moderado	Moderado	Extremo
Raro	1	Bajo	Bajo	Moderado	Alto	Alto

Tabla 1 – 02: Matriz de Riesgos

De manera que si probabilidad de ocurrencia es “improbable” y el impacto es “mayor” se expresará:

Riesgo = TABLA **[**improbable, mayor**]**

Riesgo = moderado

Luego de haber realizado el análisis de riesgos es necesario implementar una serie de controles para conocer, prevenir, impedir, reducir o controlar los riesgos identificados; este proceso se llama **gestión de riesgos.**

Hay que tener claro que ningún proceso de gestión de riesgos brindara una seguridad absoluta, pero nos permitirá conocer y minimizar el riesgo según las necesidades de la organización.

1.4.2. Metodologías para el Análisis de Riesgos

Existen múltiples metodologías para el análisis de riesgos, pero independiente del método que se elija, es necesario realizar el análisis para determinar los riesgos y establecer los controles necesarios, lo más recomendable para realizar el análisis de riesgos es tomar un modelo de seguridad como referencia para tener una mayor certeza que se han considerado todos los escenarios posibles.

Entre las metodologías para el análisis de riegos podemos mencionar algunas como:

- **MARION[1]:** A principios de los ochenta el CLUSIF[2] desarrolló esta metodología, cuyo objetivo fue hacer un estándar para analizar la situación ante veinte y siete factores de riesgo que están ponderados con un arreglo a criterios de gravedad.

- **MEHARI[3]:** fue desarrollado por el mismo CLUSIF y clasifica los riesgos en 2 grupos:
  - ✓ Según sus causas en accidentes, errores y actos mal intencionados.

[1] **M**éthodologie d’**A**nalyse de **R**iesques **I**nformatiques **O**rientée par **N**iveaux

[2] **CLU**b de la **S**écurité des **S**ystémes d’**I**nformation **F**rancais

[3] **ME**thode **H**armonisée d’**A**nalyse des **RI**sques

- ✓ Según la características de la seguridad de la información que vulnera (confidencialidad, integridad y disponibilidad).

- **McCumber:** Expuesto en 1991 por John R McCumber en la 14th National Computer Security Conferen bajo el patrocinio del National Institute of Standards and Technology/National Computer Security Center.

  Este modelo abarca 3 dimensiones que son:

  - ✓ Estados de la información: proceso, almacenamiento y transporte.
  - ✓ Características de la información: disponibilidad, integridad, confidencialidad.
  - ✓ Medidas de seguridad: tecnológicas, normas y procedimientos, formación y entrenamiento.

  En este modelo representa un cubo formado por las 3 dimensiones y divido en celdas que son una medida de seguridad que se implementará según la celda en la cual la vulnerabilidad descubierta sea encasillada.

- **MAGERIT[4]:** Fue desarrollado a finales de los noventa por el Consejo Superior de Administración Electrónica y se aplica ampliamente por la Administración Española.

  Magerit en su versión 2 está distribuido en 3 libros que son:

  - ✓ Método: es una guía que tiene 3 ángulos que abarcan uno (capítulo 2) los pasos para realizar un análisis del estado del riesgo y gestionar su mitigación, dos (capítulo 3) describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos y tres (capítulo 4) como aplicar la metodología en el desarrollo de un sistema de información.
  - ✓ Catálogo de Elementos: facilita la realización del proyecto y estandariza la terminología y criterios permitiendo integrar análisis realizados por diferentes equipos.
  - ✓ Guía de Técnicas: busca describir las técnicas utilizadas en los proyectos de análisis y gestión de riesgos

  Magerit ofrece una aplicación para el análisis y gestión de riesgos de un Sistema de Información llamada PILAR.

[4] **M**etodología de **A**nálisis y **GE**stión de **R**iesgos de los Sistemas de **I**nformación de las Adminis**T**raciones Públicas

1.5. Estándares Internacionales para la Seguridad de la Información

En este apartado se revisarán 3 estándares internacionales para la seguridad de la información que son ISO/IEC 27002, BCI (Business Continuity Institute) y Oficial (ISC)[2] guía para el CISSP CBK.

1.5.1. ISO/IEC 27002

Existen varios estándares ISO/IEC 27000 desarrollados y en fase de desarrollo, que proporcionan un marco de gestión de la seguridad de la información para todo tipo de organizaciones.

De la familia de los estándares ISO/IEC 27000 mencionaremos 2 el 27001 y 27005 y detallaremos el 27002.

El estándar ISO/IEC 27001 nos da un marco de referencia para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de información, adoptando el modelo del proceso PDCA (planear, hacer, chequear, actuar).

El estándar ISO/IEC 27005 es una guía que ayuda en la gestión del riesgo en el sistema de seguridad de información.

El estándar ISO/IEC 27002 fue creado para proporcionar recomendaciones de las mejores prácticas en la gestión de la seguridad de la información, y consta de once secciones principales:

1. **Política de Seguridad de la Información:** En esta sección se definen como obligatorias que las políticas de seguridad y procedimientos internos de la organización estén documentados y que permitan su actualización y revisión por parte de un Comité de Seguridad.

2. **Organización de la Seguridad de la Información:** Esta sección establece el marco formal de seguridad que debe integrar una organización, proporciona un foro para revisar y aprobar las políticas de seguridad y asignar los roles de seguridad.

3. **Gestión de Activos de Información:** En esta sección para la realización del análisis de riesgos se creará un inventario de activos que deben ser administrados y controlados con base en ciertos criterios de clasificación y etiquetado de información, de acuerdo con su nivel de confidencialidad. Permite determinar quién es el responsable de que activo en la organización.

4. **Seguridad de los Recursos Humanos:** Esta sección se refiere a establecer las responsabilidades y controles necesarios en materia de la seguridad de la información hacia las personas que operan los activos de información. Estas responsabilidades deben ser establecidas desde la vinculación del personal a lo largo de su permanencia en la organización.
5. **Seguridad Física y del entorno:** En esta sección el objetivo es identificar los perímetros de seguridad, para establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas tanto para empleados, proveedores o clientes.
6. **Gestión de las Comunicaciones y Operaciones:** En esta sección se integran los procedimientos de operación de la infraestructura tecnológica y los controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
7. **Control de Accesos:** El objetivo de esta sección es habilitar los mecanismos que permitan monitorear el acceso a los activos de información, estableciendo niveles de acceso para los empleados, así como niveles de acceso a la red.
8. **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información:** El objetivo de esta sección es contar con los procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.
9. **Gestión de Incidentes en la Seguridad de la Información:** El objetivo de esta sección es asegurar que las eventualidades respecto a la seguridad de la información que puedan ocurrir con los sistemas de información sean comunicados de forma oportuna para su corrección.

10. **Gestión de Continuidad del Negocio:** En esta sección se integran los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera periódica y puestos a prueba para determinar las limitaciones de los mismos.
11. **Cumplimiento (requerimientos legales):** En esta sección se establecerá los requerimientos de seguridad que deben cumplir todos los proveedores, socios y usuarios y quedarán formalizados en los contratos o convenios.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica también una guía para su implantación. El número total de controles suma 133 entre todas las secciones pero previo a la implementación de los mismos cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

El objetivo de la seguridad de los activos de información es asegurar la continuidad de las operaciones de la organización, reduciendo al mínimo los daños causados por una contingencia.

El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce como Statement of Applicability, que es la definición de los controles que aplican a la organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

La implementación del estándar ISO 17799, al igual que otros estándares no elimina el cien por ciento de los problemas de seguridad, pero permiten establecer una valoración de los riesgos a los que se enfrenta una organización en cuanto a la seguridad de la información, lo que permite administrar los riesgos en función de los recursos tecnológicos y humanos con los que cuenta la organización.

1.5.2. BCI (Business Continuity Institute)

El BCI se estableció en 1994 para obtener una guía y orientación sobre la continuidad del negocio. Aquí se establecieron las Good Practice Guidelines (GPG) que son directrices

basadas en las experiencias académico, técnico y práctico de los miembros del Instituto de Continuidad de Negocio , quienes han desarrollado un concepto de continuidad del negocio a nivel internacional.

Las GPG cubren 6 fases del ciclo de vida del Management Continuity Business (BCM) y que son definidas como Professional Practices (PP), las cuales están agrupadas en 2 prácticas de gestión y 4 prácticas técnicas.

Prácticas de Gestión:

1. **Políticas y programa de gestión:** provee las directrices de las buenas prácticas en relación a la ética y conducta de los miembros de la organización, el ciclo de vida del BCM y los 5 principios del Sistema de Gestión de la Continuidad del Negocio

2. **Incorporación de BCM en la cultura organizacional:** Integra el BCM en la estrategia de la organización y su alineación con las prioridades de las actividades.

Prácticas Técnicas:

1. **Comprensión de la organización:** Se basa en la evaluación de riesgos, aunque todas las fases son importantes, este es el pilar fundamental.

2. **Determinar la estrategia del BCM:** Se establecen las tácticas para garantizar la continuidad de las actividades que apoyan la entrega de servicios dentro del programa de continuidad del negocio.

3. **Desarrollo e implementación del BCM:** Establece las acciones y recursos necesarios para que la organización pueda gestionar una interrupción.

4. **Ejecutar, mantener y revisar el BCM:** En muy pocas ocasiones se puede realizar una prueba completa del BCM, por lo que es necesario realizar un programa de ejercicios para asegurar los aspectos que conciernen a los planes y a las personas se están cumpliendo.

1.5.3. Oficial $(ISC)^2$, guía para el CISSP CBK

La guía oficial del $(ISC)^2$ consta de 10 dominios que se describen a continuación:

1. **Seguridad de la Información y Gestión de Riesgos:** identifica los recursos de información de una organización para realizar el análisis y evaluación de riesgos, para implementar controles efectivos.

2. **Control de Acceso:** conjunto de mecanismos que crean una arquitectura de seguridad para proteger los recursos del sistema de información.

3. **Criptografía:** indica los principios, medios y métodos de camuflar la información para asegurar su integridad, confidencialidad y autenticidad.

4. **Seguridad Física (entorno):** proporciona técnicas de protección para todas las instalaciones desde el perímetro externo hasta el espacio interior, incluyendo todos los recursos del sistema de información.

5. **Diseño y arquitectura de la seguridad:** contiene los principios y estándares empleados para diseñar, supervisar y proteger los sistemas operativos, equipos, redes y aplicaciones.

6. **Continuidad del negocio y plan de recuperación de desastres:** prepara las estrategias para la conservación y recuperación de las operaciones en caso de cortes.

7. **Seguridad de redes y comunicaciones:** abarca estructura de red, métodos de transmisión, formatos de transporte, medidas de seguridad empleadas para proporcionar disponibilidad, integridad y confidencialidad, además de la autenticación para transmisiones a través de medios y redes de comunicaciones públicas y privadas.

8. **Seguridad de aplicaciones:** Describe el entorno en el cual se diseña y desarrolla el software y explica la función crítica que el software desempeña en la seguridad del sistema de información.

9. **Seguridad de operaciones:** Identifica los controles sobre hardware, medios, operadores y administradores con privilegios de acceso a cualquiera de los recursos mencionados.

10. **Leyes, regulaciones, cumplimiento e investigación:** abarca las leyes y regulaciones de delitos informáticos, así como las medidas y tecnologías empleadas en la investigación de incidentes informáticos.

1.6. Planes de continuidad de servicios de Tecnologías de Información

Día a día la tecnología se vuelve más indispensable para soportar los procesos de una organización, pero al igual que todo servicio puede estar sujeto a daños y problemas imprevistos, lo que puede ocasionar grandes pérdidas en una organización por la interrupción de estos servicios. Para mitigar estos riesgos es importante contar con plan de continuidad de servicios de tecnología de información que permita una recuperación de los servicios de una forma organizada y priorizando los servicios de mayor impacto en la organización.

Un plan de continuidad de servicios de tecnologías de información es un conjunto de tareas que se deben realizar en el caso de que los servicios presenten fallos en su funcionamiento, además establece los tiempos máximos en que la organización puede prescindir de cada servicio durante una contingencia.

Las tareas descritas en un plan de continuidad de servicios de TI deben contemplar estrategias tanto proactivas que ayudan a minimizar las consecuencias por la interrupción de un servicio y estrategias reactivas que buscan reanudar un servicio suspendido en el menor plazo posible.

Un plan de continuidad de servicios de TI brinda muchos beneficios a una organización, mencionaremos algunos de ellos:

- Identificar y reducir los riesgos en caso de pérdida de la continuidad en los servicios.
- Contar con los elementos y procedimientos necesarios para actuar en caso de contingencia.
- Reduce los tiempos de interrupción de los servicios en caso de una contingencia.

1.6.1. Elaboración de un plan de continuidad de servicios de TI

Para la elaboración de un plan de continuidad de servicios de TI existen varios criterios, tomaremos como referencia la opinión de un experto en el tema Josep Micolau, Delivery Director de CA, quien basa su opinión según la Internacional Organization for Standarization (ISO) y el British Standard Institute quienes establecen las mejores prácticas para la elaboración de un Plan de Continuidad de Negocio.

El desarrollo de un Plan de Continuidad de Negocio se puede dividir en cinco áreas principales, que son comúnmente conocidas como el ciclo de vida de un plan de negocio[5]:

a. En la fase de Análisis se debe proceder a realizar una Análisis de Riesgos acerca de las amenazas potenciales sobre los procesos de negocio. A continuación se deberá realizar un Análisis de Impacto, conocido como Business Impact Assessment (BIA), con el objetivo de identificar los procesos de negocio que pueden verse afectados por estas amenazas. Como resultado de este análisis se procederá a la Definición de Escenarios de Impacto donde se detallen los requerimientos de continuidad de los distintos procesos de negocio afectados y la Documentación de los Requerimientos de Recuperación.
b. En la fase de Diseño de la Solución se establecerán las medidas lógicas y adecuadas para mitigar el riesgo, minimizar el impacto o permitir la recuperación adecuada según los requerimientos de negocio identificados en la fase de Análisis, estas medidas serán

[5] Tomado del artículo ¿Qué debe incluir su Plan de Continuidad de Negocio?-15/julio/2008- Recursos e información tecnológica empresarial para CIOs.

tanto preventivas como correctivas. Estos mecanismos deben aumentar la Disponibilidad y reducir el ciclo de contingencia.

c. La tercera fase, la de Implementación, consiste en la realización práctica de la solución establecida en la fase de diseño. Esta implementación puede consistir en la instalación de componentes tecnológicos o en la comunicación oficial de las asignaciones personales que deben cubrir las funciones definidas para el momento de crisis.

d. La fase de Pruebas debe permitir obtener la garantía y la aceptación por parte de la organización de que se satisfacen los requerimientos de continuidad de negocio establecidos.

e. El Mantenimiento continuo es necesario para garantizar que el Plan de Continuidad de Negocio permanece viable y típicamente se revisa anualmente o cada dos años dependiendo de la organización. El plan debe ser un documento vivo que se actualice regularmente para estar actualizado con los cambios de los sistemas.

2. Capítulo II: Análisis y Gestión de Riesgos de Servicios de TI

En el capítulo 2 se realizará en primera instancia el análisis y la gestión de riesgos para los activos de TI, con el análisis previo luego se realizará el análisis del impacto al negocio, este capítulo será el pilar para el desarrollo propiamente dicho del proyecto ya que permitirá levantar las estrategias de continuidad y conocer los servicios críticos de TI de los cuales se elaborará el plan de continuidad.

2.1. Análisis y Gestión de Riesgos

Para el análisis y gestión de riesgos se ha tomado como marco de referencia la metodología MAGERIT cuyos objetivos son:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y la importancia de tratarlos a tiempo.
- Ofrecer un método sistemático para analizar los riesgos.
- Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Prepara a una organización para procesos de evaluación, auditoria y certificación.

Esta metodología también cuenta con una herramienta informática que permite realizar el proceso de análisis y gestión de riesgos de una forma más eficiente y contar con informes que recogen los hallazgos y las conclusiones de la gestión de riesgos como:

- Modelo de valor
- Mapa de riesgos
- Evaluación de salvaguardas
- Estado de riesgo
- Informe de insuficiencias
- Plan de seguridad

El análisis y la gestión de riesgos que se describe a continuación se adjuntan en el archivo BCP_TI.mgr.

2.1.1. Análisis de Riesgos

El análisis de riesgos permite determinar que tiene la organización en término de activos y que eventualidades puede ocurrir con los mismos. Para este análisis se necesitan 3 elementos que son:

- Activos, que son los elementos del sistema de información y que aportan valor a la Organización.
- Amenazas, cosas que le pueden ocurrir a los activos y que causarían un perjuicio.
- Salvaguardas, medidas de defensa para que el daño provocado por la amenazas sea menor.

Para realizar el análisis de riesgos se proponen 4 pasos que son:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor (costo por su degradación).
2. Determinar las amenazas a las que están expuestos los activos.
3. Estimar el impacto, daño causado de la materialización de la amenaza.
4. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Paso 1: Determinar los activos

Se determinaron los activos dividiéndolos en 6 capas que son:

- Sistemas de información, en la cual se encuentran los sistemas de información en los que se basa la misión de la organización.
- Servicios de apoyo, que agrupa servicios que sirven de apoyo en la operación diaria de la organización.
- Equipamiento, conjunto de software, hardware y comunicaciones que soportan tanto los sistemas de información como los servicios de apoyo.
- Instalaciones, entorno físico que se necesita para la prestación de los servicios.
- Personal, colaboradores que operan los activos ya mencionados
- Datos, corresponde a la información, claves, etc.

Figura 2 - 01: Determinación de activos [A]

Si generamos una estadística de activos por capas tenemos el cuadro mostrado a continuación que indica para cada capa la cantidad de activos según el grupo en el que se encuentra:

capa	[or]	[essential]	[null]	[availability]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	total
SI	0	0	0	0	0	0	3	3	0	0	0	0	0	0	3
SA	0	0	0	0	0	0	2	0	1	1	0	0	0	0	3
E	0	0	0	0	0	0	2	16	9	4	0	0	0	0	23
L	0	0	0	0	0	0	0	0	0	0	0	0	2	0	2
P	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2
DAT	0	0	0	0	3	0	0	0	0	0	0	0	0	0	3
TOTAL	0	0	0	0	3	0	7	19	10	5	0	0	2	2	36

OK

Figura 2 - 02: Estadística de activos [A]

Para cada activo se construirán las dependencias, para identificar que activos están relacionados y cuales dependen unos de otros sea de forma directa o indirecta. Para identificar la clase de dependencia la herramienta PILAR usa la siguiente leyenda:

Figura 2 - 03: Leyenda para dependencia de activos [A]

Con la leyenda mostrada podremos identificar de manera gráfica la dependencia entre activos y como se relacionan.

A continuación veremos la relación de dependencia para el sistema de información SIS.

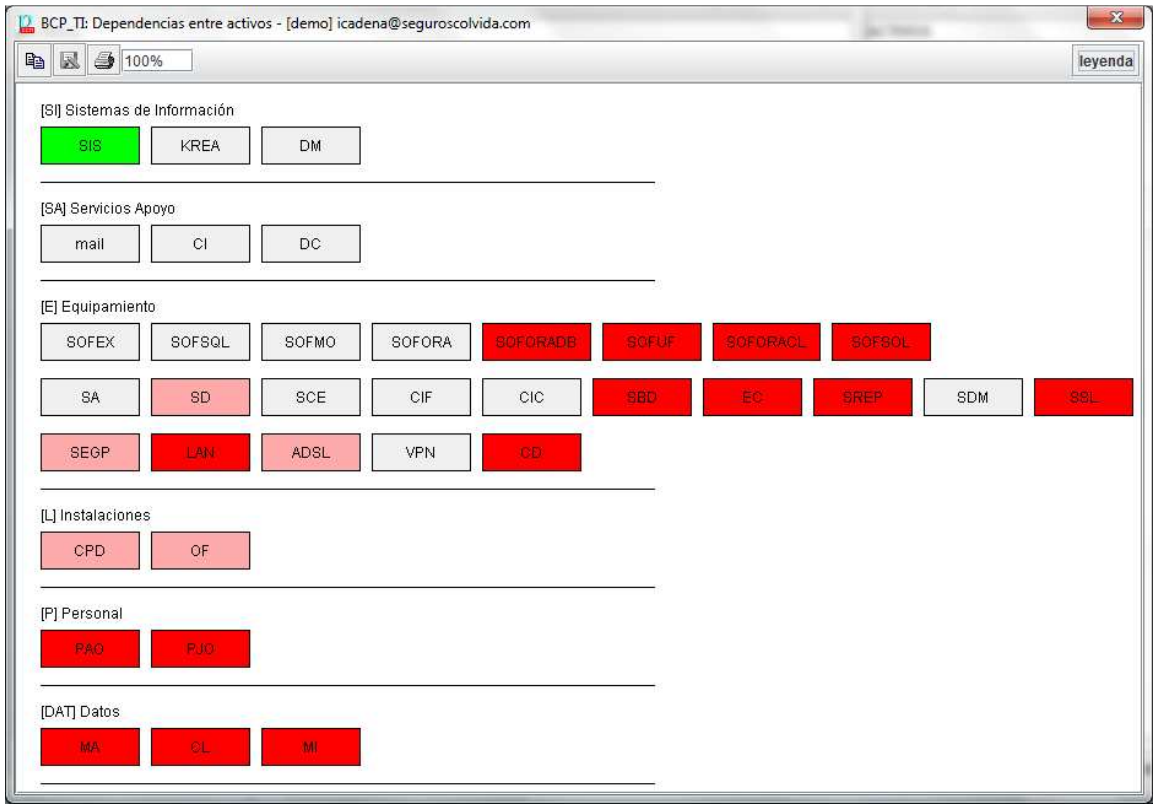


Figura 2 - 04: Dependencia entre activos [A]

Luego de establecer las dependencias se debe establecer la valoración de cada activo, esta valoración se la realizará en la dimensión que se está analizando, en este caso la disponibilidad, a continuación se presenta la valoración de varios activos.

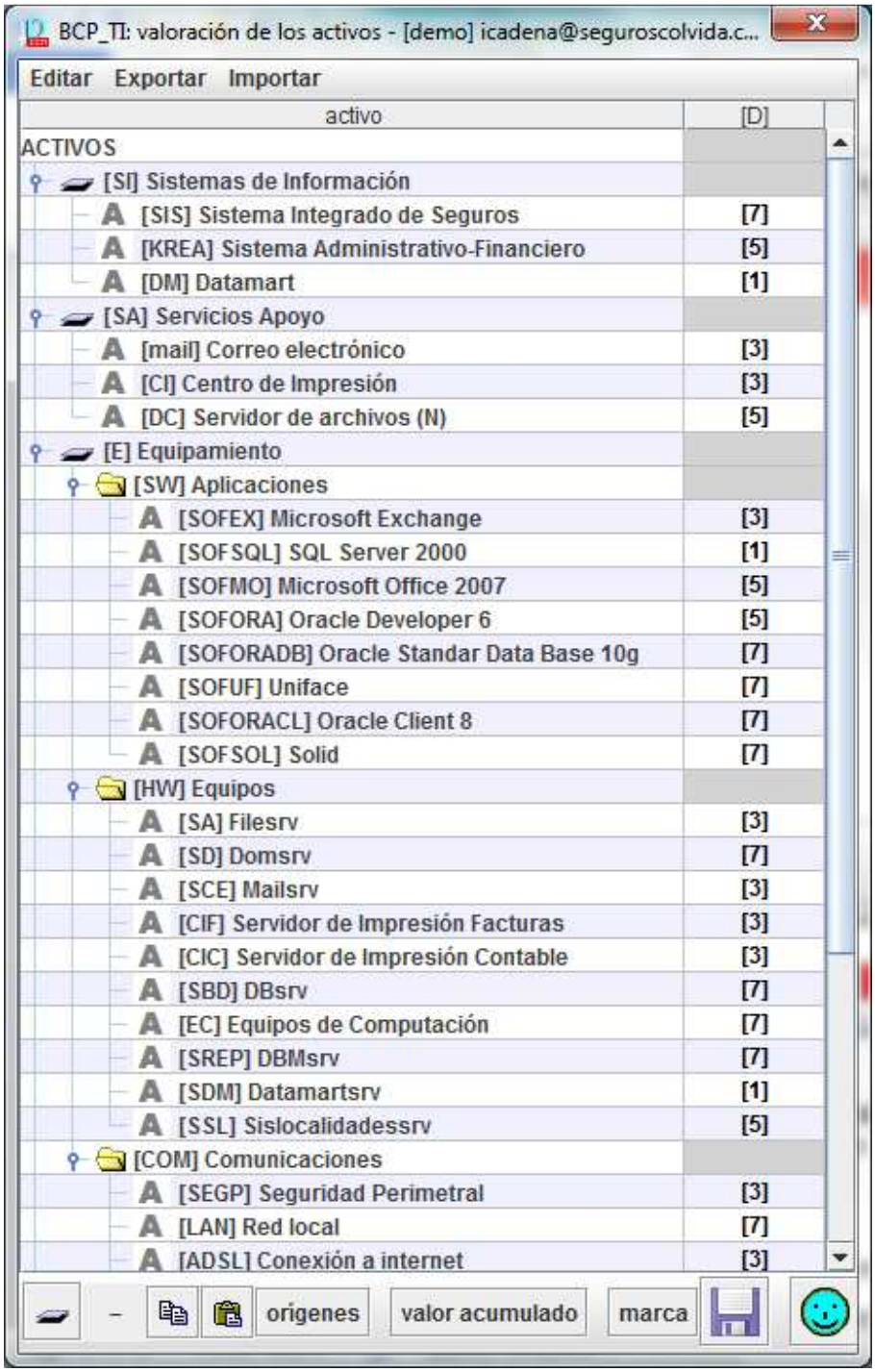


Figura 2 - 05: Valoración de activos [A]

Ingrid Cadena

Paso 2: Determinar las amenazas

Al utiliza la herramienta PILAR las amenazas ya vienen determinadas y están clasificadas en 4 grupos que son:

- Desastres naturales, en donde encontramos amenazas por fuego, daños por agua y desastres naturales como huracanes, terremotos, etc.
- De origen industrial, en donde encontramos corte de suministro eléctrico, fallo de servicios de comunicaciones, emanaciones electromagnéticas, etc.
- Errores y fallos no intencionados, en donde encontramos errores de usuario, errores de administrador del sistema, errores de configuración, etc.
- Ataques deliberados, en donde encontraremos abuso de privilegio de accesos, acceso no autorizado, ataque destructivo, etc.

En la herramienta PILAR la identificación de las amenazas es automática, cada activo se relaciona con las amenazas ya preestablecidas de acuerdo a la naturaleza del activo.

A continuación se coloca una vista de la identificación de amenazas para el servicio de correo electrónico.

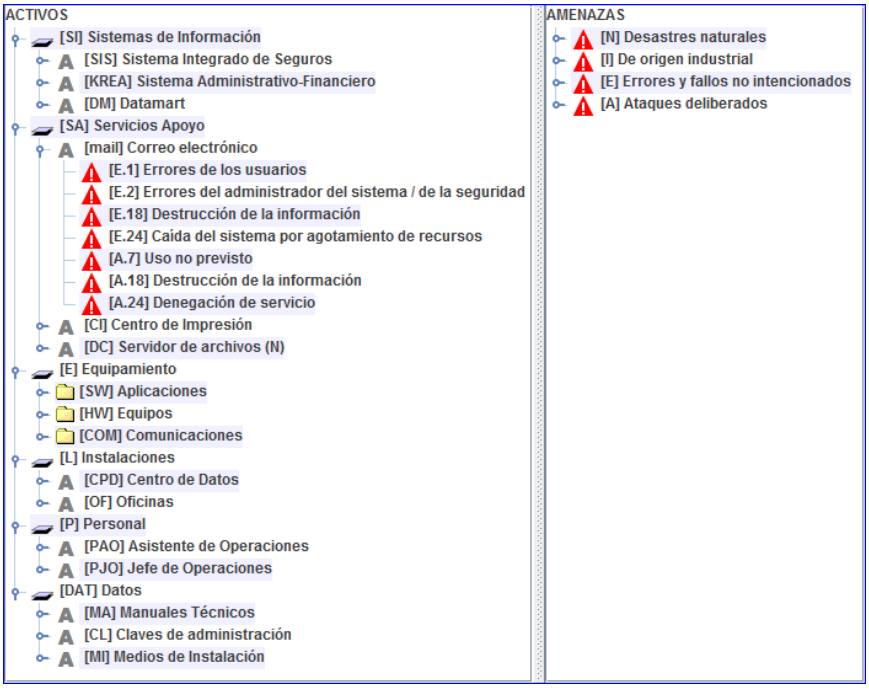


Figura 2 - 06: Amenazas por activos [A]

Paso 3: Determinar el impacto

El impacto es determinado para cada activo, por cada amenaza en este caso para la dimensión de la disponibilidad [D], podemos obtener 2 tipos de impacto:

El impacto acumulado es el calculado teniendo en cuenta su valor más el acumulado de los activos que dependen de él y las amenazas a las que está expuesto.

activo	[D]
ACTIVOS	[9]
[SI] Sistemas de Información	[7]
[SA] Servicios Apoyo	[5]
[mail] Correo electrónico	[3]
[E.1] Errores de los usuarios	[0]
[E.2] Errores del administrador del sistema / de la seguridad	[1]
[E.18] Destrucción de la información	[0]
[E.24] Caída del sistema por agotamiento de recursos	[2]
[A.7] Uso no previsto	[3]
[A.18] Destrucción de la información	[2]
[A.24] Denegación de servicio	[2]
[CI] Centro de Impresión	[3]
[DC] Servidor de archivos (N)	[5]
[E] Equipamiento	[7]
[L] Instalaciones	[9]
[P] Personal	[6]
[DAT] Datos	[6]

Figura 2 - 07: Impacto acumulado por activo [A]

El impacto repercutido es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a las que están expuestas los activos que dependen de él. En la siguiente figura podemos observar el impacto repercutido con el detalle para el correo electrónico.

activo	[D]
ACTIVOS	
[SIS] Sistema Integrado de Seguros	[7]
[KREA] Sistema Administrativo-Financiero	[5]
[DM] Datamart	[1]
[mail] Correo electrónico	[3]
[mail] Correo electrónico	[3]
[SW.SOFEX] Microsoft Exchange	[3]
[HW.SD] Domsrv	[3]
[HW.SCE] Mailsrv	[3]
[HW.EC] Equipos de Computación	[3]
[COM.SEGP] Seguridad Perimetral	[3]
[COM.LAN] Red local	[2]
[COM.ADSL] Conexión a internet	[2]
[COM.CD] Canal de Datos	[2]
[CPD] Centro de Datos	[3]
[OF] Oficinas	[3]
[PAO] Asistente de Operaciones	[2]
[PJO] Jefe de Operaciones	[1]
[MA] Manuales Técnicos	[2]
[CL] Claves de administración	[2]
[MI] Medios de Instalación	[2]
[CI] Centro de Impresión	[3]
[DC] Servidor de archivos (N)	[5]
[SOFEX] Microsoft Exchange	[3]
[SOFSQL] SQL Server 2000	[1]
[SOFMO] Microsoft Office 2007	[5]
[SOFORA] Oracle Developer 6	[5]
[SOFORADB] Oracle Standar Data Base 10g	[7]
[SOFUF] Uniface	[7]
[SOFORACL] Oracle Client 8	[7]
[SOFSOL] Solid	[7]
[SA] Filesrv	[3]
[SD] Domsrv	[7]
[SCE] Mailsrv	[3]
[CIF] Servidor de Impresión Facturas	[3]
[CIC] Servidor de Impresión Contable	[3]
[SBD] DBsrv	[7]

Figura 2 - 08: Impacto repercutido por activos [A]

Paso 4: Estimar el riesgo

En este paso se debe estimar el riesgo para cada activo, por cada amenaza en la dimensión de la disponibilidad, en la herramienta PILAR los niveles de criticidad definidos vienen dados como se muestrea en la figura:

Figura 2 - 09: Leyenda para niveles de criticidad [A]

El riesgo acumulado que es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza.

A continuación se muestra el riesgo acumulado de cada grupo de activos, teniendo en cuenta que no se considera ninguna salvaguarda.

activo	[D]
ACTIVOS	{6,2}
[SI] Sistemas de Información	{5,4}
[SIS] Sistema Integrado de Seguros	{5,4}
[KREA] Sistema Administrativo-Financiero	{4,2}
[DM] Datamart	{1,9}
[SA] Servicios Apoyo	{4,2}
[mail] Correo electrónico	{3,1}
[E.1] Errores de los usuarios	{0,98}
[E.2] Errores del administrador del sistema / de la seguridad	{1,5}
[E.18] Destrucción de la información	{0,98}
[E.24] Caída del sistema por agotamiento de recursos	{3,1}
[A.7] Uso no previsto	{2,7}
[A.18] Destrucción de la información	{2,2}
[A.24] Denegación de servicio	{3,1}
[CI] Centro de Impresión	{3,1}
[DC] Servidor de archivos (N)	{4,2}
[E] Equipamiento	{5,4}
[SW] Aplicaciones	{5,1}
[HW] Equipos	{5,4}
[COM] Comunicaciones	{5,4}
[L] Instalaciones	{6,2}
[CPD] Centro de Datos	{6,2}
[OF] Oficinas	{5,1}
[P] Personal	{4,3}
[PAO] Asistente de Operaciones	{4,3}
[PJO] Jefe de Operaciones	{3,8}
[DAT] Datos	{5,4}
[MA] Manuales Técnicos	{5,4}
[CL] Claves de administración	{5,4}
[MI] Medios de Instalación	{5,4}

Figura 2 - 10: Riesgo acumulado por cada activo [A]

También podemos obtener el riesgo repercutido que es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre el activo debido a una amenaza y la frecuencia de la amenaza.

activo	[D]
ACTIVOS	
[SIS] Sistema Integrado de Seguros	{5,4}
[KREA] Sistema Administrativo-Financiero	{4,2}
[DM] Datamart	{1,9}
[mail] Correo electrónico	{3,1}
[mail] Correo electrónico	{3,1}
[SW.SOFEX] Microsoft Exchange	{2,7}
[HW.SD] Domsrv	{3,1}
[HW.SCE] Mailsrv	{3,1}
[HW.EC] Equipos de Computación	{3,1}
[COM.SEGP] Seguridad Perimetral	{3,1}
[COM.LAN] Red local	{3,1}
[COM.ADSL] Conexión a internet	{3,1}
[COM.CD] Canal de Datos	{3,1}
[CPD] Centro de Datos	{2,7}
[OF] Oficinas	{2,7}
[PAO] Asistente de Operaciones	{1,9}
[PJO] Jefe de Operaciones	{1,5}
[MA] Manuales Técnicos	{3,1}
[CL] Claves de administración	{3,1}
[MI] Medios de Instalación	{3,1}
[E.1] Errores de los usuarios	{4,2}
[E.2] Errores del administrador del sistema / de la seguridad	{3,8}
[E.18] Destrucción de la información	{1,5}
[A.18] Destrucción de la información	{5,4}
[CI] Centro de Impresión	{3,1}
[DC] Servidor de archivos (N)	{4,2}
[SOFEX] Microsoft Exchange	{2,7}
[SOFSQL] SQL Server 2000	{1,5}
[SOFMO] Microsoft Office 2007	{3,9}
[SOFORA] Oracle Developer 6	{3,9}
[SOFORADB] Oracle Standar Data Base 10g	{5,1}
[SOFUF] Uniface	{5,1}
[SOFORACL] Oracle Client 8	{5,1}
[SOFSOL] Solid	{5,1}
[SA] Filesrv	{3,1}
[SD] Domsrv	{5,4}

Figura 2 - 11: Riesgo repercutido por activo [A]

2.1.2. Gestión de Riesgos

Permite organizar una defensa frente a los riesgos que se pueden presentar y estar preparado ante eventualidades. Como se había mencionado tener un nivel de riesgo cero es casi imposible por lo que el resultado de la gestión de riesgos es el riesgo residual, es decir el nivel de riesgo reducido que la Organización decide asumir.

La herramienta PILAR nos muestra ya una lista predefinida de salvaguardas, las mismas que podemos calificarlas de acuerdo al estado de madurez de cada una y si se considera aplicarla o no.

Los estados de madurez considerados para valorar cada salvaguarda son:

- L0: inexistente
- L1: inicial / ad hoc
- L2: reproducible, pero intuitivo
- L3: proceso definido
- L4: gestionado y medible
- L5: optimizado
- n.a.: no es aplicable

Adicionalmente podemos realizar la valoración de las salvaguardas tanto para el momento actual como para cada fase del tratamiento de los riesgos que queremos establecer. En este caso se establecieron 3 períodos de tiempo: ahora, 6 meses y un año.

aspecto	estrategia	salvaguarda	du...	fue...	co...	reco...		ah...	6m	1Y
		SALVAGUARDAS								
G	PR	[H] Protecciones Generales				9		-L5	-L5	-L5
G	PR	[D] Protección de la Información				5		-L3	-L3	-L4
G	PR	[S] Protección de los Servicios				7		-L3	-L3	-L4
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				8		-L4	-L5	-L5
G	PR	[HW] Protección de los Equipos Informáticos (HW)				6		-L3	-L3	-L4
G	PR	[COM] Protección de las Comunicaciones				9		L0-...	L0-L5	L0-L5
G	PR	[IP] Puntos de interconexión: conexiones con otros sistemas						n.a.	n.a.	n.a.
G	PR	[SI] Protección de los Soportes de Información						L0-...	L0-L1	L1-L2
G	PR	[AUX] Elementos Auxiliares				8		L0-...	L0-L3	L1-L3
F	PR	[L] Protección de las Instalaciones				8		L0-...	L0-L3	L0-L3
P	PR	[P] Gestión del Personal				6		L0-...	L0-L3	L1-L3
G	AD	[G] Organización				4		L0-...	L0-L3	L0-L4
G	RC	[BC] {or} Continuidad del negocio				5		L1-...	L1-L3	L3
G	AD	[E] Relaciones Externas				7		L0-...	L0-L3	L1-L3
G	AD	[C] Productos certificados o acreditados						n.a.	n.a.	n.a.

Figura 2 - 12: Valoración de salvaguardas [A]

Las salvaguardas están catalogadas según su aspecto en:

- G: Gestión.
- T: Técnico.
- P: Personal.
- F: Seguridad física.

Luego de determinar el estado de las salvaguardas que la compañía ha decidió trabajar se obtiene el impacto y el riesgo residuales y el impacto y el riesgo repercutido que se puede apreciar para las 3 fases del tratamiento de los riesgos establecidos.

A continuación se muestra el impacto y el riesgo residuales para la fase actual del tratamiento de los riesgos:

Impacto residual acumulado

potencial | ahora | 6m | 1Y

activo	[D]
ACTIVOS	[8]
[SI] Sistemas de Información	[6]
[SIS] Sistema Integrado de Seguros	[6]
[KREA] Sistema Administrativo-Financiero	[4]
[DM] Datamart	[0]
[SA] Servicios Apoyo	[4]
[mail] Correo electrónico	[2]
[CI] Centro de Impresión	[2]
[DC] Servidor de archivos (N)	[4]
[E] Equipamiento	[6]
[SW] Aplicaciones	[6]
[HW] Equipos	[6]
[COM] Comunicaciones	[6]
[L] Instalaciones	[8]
[CPD] Centro de Datos	[8]
[OF] Oficinas	[6]
[P] Personal	[5]
[PAO] Asistente de Operaciones	[5]
[PJO] Jefe de Operaciones	[3]
[DAT] Datos	[4]
[MA] Manuales Técnicos	[4]
[CL] Claves de administración	[4]
[MI] Medios de Instalación	[4]

Figura 2 - 13: Impacto residual por activo [A]

Riesgo residual acumulado

potencial | ahora | 6m | 1Y

activo	[D]
ACTIVOS	{5,5}
[SI] Sistemas de Información	{4,1}
[SIS] Sistema Integrado de Seguros	{4,1}
[KREA] Sistema Administrativo-Financiero	{3,3}
[DM] Datamart	{0,92}
[SA] Servicios Apoyo	{3,0}
[mail] Correo electrónico	{1,7}
[CI] Centro de Impresión	{1,8}
[DC] Servidor de archivos (N)	{3,0}
[E] Equipamiento	{4,5}
[SW] Aplicaciones	{4,1}
[HW] Equipos	{4,5}
[COM] Comunicaciones	{4,4}
[L] Instalaciones	{5,5}
[CPD] Centro de Datos	{5,5}
[OF] Oficinas	{4,3}
[P] Personal	{3,0}
[PAO] Asistente de Operaciones	{3,0}
[PJO] Jefe de Operaciones	{2,6}
[DAT] Datos	{3,9}
[MA] Manuales Técnicos	{3,9}
[CL] Claves de administración	{3,7}
[MI] Medios de Instalación	{3,9}

Figura 2 - 14: Riesgo residual [A]

A continuación se muestra el impacto y el riesgo residuales repercutidos para la fase actual del tratamiento de los riesgos:

Impacto residual repercutido

potencial | ahora | 6m | 1Y

activo	[D]
ACTIVOS	
[SIS] Sistema Integrado de Seguros	[6]
[KREA] Sistema Administrativo-Financiero	[4]
[DM] Datamart	[0]
[mail] Correo electrónico	[2]
[CI] Centro de Impresión	[2]
[DC] Servidor de archivos (N)	[4]
[SOFEX] Microsoft Exchange	[2]
[SOFSQL] SQL Server 2000	[0]
[SOFMO] Microsoft Office 2007	[4]
[SOFORA] Oracle Developer 6	[4]
[SOFORADB] Oracle Standar Data Base 10g	[6]
[SOFUF] Uniface	[6]
[SOFORACL] Oracle Client 8	[6]
[SOFSOL] Solid	[6]
[SA] Filesrv	[2]
[SD] Domsrv	[6]
[SCE] Mailsrv	[2]
[CIF] Servidor de Impresión Facturas	[2]
[CIC] Servidor de Impresión Contable	[2]
[SBD] DBsrv	[6]
[EC] Equipos de Computación	[6]
[SREP] DBMsrv	[6]
[SDM] Datamartsrv	[0]
[SSL] Sislocalidadessrv	[4]
[SEGP] Seguridad Perimetral	[2]
[LAN] Red local	[6]
[ADSL] Conexión a internet	[2]
[VPN] Canal virtual privado	[0]
[CD] Canal de Datos	[2]
[CPD] Centro de Datos	[8]
[OF] Oficinas	[4]
[PAO] Asistente de Operaciones	[1]
[PJO] Jefe de Operaciones	[0]
[MA] Manuales Técnicos	[0]

Figura 2 - 15: Impacto residual repercutido [A]

Riesgo residual repercutido

potencial | ahora | 6m | 1Y

activo	[D]
ACTIVOS	
[SIS] Sistema Integrado de Seguros	{4,5}
[KREA] Sistema Administrativo-Financiero	{3,3}
[DM] Datamart	{0,98}
[mail] Correo electrónico	{2,1}
[CI] Centro de Impresión	{2,1}
[DC] Servidor de archivos (N)	{3,3}
[SOFEX] Microsoft Exchange	{1,7}
[SOFSQL] SQL Server 2000	{0,88}
[SOFMO] Microsoft Office 2007	{2,9}
[SOFORA] Oracle Developer 6	{2,9}
[SOFORADB] Oracle Standar Data Base 10g	{4,1}
[SOFUF] Uniface	{4,1}
[SOFORACL] Oracle Client 8	{4,1}
[SOFSOL] Solid	{4,1}
[SA] Filesrv	{2,0}
[SD] Domsrv	{4,5}
[SCE] Mailsrv	{2,1}
[CIF] Servidor de Impresión Facturas	{1,9}
[CIC] Servidor de Impresión Contable	{1,9}
[SBD] DBsrv	{4,5}
[EC] Equipos de Computación	{4,5}
[SREP] DBMsrv	{4,5}
[SDM] Datamartsrv	{0,97}
[SSL] Sislocalidadessrv	{3,3}
[SEGP] Seguridad Perimetral	{2,0}
[LAN] Red local	{4,5}
[ADSL] Conexión a internet	{2,0}
[VPN] Canal virtual privado	{1,1}
[CD] Canal de Datos	{2,0}
[CPD] Centro de Datos	{5,5}
[OF] Oficinas	{3,1}
[PAO] Asistente de Operaciones	{0,93}
[PJO] Jefe de Operaciones	{0,84}
[MA] Manuales Técnicos	{0,86}

Figura 2 - 16: Riesgo residual repercutido [A]

Luego de haber establecido las salvaguardas se debe generar el informe de insuficiencias, el cual nos indica aquellas salvaguardas en las cuales es necesario trabajar para mitigar los riesgos.

El informe de insuficiencias para la etapa de un año se coloca como anexo 1, en el cual se indican solamente aquellas con recomendación de mayor o igual a 6 por la extensión del informe.

2.2. Análisis de Impacto al Negocio

Para la realización del análisis de impacto se hará de forma cualitativa asignando valores relativos. Con la ayuda de la herramienta podemos realizar el análisis de impacto en 6 pasos.

Paso 1: Determinar escalones de interrupción

Determinar los escalones de interrupción en los cuales se va a analizar el impacto luego de transcurrido el tiempo de cada escalón.

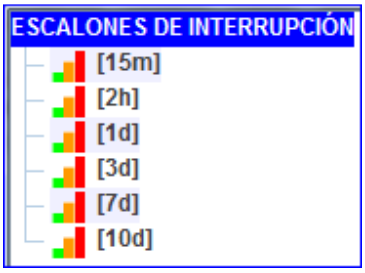


Figura 2 - 17: Escalones de interrupción [A]

Paso 2: Valoración de los activos

Los activos deben ser valorados para cada escalón de interrupción que se determinó ya que el impacto por la indisponibilidad es distinta en un lapso de tiempo corto que en uno mayor.

activo	[15m]	[2h]	[1d]	[3d]	[7d]	[10d]
ACTIVOS						
[SI] Sistemas de Información						
[SIS] Sistema Integrado de Seguros	[1]	[1]	[5]	[5]	[9]	[9]
[KREA] Sistema Administrativo-Financiero	[1]	[1]	[3]	[3]	[7]	[7]
[DM] Datamart	[1]	[1]	[1]	[1]	[3]	[3]
[SA] Servicios Apoyo						
[mail] Correo electrónico	[1]	[1]	[3]	[3]	[5]	[7]
[CI] Centro de Impresión	[1]	[1]	[3]	[3]	[5]	[7]
[DC] Servidor de archivos (N)	[1]	[1]	[3]	[5]	[5]	[9]
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[COM] Comunicaciones						
[L] Instalaciones						
[CPD] Centro de Datos	[1]	[3]	[5]	[5]	[9]	[9]
[OF] Oficinas	[1]	[1]	[3]	[3]	[5]	[7]
[P] Personal						
[PAO] Asistente de Operaciones	[1]	[1]	[1]	[3]	[3]	[3]
[PJO] Jefe de Operaciones	[1]	[1]	[1]	[3]	[3]	[5]
[DAT] Datos						
[MA] Manuales Técnicos	[1]	[1]	[1]	[3]	[3]	[3]
[CL] Claves de administración	[1]	[1]	[3]	[3]	[7]	[7]
[MI] Medios de Instalación	[1]	[1]	[1]	[3]	[3]	[3]

Figura 2 - 18: Valoración de activos por cada escala de interrupción [A]

Paso 3: Valoración de Amenazas

Aquí se debe definir la frecuencia de ocurrencia de cada amenaza, en este caso tomaremos la posibilidad de que se materialice una amenaza, bajo la siguiente escala:

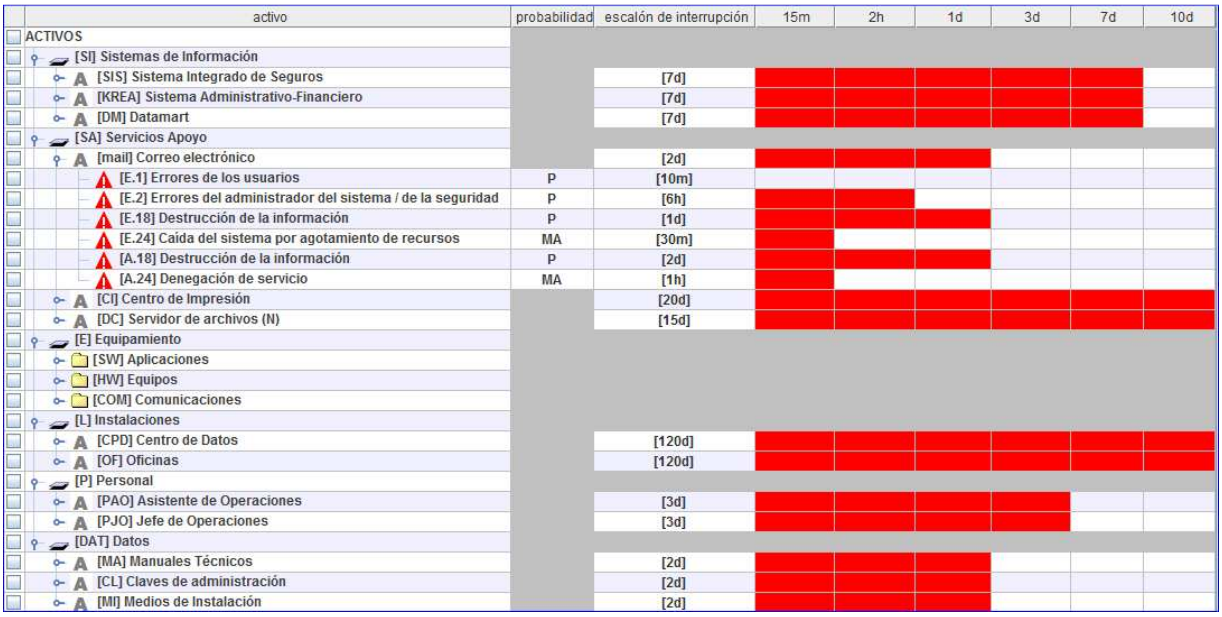
I – Improbable

PP – Poco probable

P – Probable

MA – Muy Probable

La herramienta muestra por sí sola la escala de interrupción que se provocará según la amenaza y su probabilidad de ocurrencia.



activo	probabilidad	escalón de interrupción	15m	2h	1d	3d	7d	10d
ACTIVOS								
[SI] Sistemas de Información								
[SIS] Sistema Integrado de Seguros		[7d]						
[KREA] Sistema Administrativo-Financiero		[7d]						
[DM] Datamart		[7d]						
[SA] Servicios Apoyo								
[mail] Correo electrónico		[2d]						
[E.1] Errores de los usuarios	P	[10m]						
[E.2] Errores del administrador del sistema / de la seguridad	P	[6h]						
[E.18] Destrucción de la información	P	[1d]						
[E.24] Caída del sistema por agotamiento de recursos	MA	[30m]						
[A.18] Destrucción de la información	P	[2d]						
[A.24] Denegación de servicio	MA	[1h]						
[CI] Centro de Impresión		[20d]						
[DC] Servidor de archivos (N)		[15d]						
[E] Equipamiento								
[SW] Aplicaciones								
[HW] Equipos								
[COM] Comunicaciones								
[L] Instalaciones								
[CPD] Centro de Datos		[120d]						
[OF] Oficinas		[120d]						
[P] Personal								
[PAO] Asistente de Operaciones		[3d]						
[PJO] Jefe de Operaciones		[3d]						
[DAT] Datos								
[MA] Manuales Técnicos		[2d]						
[CL] Claves de administración		[2d]						
[MI] Medios de Instalación		[2d]						

Figura 2 - 19: Escala de interrupción por activo según la probabilidad de ocurrencia de cada amenaza [A]

Paso 4: Determinación del Impacto y el Riesgo

La determinación del impacto y el riesgo acumulado se mostrarán automáticamente al terminar los 3 pasos anteriores, en esta valoración se puede ver la probabilidad de ocurrencia de cada amenaza y la escala de interrupción que la materialización de cada amenaza provocaría, así obtendremos el impacto y el riesgo acumulado

En la gráfica veremos para cada activo el tiempo de interrupción (EDI), el impacto en ese tiempo y el riesgo.

activo / amenaza	P	EDI	impacto	riesgo
ACTIVOS		120d	[9]	{6,2}
[SI] Sistemas de Información				
[SIS] Sistema Integrado de Seguros		7d	[9]	{6,2}
[KREA] Sistema Administrativo-Financiero		7d	[7]	{5,1}
[DM] Datamart		7d	[3]	{2,7}
[SA] Servicios Apoyo				
[mail] Correo electrónico		2d	[3]	{2,7}
[E.1] Errores de los usuarios	P	[10m]		{0}
[E.2] Errores del administrador del sistema / de la seguridad	P	[6h]	[1]	{1,5}
[E.18] Destrucción de la información	P	[1d]	[3]	{2,7}
[E.24] Caída del sistema por agotamiento de recursos	MA	[30m]	[1]	{2,4}
[A.18] Destrucción de la información	P	[2d]	[3]	{2,7}
[A.24] Denegación de servicio	MA	[1h]	[1]	{2,4}
[CI] Centro de Impresión		20d	[7]	{5,1}
[DC] Servidor de archivos (N)		15d	[9]	{6,2}
[E] Equipamiento				
[SW] Aplicaciones		7d	[9]	{6,2}
[HW] Equipos		20d	[9]	{6,2}
[COM] Comunicaciones		20d	[9]	{6,2}
[L] Instalaciones				
[CPD] Centro de Datos		120d	[9]	{6,2}
[OF] Oficinas		120d	[9]	{6,2}
[P] Personal				
[PAO] Asistente de Operaciones		3d	[5]	{3,9}
[PJO] Jefe de Operaciones		3d	[5]	{3,9}
[DAT] Datos				
[MA] Manuales Técnicos		2d	[5]	{4,8}
[CL] Claves de administración		2d	[5]	{4,8}
[MI] Medios de Instalación		2d	[5]	{4,8}

Figura 2 - 20: Impacto y Riesgo según la probabilidad de ocurrencia de una amenaza en un EDI [A]

Si vemos con más detalle para cada activo podremos ver la misma información para cada amenaza y adicionalmente podemos ver la probabilidad de ocurrencia de cada amenaza.

Impacto y Riesgo Repercutido

activo / amenaza	P	EDI	impacto	riesgo
ACTIVOS		[120d]	[9]	{6,2}
[SIS] Sistema Integrado de Seguros		[120d]	[9]	{6,2}
[KREA] Sistema Administrativo-Financiero		[120d]	[7]	{5,1}
[DM] Datamart		[120d]	[3]	{2,7}
[mail] Correo electrónico		[120d]	[7]	{5,1}
[mail] Correo electrónico		[2d]	[3]	{2,7}
[SW.SOFEX] Microsoft Exchange		[7d]	[5]	{3,9}
[HW.SD] Domsrv		[20d]	[7]	{5,1}
[HW.SCE] Mailsrv		[20d]	[7]	{5,1}
[HW.EC] Equipos de Computación		[20d]	[7]	{5,1}
[COM.SEGP] Seguridad Perimetral		[20d]	[7]	{5,1}
[COM.LAN] Red local		[15d]	[7]	{5,1}
[COM.ADSL] Conexión a internet		[15d]	[7]	{5,1}
[COM.CD] Canal de Datos		[15d]	[7]	{5,1}
[CPD] Centro de Datos		[120d]	[7]	{5,1}
[OF] Oficinas		[120d]	[7]	{5,1}
[PAO] Asistente de Operaciones		[3d]	[3]	{2,7}
[PJO] Jefe de Operaciones		[3d]	[3]	{2,7}
[MA] Manuales Técnicos		[2d]	[3]	{3,6}
[CL] Claves de administración		[2d]	[3]	{3,6}
[MI] Medios de Instalación		[2d]	[3]	{3,6}
[CI] Centro de Impresión		[120d]	[7]	{5,1}
[DC] Servidor de archivos (N)		[120d]	[9]	{6,2}
[SOFEX] Microsoft Exchange		[7d]	[5]	{3,9}
[SOFSQL] SQL Server 2000		[7d]	[3]	{2,7}
[SOFMO] Microsoft Office 2007		[7d]	[3]	{2,7}
[SOFORA] Oracle Developer 6		[7d]	[7]	{5,1}
[SOFORADB] Oracle Standar Data Base 10g		[7d]	[9]	{6,2}
[SOFUF] Uniface		[7d]	[9]	{6,2}
[SOFORACL] Oracle Client 8		[7d]	[9]	{6,2}
[SOFSOL] Solid		[7d]	[9]	{6,2}
[SA] Filesrv		[120d]	[9]	{6,2}
[SD] Domsrv		[120d]	[9]	{6,2}
[SCE] Mailsrv		[120d]	[7]	{5,1}
[CIF] Servidor de Impresión Facturas		[120d]	[7]	{5,1}
[CIC] Servidor de Impresión Contable		[120d]	[7]	{5,1}
[SBD] DBsrv		[120d]	[9]	{6,2}

Figura 2 - 21: Impacto y riesgo repercutido para la escala de interrupción [A]

Paso 5: Equipamiento de Respaldo

Previo a establecer el equipamiento de respaldo primero se debe definir las fases para el tratamiento de los riesgos, estas fases son el lapso del tiempo en el cual se trabajará en el equipamiento de respaldo necesario.

Con las fases para el tratamiento de riesgo establecidas, en este caso 3: ahora, dentro de 6 meses y dentro de un año se debe definir el equipamiento de respaldo y el tiempo de respuesta de cada uno contribuirá a alcanzar.

activo	ahora	6m	1Y
ACTIVOS			
[SI] Sistemas de Información			
[SIS] Sistema Integrado de Seguros	[12d] / L1	[4d] / L3	[2d] / L4
[KREA] Sistema Administrativo-Financiero	[4d] / L3	[2d] / L4	[1d] / L4
[DM] Datamart	[15d] / L0	[7d] / L2	[2d] / L3
[SA] Servicios Apoyo			
[mail] Correo electrónico	[5d] / L1	[2d] / L2	[2d] / L3
[CI] Centro de Impresión	[3d] / L1	[3d] / L3	[3d] / L3
[DC] Servidor de archivos (N)	[2d] / L1	[2d] / L3	[1d] / L4
[E] Equipamiento			
[SW] Aplicaciones			
[HW] Equipos			
[COM] Comunicaciones			
[L] Instalaciones			
[CPD] Centro de Datos	[15d] / L1	[7d] / L3	[3d] / L3
[OF] Oficinas	[5d] / L0	[2d] / L0	[2d] / L2
[P] Personal			
[PAO] Asistente de Operaciones	[30m] / L1	[30m] / L1	[15m] / L3
[PJO] Jefe de Operaciones	[30d] / L1	[30d] / L1	[15d] / L2
[DAT] Datos			
[MA] Manuales Técnicos	[1d] / L2	[15m] / L3	[15m] / L3
[CL] Claves de administración	[15d] / L1	[5d] / L2	[15m] / L3
[MI] Medios de Instalación	[8d] / L0	[8d] / L0	[30m] / L3

Figura 2 - 22: Equipamiento de respaldo y tiempo de respuesta para cada fase del tratamiento de riesgos [A]

Paso 6: Determinación del Impacto y el Riesgo residuales

En este paso obtendremos el impacto y riesgo residuales y ver como varían para cada fase del tratamiento del riesgo luego de haber establecido las salvaguardas y los equipamientos de respaldo, aquí se puede apreciar como el impacto y el riesgo disminuyen en la medida que se establecen las medidas de control o mejoran las mismas en el tiempo. Este paso puede ser también muy útil pues permite realizar simulaciones del comportamiento del impacto y el riesgo según las salvaguardas y los equipamientos de respaldo que se determinen.

Impacto Residual

activo	potencial	ahora	6m	1Y
ACTIVOS				
[SI] Sistemas de Información				
[SIS] Sistema Integrado de Seguros	[9]	[5]	[5]	[5]
[KREA] Sistema Administrativo-Financiero	[7]	[3]	[3]	[1]
[DM] Datamart	[3]	[1]	[1]	[1]
[SA] Servicios Apoyo				
[mail] Correo electrónico	[3]	[3]	[3]	[3]
[CI] Centro de Impresión	[7]	[3]	[3]	[3]
[DC] Servidor de archivos (N)	[9]	[3]	[3]	[1]
[E] Equipamiento				
[SW] Aplicaciones	[9]	[5]	[5]	[5]
[HW] Equipos	[9]	[9]	[5]	[5]
[COM] Comunicaciones	[9]	[9]	[5]	[5]
[L] Instalaciones				
[CPD] Centro de Datos	[9]	[9]	[5]	[5]
[OF] Oficinas	[9]	[5]	[5]	[5]
[P] Personal				
[PAO] Asistente de Operaciones	[5]	[1]	[1]	
[PJO] Jefe de Operaciones	[5]	[5]	[5]	[5]
[DAT] Datos				
[MA] Manuales Técnicos	[5]	[1]		
[CL] Claves de administración	[5]	[5]	[5]	
[MI] Medios de Instalación	[5]	[5]	[5]	[1]

Figura 2 - 23: Impacto residual para cada fase del tratamiento de riesgos [A]

Riesgo Residual

activo	potencial	ahora	6m	1Y
ACTIVOS				
[SI] Sistemas de Información				
[SIS] Sistema Integrado de Seguros	{6,2}	{3,4}	{3,3}	{3,0}
[KREA] Sistema Administrativo-Financiero	{6,1}	{2,4}	{2,3}	{1,7}
[DM] Datamart	{2,7}	{2,0}	{1,9}	{1,6}
[SA] Servicios Apoyo				
[mail] Correo electrónico	{2,7}	{2,2}	{2,1}	{1,8}
[CI] Centro de Impresión	{5,1}	{2,5}	{2,2}	{1,9}
[DC] Servidor de archivos (N)	{6,2}	{2,5}	{2,4}	{1,8}
[E] Equipamiento				
[SW] Aplicaciones	{6,2}	{3,6}	{3,5}	{3,2}
[HW] Equipos	{6,2}	{5,9}	{3,5}	{3,2}
[COM] Comunicaciones	{6,2}	{5,8}	{3,5}	{3,3}
[L] Instalaciones				
[CPD] Centro de Datos	{6,2}	{6,1}	{3,8}	{3,3}
[OF] Oficinas	{6,2}	{3,8}	{3,8}	{3,3}
[P] Personal				
[PAO] Asistente de Operaciones	{3,9}	{1,1}	{1,1}	{0}
[PJO] Jefe de Operaciones	{3,9}	{3,4}	{3,4}	{3,0}
[DAT] Datos				
[MA] Manuales Técnicos	{4,8}	{1,9}	{0}	{0}
[CL] Claves de administración	{4,8}	{4,3}	{4,3}	{0}
[MI] Medios de Instalación	{4,8}	{4,3}	{4,3}	{1,5}

Figura 2 - 24: Riesgo residual para cada fase del tratamiento de riesgos [A]

Finalmente podemos obtener el impacto y riesgo residual repercutido, para cada fase del tratamiento de riesgos, permitiendo así apreciar el comportamiento según las salvaguardas y el equipamiento establecido.

Impacto Residual Repercutido

activo	potencial	ahora	6m	1Y
ACTIVOS	[9]	[9]	[5]	[5]
[SIS] Sistema Integrado de Seguros	[9]	[9]	[9]	[5]
[KREA] Sistema Administrativo-Financiero	[7]	[7]	[7]	[3]
[DM] Datamart	[3]	[3]	[3]	[1]
[mail] Correo electrónico	[7]	[7]	[5]	[3]
[CI] Centro de Impresión	[7]	[7]	[5]	[3]
[DC] Servidor de archivos (N)	[9]	[9]	[5]	[5]
[SOFEX] Microsoft Exchange	[5]	[3]	[3]	[3]
[SOFSQL] SQL Server 2000	[3]	[3]	[3]	[1]
[SOFMO] Microsoft Office 2007	[3]	[3]	[3]	[1]
[SOFORA] Oracle Developer 6	[7]	[3]	[3]	[3]
[SOFORADB] Oracle Standar Data Base 10g	[9]	[9]	[5]	[5]
[SOFUF] Uniface	[9]	[9]	[5]	[5]
[SOFORACL] Oracle Client 8	[9]	[9]	[5]	[5]
[SOFSOL] Solid	[9]	[9]	[5]	[5]
[SA] Filesrv	[9]	[9]	[5]	[5]
[SD] Domsrv	[9]	[9]	[7]	[5]
[SCE] Mailsrv	[7]	[7]	[5]	[3]
[CIF] Servidor de Impresión Facturas	[7]	[3]	[3]	[3]
[CIC] Servidor de Impresión Contable	[7]	[3]	[3]	[3]
[SBD] DBsrv	[9]	[9]	[9]	[5]
[EC] Equipos de Computación	[9]	[5]	[5]	[5]
[SREP] DBMsrv	[9]	[9]	[9]	[5]
[SDM] Datamartsrv	[3]	[3]	[3]	[1]
[SSL] Sislocalidadessrv	[9]	[9]	[7]	[5]
[SEGP] Seguridad Perimetral	[5]	[5]	[5]	[3]
[LAN] Red local	[9]	[9]	[9]	[5]
[ADSL] Conexión a internet	[9]	[9]	[7]	[5]
[VPN] Canal virtual privado	[5]	[5]	[5]	[5]
[CD] Canal de Datos	[7]	[7]	[5]	[3]
[CPD] Centro de Datos	[9]	[9]	[9]	[5]
[OF] Oficinas	[7]	[3]	[3]	[3]
[PAO] Asistente de Operaciones	[3]	[1]	[1]	[1]
[PJO] Jefe de Operaciones	[3]	[3]	[3]	[3]
[MA] Manuales Técnicos	[1]	[1]	[1]	[1]
[CL] Claves de administración	[3]	[3]	[3]	[1]
[MI] Medios de Instalación	[1]	[1]	[1]	[1]

Figura 2 - 25: Impacto residual repercutido para cada fase del tratamiento de riesgos [A]

Riesgo Residual Repercutido

activo	potencial	ahora	6m	1Y
ACTIVOS	{6,2}	{6,1}	{4,3}	{3,3}
[SIS] Sistema Integrado de Seguros	{6,2}	{6,1}	{6,1}	{3,3}
[KREA] Sistema Administrativo-Financiero	{5,1}	{5,0}	{4,9}	{2,1}
[DM] Datamart	{2,7}	{2,6}	{2,6}	{1,7}
[mail] Correo electrónico	{5,1}	{5,0}	{3,8}	{2,2}
[CI] Centro de Impresión	{5,1}	{5,0}	{3,8}	{2,1}
[DC] Servidor de archivos (N)	{6,2}	{6,1}	{3,8}	{3,3}
[SOFEX] Microsoft Exchange	{3,9}	{2,4}	{2,3}	{2,0}
[SOFSQL] SQL Server 2000	{2,7}	{2,4}	{2,3}	{1,7}
[SOFMO] Microsoft Office 2007	{2,7}	{2,4}	{2,3}	{1,7}
[SOFORA] Oracle Developer 6	{5,1}	{2,4}	{2,3}	{2,0}
[SOFORADB] Oracle Standar Data Base 10g	{6,2}	{5,9}	{3,5}	{3,2}
[SOFUF] Uniface	{6,2}	{5,9}	{3,5}	{3,2}
[SOFORACL] Oracle Client 8	{6,2}	{5,9}	{3,5}	{3,2}
[SOFSOL] Solid	{6,2}	{5,9}	{3,5}	{3,2}
[SA] Filesrv	{6,2}	{6,1}	{3,8}	{3,3}
[SD] Domsrv	{6,2}	{6,1}	{4,9}	{3,3}
[SCE] Mailsrv	{5,1}	{5,0}	{3,8}	{2,1}
[CIF] Servidor de Impresión Facturas	{5,1}	{2,6}	{2,6}	{2,1}
[CIC] Servidor de Impresión Contable	{5,1}	{2,6}	{2,6}	{2,1}
[SBD] DBsrv	{6,2}	{6,1}	{6,1}	{3,3}
[EC] Equipos de Computación	{6,2}	{3,8}	{3,8}	{3,3}
[SREP] DBMsrv	{6,2}	{6,1}	{6,1}	{3,3}
[SDM] Datamartsrv	{2,7}	{2,6}	{2,6}	{1,7}
[SSL] Sislocalidadessrv	{6,2}	{6,1}	{4,9}	{3,3}
[SEGP] Seguridad Perimetral	{3,9}	{3,8}	{3,8}	{2,1}
[LAN] Red local	{6,2}	{6,1}	{6,1}	{3,3}
[ADSL] Conexión a internet	{6,2}	{6,1}	{4,9}	{3,3}
[VPN] Canal virtual privado	{3,9}	{3,8}	{3,8}	{3,3}
[CD] Canal de Datos	{5,1}	{5,0}	{3,8}	{2,2}
[CPD] Centro de Datos	{6,2}	{6,1}	{6,1}	{3,3}
[OF] Oficinas	{5,1}	{2,6}	{2,6}	{2,1}
[PAO] Asistente de Operaciones	{2,4}	{1,1}	{1,1}	{0,93}
[PJO] Jefe de Operaciones	{2,7}	{2,3}	{2,2}	{1,9}
[MA] Manuales Técnicos	{2,4}	{1,9}	{1,9}	{1,5}
[CL] Claves de administración	{3,6}	{3,1}	{3,1}	{1,5}
[MI] Medios de Instalación	{2,4}	{1,9}	{1,9}	{1,5}

Figura 2 - 26: Riesgo residual repercutido para cada fase del tratamiento de riesgos [A]

3. Capítulo III: Elaboración del plan de continuidad de los servicios de TI

El capítulo tres es el capítulo principal del proyecto ya que es en el cual se desarrollará el aporte del presente proyecto, es decir es en este capítulo en el cual se construirá el documento que contendrá el plan de continuidad de servicios de tecnologías de información para una empresa de seguros en Ecuador. En el presente capítulo consta de dos partes la primera en la cual se establecerán las estrategias de continuidad y la segunda en la cual se desarrollará el plan, en esta última parte solo constará el como elaborar el plan, ya que el plan propiamente dicho se lo elaborará en un documento separado y se lo colocará como un anexo.

3.1. Selección de la Estrategia de Continuidad

Consiste en identificar las alternativas de recuperación de las operaciones en los tiempos identificados en el BIA.

Luego del análisis realizado, se escoge como objetivo de recuperación a los 3 servicios más críticos de TI que son:

- Sistema Integrado de Seguros
- Sistema Administrativo – Financiero (KREA)
- Servidor de archivos (N)

Tomando en cuenta que los servicios de TI mencionados son aquellos sin los cuales la compañía no podría seguir con sus operaciones, ya que soportan procesos críticos de la organización.

Colocando estos servicios como nuestro objetivo principal de recuperación frente a una eventualidad, la herramienta PILAR nos permite colocarlos como objetivo y automáticamente catalogará el estado de los servicios de los que dependen. Así si algún servicio dependiente está como requerido podemos colocar la estrategia de continuidad que se escogerá y el tiempo que la misma conseguirá rehabilitar el servicio, así lograremos el objetivo de tener disponible en el tiempo establecido los servicios objetivos.

Las estrategias se determinan para cada grupo de activos que se requiere para lograr los objetivos establecidos y que no están listos, según el grupo de activos se estableció una o varias estrategias que se muestran en el siguiente cuadro:

Capa Activos	Activos	Objetivo	Estrategia	Descripción Estrategia
Instalaciones	Centro de Datos	Garantizar el espacio físico adecuado para levantar la infraestructura tecnológica necesaria para restaurar las operaciones.	Otra sede propia	Centro de datos alternativo en la localidad de Guayaquil (CDAG)
Instalaciones	Oficinas	Contar con instalaciones disponibles para reubicar los puestos de trabajo	Otra sede propia	Oficinas alternativas en la localidad de Quito en las instalaciones de las Operaciones Comerciales (OAQ)
Equipamiento	Hardware (servidores)	Garantizar la disponibilidad de los servidores necesarios para soportar las actividades críticas	Equipos dedicados	Servidores dedicados en el CDAG
			Equipos en otras funciones en otra sede propia	Equipos existentes en las OAQ dedicados en la operación diaria en otras funciones
Equipamiento	Hardware (equipos de computación)	Contar con los equipos de cómputo necesarios para reanudar las actividades críticas	Proveedor preferente	Proveedor preferente de hardware que renta equipos de computación que se solicitarán de ser necesario en caso de contingencia para instaurar nuevas oficinas en las OAQ

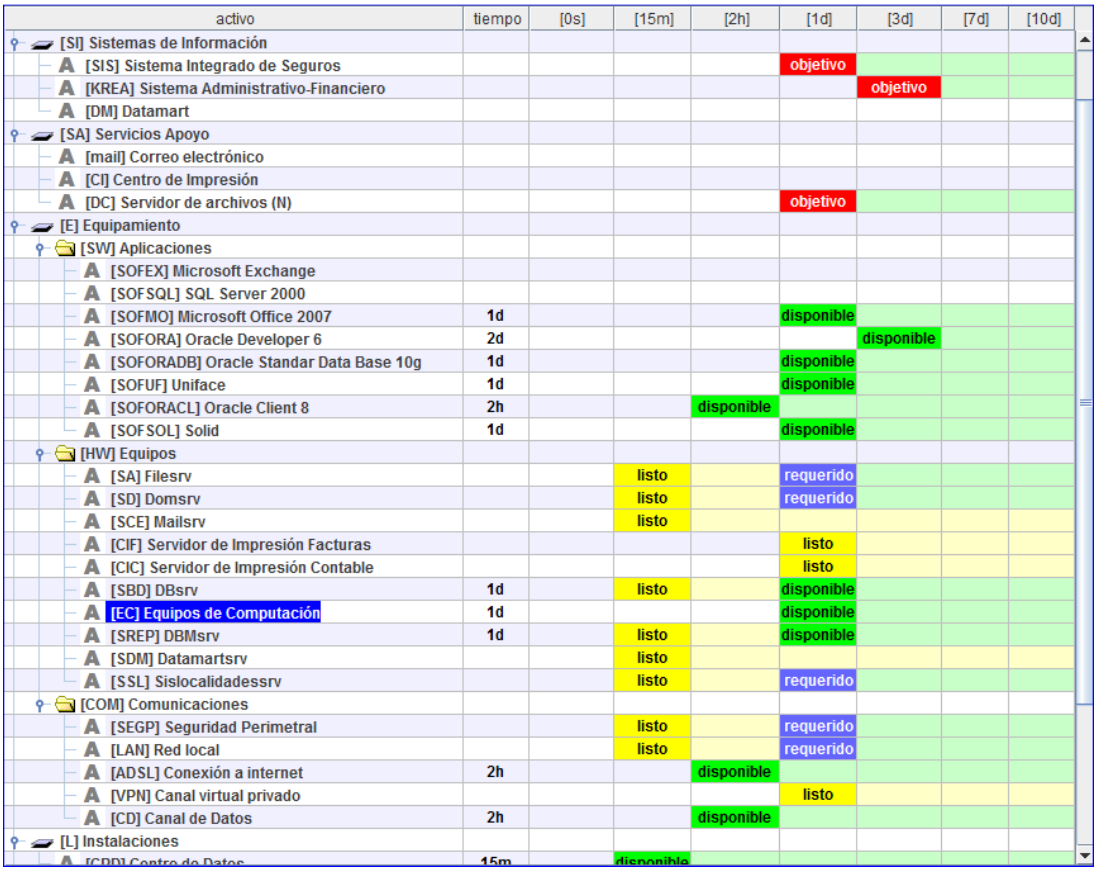
Capa Activos	Activos	Objetivo	Estrategia	Descripción Estrategia
Equipamiento	Comunicaciones	Disponer de una red alternativa que permita la disponibilidad de las comunicaciones	Red alternativa de conmutación manual con acuerdos de servicio (SLA) con un proveedor	Red alternativa con un proveedor, con un SLA de 2 horas fuera de servicio en caso de contingencia luego de la notificación para la activación del uso de la línea alternativa
Datos	Datos Sistemas de Información	Contar con la información de los sistemas con un RPO de un día.	Backup de la información	Realizar un respaldo diario con la metodología abuelo, padre, hijo de los datos de los sistemas de información
Datos	Manuales Técnicos	Contar con la documentación de las actividades críticas	Copias electrónicas en otra sede propia	Copias electrónicas de los manuales técnicos CDAG
Datos	Claves de Administración	Contar con las claves que permitan la administración de los servicios	Copias en papel en otra sede propia	Copias en papel en la caja fuerte de las OAQ
Datos	Medios de Instalación	Garantizar la disponibilidad de los medios de instalación del software que soporta los	Copias electrónicas en otra sede propia	Copias electrónicas de los medios de instalación en el CDAG

Capa Activos	Activos	Objetivo	Estrategia	Descripción Estrategia
		procesos críticos		
Personal	Jefe de Operaciones	Garantizar la	Prestación de personal formado	Servicios de un proveedor de técnicos especializados (ej. DBA), con un contrato con SLA.
Personal	Asistente de Operaciones	Mantener el conocimiento y las capacidades del personal en las actividades críticas	Personal alternativo propio de formación genérica	Actualización periódica al personal del área de Desarrollo de Software en las actividades críticas

Tabla 3 – 01: Cuadro de Estrategias de Continuidad [A]

Luego de ingresar las estrategias planteadas para cada servicio requerido podemos verificar que todos los servicios de los que dependen los servicios objetivos estén listos o disponibles en el tiempo requerido.

Para revisar el drp se debe cargar el archivo drp.drp ajdunto al documento.



activo	tiempo	[0s]	[15m]	[2h]	[1d]	[3d]	[7d]	[10d]
[SI] Sistemas de Información								
[SIS] Sistema Integrado de Seguros					objetivo			
[KREA] Sistema Administrativo-Financiero						objetivo		
[DM] Datamart								
[SA] Servicios Apoyo								
[mail] Correo electrónico								
[CI] Centro de Impresión								
[DC] Servidor de archivos (N)					objetivo			
[E] Equipamiento								
[SW] Aplicaciones								
[SOFEX] Microsoft Exchange								
[SOFSQL] SQL Server 2000								
[SOFMO] Microsoft Office 2007	1d				disponible			
[SOFORA] Oracle Developer 6	2d					disponible		
[SOFORADB] Oracle Standar Data Base 10g	1d				disponible			
[SOFUF] Uniface	1d				disponible			
[SOFORACL] Oracle Client 8	2h			disponible				
[SOFSOL] Solid	1d				disponible			
[HW] Equipos								
[SA] Filesrv			listo		requerido			
[SD] Domsrv			listo		requerido			
[SCE] Mailsrv			listo					
[CIF] Servidor de Impresión Facturas					listo			
[CIC] Servidor de Impresión Contable					listo			
[SBD] DBsrv	1d		listo		disponible			
[EC] Equipos de Computación	1d				disponible			
[SREP] DBMsrv	1d		listo		disponible			
[SDM] Datamartsrv			listo					
[SSL] Sislocalidadessrv			listo		requerido			
[COM] Comunicaciones								
[SEGP] Seguridad Perimetral			listo		requerido			
[LAN] Red local			listo		requerido			
[ADSL] Conexión a internet	2h			disponible				
[VPN] Canal virtual privado					listo			
[CD] Canal de Datos	2h			disponible				
[L] Instalaciones								
[CDD] Centro de Datos	15m		disponible					

Figura 3 - 01: Plan de recuperación para los servicios objetivo [A]

3.2. Desarrollo del Plan de Continuidad de los Servicios de TI

Luego de haber realizado el análisis de riesgos, el impacto en el negocio y establecer las estrategias de continuidad podemos realizar la construcción del plan de continuidad para los servicios de TI.

3.2.1. Organización de los Equipos

Los equipos de emergencia se conforman de acuerdo al tamaño de la organización y deberán cumplir con los procedimientos descritos en el plan para cada equipo. En la conformación de los equipos una persona puede pertenecer a varios equipos, siempre y cuando las actividades que deba desarrollar sean compatibles, esta conformación también dependerá del tamaño de la organización ya que si mientras más pequeña sea la organización los equipos también contarán con un número menor de integrantes.

Estableceremos 4 equipos que serán: el equipo director, el equipo de recuperación, equipo de logística y el equipo de pruebas. Cada equipo tendrá sus integrantes y sus funciones.

En cada equipo habrá un líder, el mismo que debe contar con suplente en caso que el líder no esté disponible y se debe tener la información de todos los miembros del equipo.

Para recopilar la información de los integrantes se crearon plantillas en las cuales se llenarán los datos necesarios para poder contactar a los miembros del grupo y que conformarán la primera parte del plan de continuidad.

A continuación se muestra de manera gráfica cual es el modelo de comunicación entre los diferentes equipos.

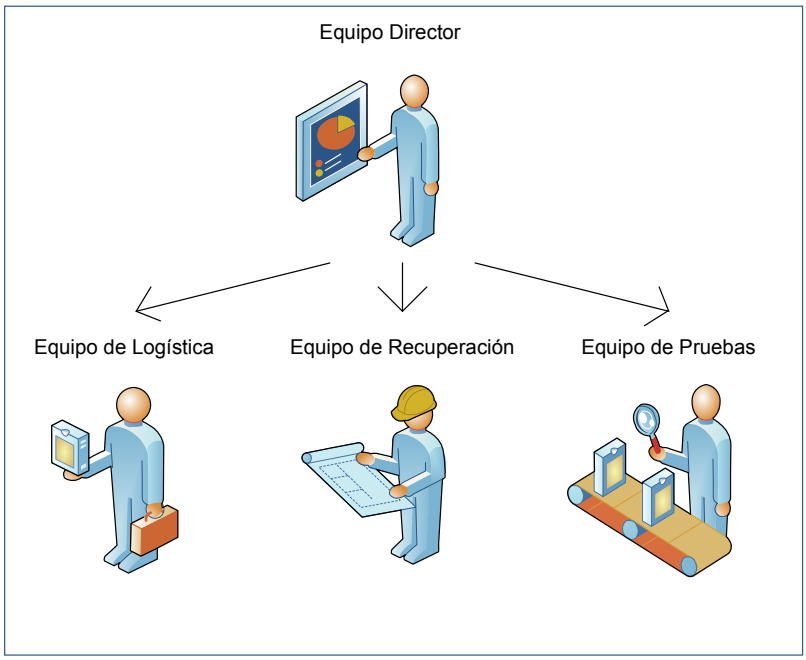


Figura 3 - 02: Árbol de llamadas [A]

3.2.2. Desarrollo de Procedimientos

Los procedimientos de recuperación deben recoger las actividades que se realizarán por cada equipo en caso de una contingencia. El procedimiento describe para cada fase el evento que se realizará con detalle así como el responsable de cada evento y si existe también indicará el registro que deberá elaborarse de esa actividad. A continuación se presenta un esquema del procedimiento a seguir desde la materialización de la incidencia hasta la decisión de activar o no el plan de continuidad de los servicios de TI.

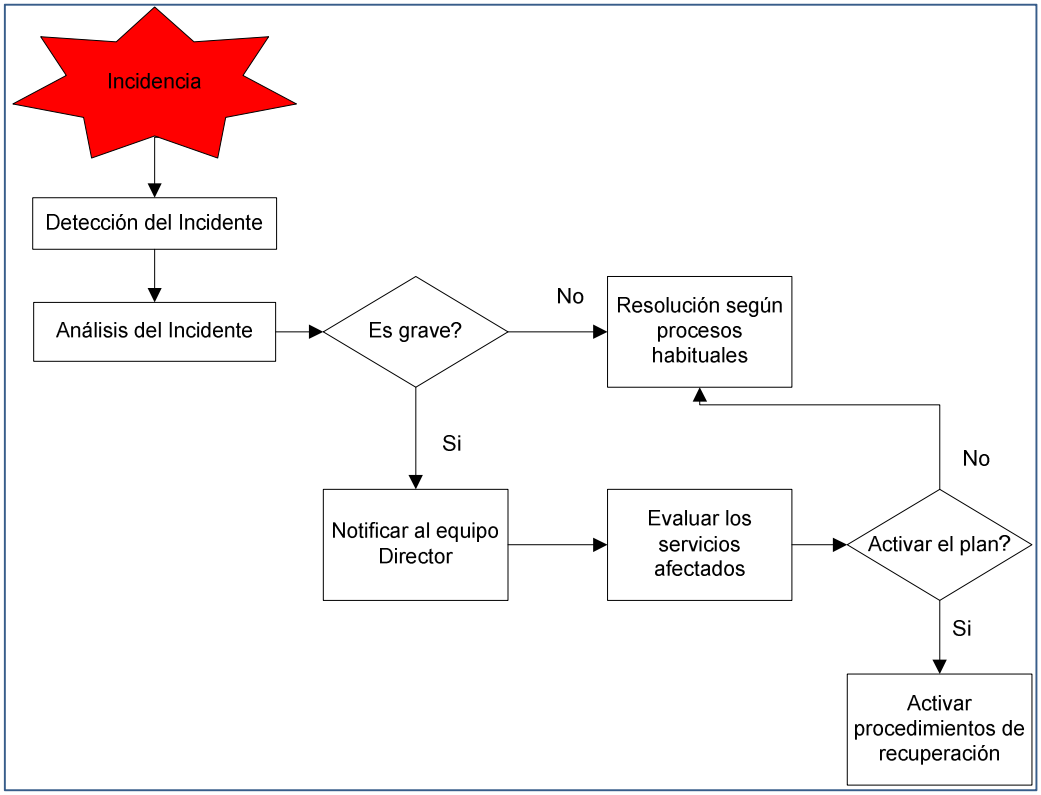


Figura 3 - 03: Procedimiento de acción en caso de incidencia [A]

Luego que se ha decidió activar el plan de continuidad de servicios de TI podemos dividir los procedimientos en 4 fases que abarcan el ciclo del plan desde la activación hasta la vuelta a la normalidad de las operaciones, estas fases son:

- Fase de Alerta
- Fase de Transición
- Fase de Recuperación
- Fase de Vuelta a la Normalidad

3.2.2.1. Fase de Alerta

En esta fase se definirán los procedimientos de actuación frente al inicio del incidente sea que implique la pérdida total o parcial de uno o varios servicios críticos, en el procedimiento de esta

fase se detallarán las actividades que se realizarán desde que se produce la incidencia hasta la notificación de la misma, así como los integrantes y el registro del evento si fuese necesario.

3.2.2.2. Fase de Transición

Esta es la fase previa a la recuperación de los servicios de TI y es importante la coordinación entre los equipos y el equipo de logística que será el encargado de proveer las herramientas de logística necesarias para la recuperación de los servicios. En esta fase se definirán las actividades necesarias para que el equipo de logística dote de las herramientas necesarias a los diferentes equipos para poder trabajar posteriormente en la recuperación de servicios.

3.2.2.3. Fase de Recuperación

Esta es la fase en la cual se recuperarán el(os) servicio(s) de TI que se han visto afectados con la incidencia, esta fase es fundamental ya que serán las actividades descritas en esta fase las que logren reactivar los servicios suspendidos.

3.2.2.4. Fase de Vuelta a la Normalidad

Luego que los procesos críticos han sido puestos en marcha y verificado su funcionamiento, se deben establecer las acciones para la volver a la normalidad, es decir para volver a operar normalmente.

4. Capítulo IV: Evaluación del Plan de Continuidad de los Servicios de TI

En este capítulo se detallará como se puede realizar la evaluación del plan de continuidad de los servicios de TI, la evaluación es una parte fundamental del plan ya que la evaluación continua permite conocer la efectividad del plan y los ajustes que se deben realizar al mismo.

4.1. Justificación de la Evaluación

Finalmente y para poder verificar la eficacia del plan de continuidad de los servicios de TI se deben realizar pruebas periódicas que permitan evaluar el mismo.

Los propósitos de evaluar un plan de continuidad son múltiples, y a continuación se muestran los principales:

- Asegurar la mejora continua del plan.
- Actualizar el plan de acuerdo a los cambios de la organización.
- Identificar aspectos que no fueron cubiertos inicialmente.
- Determinar debilidades del plan y fortalecerlas.
- Entrenar al personal en el procedimiento en caso de contingencia.
- Incrementar la conciencia y conocimiento del plan.
- Verificar la disponibilidad de los datos y recursos críticos almacenados fuera del sitio.

La evaluación del plan no puede ni debe realizarse en una única ocasión, por lo que las evaluaciones deben ser parte de un calendario establecido con el alcance o escenarios que se va a evaluar.

4.2. Pruebas de Continuidad de los Servicios Críticos de TI

Existen varios tipos de pruebas que se puede realizar para valorar un plan de continuidad de servicios de TI entre los cuales tenemos: pruebas aisladas, pruebas en línea y pruebas en paralelo.

Pruebas aisladas: este tipo de pruebas consiste en provocar intencionalmente o simular una amenaza que permita activar el plan de continuidad como por ejemplo un terremoto, robo de hardware, etc.

Pruebas en línea: este tipo de pruebas se las realiza mientras los activos de TI operan normalmente, y se interrumpe su servicio, la interrupción puede realizarse contemplando distintos escenarios que se pueden construir en base a las pruebas que se quiera realizar por ejemplo interrupción de la red interna LAN, etc.

Pruebas en paralelo este tipo de pruebas permiten la normal operación de los servicios de la organización ya que solamente una parte de la operación se simulará un estado de contingencia. Por ejemplo errores en la realización de copias de respaldo, ataques a la red privada VPN, etc.

Cualquiera sea el tipo de pruebas que se decida realizar, estas pruebas deben planificarse, registrarse y documentarse para que de esta manera se puedan realizar los ajustes y modificaciones correspondientes al plan de continuidad de servicios de TI.

4.2.1. Planificación de las Pruebas

La planificación de las pruebas debe realizarse con la debida antelación y calendarizando todas las actividades que implica realizar las pruebas.

En la planificación de las pruebas se debe tener en cuenta los siguientes aspectos:

- Qué tipo de pruebas se van a realizar.
- Qué activos de TI se va a someter a prueba.
- En qué fechas se realizarán las pruebas y que tiempo destinaré para las pruebas.

Las pruebas deben ser periódicas, por lo que la planificación que se realice debe ser para un período de tiempo puede ser un trimestre, semestre o un año, ya que si solo se planifica las pruebas que realizará en un momento determinado se puede correr el riesgo que las

actividades urgentes del día a día de la organización no permitan realizar las pruebas al plan y se convierta en un documento obsoleto.

Para la realización de la planificación, teniendo en cuenta los principales puntos se adjunta una plantilla en el anexo 4 con nombre **"**Planificación de pruebas del plan de continuidad de Servicios de TI**"**.

4.2.2. Registro de las Pruebas

Es necesario llevar un registro de las pruebas que se realizan al plan de continuidad de servicios de TI, esto nos permitirá al final de un periodo establecer puntos importantes como cuantas pruebas realizamos, si las pruebas fueron satisfactorias, si se ajustó el plan luego de las pruebas, etc.

Para el registro de las pruebas se adjunta el formato que permitirá llevar el control de la información obtenida como resultado de cada prueba en el anexo 4 con nombre **"**Registro de Pruebas del Plan de Continuidad de Servicios de TI**".**

4.2.3. Documentación de las Pruebas

Cada vez que se realicen las pruebas al plan de continuidad de servicios de TI se debe documentar dichas pruebas ya que el posterior análisis de la información obtenida permitirá conocer la efectividad del plan y los ajustes si los hubiera que se pueden realizar al plan, además como debilidades en los activos de TI que se pueden encontrar y también corregir.

Para documentar las pruebas realizadas se adjunta el formato en el anexo 4 con nombre **"**Documentación de pruebas del Plan de Continuidad de Servicios de TI**".**

5. Capítulo V: Conclusiones y Recomendaciones

En el capítulo cinco se detallarán las conclusiones y recomendaciones que se recogieron a lo largo del desarrollo del presente proyecto como un aporte a todos los interesados.

5.1. Conclusiones

- ✓ Al generar el informe de insuficiencias todavía existen puntos que se deben fortalecer pese a las salvaguardas implementadas, la lista de insuficiencias que influyen en que el nivel del riesgo sea mayor para ciertos activos.

- ✓ Al contar con un plan de continuidad de negocio para servicios de TI cada miembro de los equipos sabe cómo proceder y el papel que debe desempeñar en caso de contingencia, lo que permite una reanudación oportuna y ordenada de los servicios.

- ✓ El plan de continuidad de servicios de TI debe ser evaluado y actualizado periódicamente para que sea efectivo, por lo que requiere una calendarización y planificación de las pruebas que se ejecutarán.

- ✓ Con la creciente automatización de procesos y el aumento del uso de herramientas informáticas como apoyo para los diferentes procesos de las organizaciones, es necesario contar con un plan de continuidad de negocio que permita garantizar la disponibilidad de los mismos.

- ✓ En el país existen empresas de seguros que pese a que su negocio se basa en servicios de TI no cuentan con un plan de continuidad que les permita mantener sus operaciones en caso de una contingencia, lo que significa un riesgo alto para la empresa.

5.2. Recomendaciones

- ✓ Se debe trabajar en mitigar las insuficiencias reportadas para mitigar los riesgos, si la Cía no tiene los recursos para realizarlo en ninguna de las fases establecidas inicialmente (6 meses y 1 año), posteriormente al cumplir las fases se puede hacer una actualización al análisis y gestión de riesgos para analizar la factibilidad de establecer nuevas o mejorar las salvaguardas que permitan mitigar las insuficiencias.

- ✓ Se debe actualizar el plan de continuidad de servicios de TI para garantizar su efectividad, mejora continua y evolución paralelamente con los cambios de la organización.

- ✓ El plan de continuidad debe ser sociabilizado y practicado por los colaboradores de la organización y la mejor manera es hacerlo mediante las pruebas periódicas.

- ✓ La Pontificia Universidad Católica del Ecuador debería contar con un plan de continuidad de servicios críticos de tecnologías de información que le permitan mantener sus actividades en caso de una contingencia.

- ✓ Los Ingenieros Informáticos debemos concientizar al alto mando de las empresas en las cuales colaboramos la importancia que tiene la elaboración de un plan de continuidad de servicios de TI para garantizar las operaciones de la empresa en caso de una contingencia.

Referencias

[A] Construcción de un Plan de Continuidad de Servicios de Tecnología de Información para una empresa de Seguros, Ingrid Cadena, PUCE, 2012.

[B] Planes de Contingencia, Juan Gaspar Martínez, Editorial Díaz Santos S.A., Madrid, 2004.

[C] Official $(ISC)^2$ Guide to the CISSP CBK, $(ISC)^2$ Security Transcends Technology, Edited by Harold F. Tipton, 2007, pp 1065.

[D] ISO, ISO/IEC 17799, Junio 15, 2006, Segunda Edición, pp 170.

[E] ISO, ISO/IEC 27001, Octubre 15, 2005, Primera Edición, pp 40.

[F] Ministerio de Administraciones Públicas, MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información I – Método, Madrid, Junio 20, 2006, Versión 2.

[G] Ministerio de Administraciones Públicas, MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información II – Catálogo de Elementos, Madrid, Junio 20, 2006, Versión 2.

[H] Ministerio de Administraciones Públicas, MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información III – Guía de Técnicas, Madrid, Junio 20, 2006, Versión 2.

[I] Ministerio de Administraciones Públicas, Guía de Seguridad de las TIC Manual de Usuario Pilar Basic, Madrid, Abril, 2011, Versión 5.1, pp 108.

[1] Iso27002, El Anexo de ISO 27001 en español, Aglone3, versión 1.2, URL: http://iso27002.es/

[2] José Manuel Huidobro, Tecnología de Información y Comunicación, Universidad Politécnica de Madrid, URL: http://www.monografias.com/trabajos37/tecnologias-comunicacion/tecnologias-comunicacion.shtml#queson

[3] Gabriel G, Características de las TIC's, Septiembre 2, 2009, URL: http://kalistog.wordpress.com/133-2/

[4] Fundación Wikimedia, Inc., Tecnologías de la información y la comunicación, 25 ago 2012, URL:http://es.wikipedia.org/wiki/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_la_comunicaci%C3%B3n

[5] Osiatis S.A., ITIL-Gestión de Servicios TI, versión 2.0, URL: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_niveles_de_servicio/caso_practico_gestion_de_niveles_de_servicio/caso_practico_gestion_de_niveles_de_servicio.php

[6] Soporte Remoto de México, La importancia de producir un Catálogo de Servicios, 2008, URL: http://www.soporteremoto.com.mx/help_desk/articulo03.html

[7] DELTA, Planes de Continuidad / Contingencia, URL: http://www.deltaasesores.com/servicios/tecnologia-informatica/1259-planes-de-continuidad-contingencia

[8] Security advisor, Servicio de Continuidad de TI, 2012, URL: http://www.sadvisor.com/servicios/servicios_masinfo.php?id=75&secc=servicios

[9] Business Continuity Institute, The Good Practices Guidelines 2010, Global Edition, URL: http://www.thebci.org/index.php?option=com_content&view=article&id=60&Itemid=98

[10] Alto Nivel, @altonivel, Diseña un catálogo de servicios de TI, mauo 31, 2010, URL: http://www.altonivel.com.mx/disena-un-catalogo-de-servicios-de-ti.html

[11] Alejandro Núñez Sandoval, Estándares de seguridad en la información, Febrero 2005, Número 36, Año 4, URL: http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

[12] Egdares Futch, Continuidad de Negocios: Componente importante de la Seguridad de la Información, Jun 26, 2009, URL:http://www.slideshare.net/efutch/continuidad-de-negocios

[13] ITCIO.ES Recursos e Información Tecnológica Empresarial para CIOs, Qué debe incluir su Plan de Continuidad de Negocio?, Julio 15, 2008, URL: http://www.itcio.es/planes-contingencia/informes/1004787016902/debe-incluir-plan-continuidad-negocio.1.html

[14] Leonardo Camelo, Análisis de Impacto de Negocios / Business Impact Analysis (BIA), Mayo 30, 2010, URL: http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html

Anexos

Anexo 1: Informe de insuficiencias

Informe de insuficiencias

proyecto: [BCP_TI] Plan_Continuidad_TI

phase: [1Y] plan de seguridad

clasificación: DIFUSIÓN LIMITADA

Relación de salvaguardas que adolecen de un nivel de eficacia inferior a "L2 - reproducible, pero intuitivo".

1. Datos del proyecto

BCP_TI	Plan_Continuidad_TI
descripción	Plan de continuidad de servicios de TI
responsable	Ingrid Cadena
organización	Empresa de Seguros de Ecuador
versión	1.0
fecha	04/01/2012
biblioteca	[std] Biblioteca INFOSEC (23.3.2011)

Licencia

[demo] icadena@seguroscolvida.com
[... 27.5.2012]

Niveles de madurez

- L0 - inexistente

- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

2. Dominios de seguridad

- [base] Base

3. Fases del proyecto

- [1Y] plan de seguridad

4. Dominio de seguridad: [base] Base

4.1. [H] Protecciones Generales

Salvaguarda	aspecto	recomendación	[1Y]
[H3] Segregación de tareas	T	8	L1-L5
[H31] Todos los procesos críticos requieren al menos 2 personas	T	8	L2
[H33] Se controla la efectividad de la estructura de segregación	T	7	L1-L5
[H332] Se monitorizan todas las operaciones	T	7	L1
[H333] Se impide que alguien pueda autorizarse a sí mismo	T	6	L2
[H334] Se impide que los operadores puedan modificar datos de explotación	T	6	L1
[H335] Se impide que los operadores puedan realizar transacciones	T	6	L2

[H33c] Se revisan los periodos de vacaciones previstos de los operadores y programadores	T	6	L2
[H33e] Hay seguridad de que en todo momento hay más de un operador	T	6	L2
[H4] Gestión de incidencias	G	8	L1-L4
[H48] Gestión de la incidencia	G	8	L1-L3
[H5] Herramientas de seguridad	T	10	L0-L4
[H51] Herramienta contra código dañino	T	10	L1-L3
[H513] Se revisan los programas y servicios de arranque del sistema	T	7	L1
[H514] Se revisa cada aplicación cuando arranca	T	7	L1
[H518] Se revisan los ficheros recibidos en un medio removible	T	7	L1
[H53] Herramienta de monitorización de tráfico	T	7	L1-L4
[H538] Disparo de alarmas en tiempo real	T	7	L2
[H55] Herramienta de análisis de vulnerabilidades	T	8	L1-L3
[H553] Se revisa el sistema operativo	T	8	L1
[H554] Se revisan las aplicaciones base del sistema	T	7	L1
[H555] Se revisan las aplicaciones específicas de la organización	T	6	L2
[H57] Honey net / honey pot	T	7 (o)	L0
[H573] Se controlan las acciones de los usuarios para evitar ataques a otros sistemas	T	6	L0
[H579] {xor} Se gesionan las alertas que se produzcan	T	6	L0
[H5791] Las alertas se tratan automáticamente	T	6	L0

[H5792] Existe personal dedicado a la monitorización del sistema en tiempo real	T	6	L0
[H57a] Se emplea un producto certificado o acreditado	T	7	L0

4.2. [D] Protección de la Información

No existen insuficiencias con recomendación igual o mayor a 6

4.3. [S] Protección de los Servicios

Salvaguarda	**aspecto**	**recomendación**	**[1Y]**
[S3] Aseguramiento de la disponibilidad	G	6	L1-L3
[S31] Se han previsto protecciones frente a ataques de denegación de servicio (DoS)	G	6	L1-L3
[S313] Se han dimensionado los dispositivos accesibles (cortafuegos, servidores, ...) para soportar la máxima carga prevista	G	6	L1
[S317] Se toman medidas frente a ataques originados en las propias instalaciones	G	6	L1-L3
[S3172] Medidas de detección de ataques	G	6	L1
[S3173] Medidas reactivas para bloquear el ataque	G	6	L1
[S3174] Medidas disciplinarias contra el causante	G	6	L1

[S33] Continuidad de operaciones	G	6	L1
[S333] Se dispone de medios alternativos	G	6	L1
[S6] Se aplican perfiles de seguridad	T	7	L1-L3

4.4. [SW] Protección de las Aplicaciones Informáticas (SW)

Salvaguarda	**aspecto**	**recomendación**	**[1Y]**
[SW5] Copias de seguridad (backup) (SW)	G	7	L1-L5
[SW54] Las copias de seguridad se protegen de acuerdo al SW que contienen	G	6	L1
[SW55] Regularmente se verifica que las copias pueden ser restauradas correctamente	G	6	L1
[SW56] Las copias de seguridad se almacenan en lugares alternativos	G	7	L1
[SW6] Adquisición o desarrollo	G	7	L0-L5
[SW65] Desarrollo	G	7	L0-L5
[SW651] Metodología de desarrollo	G	6	L1-L5
[SW6511] Se tiene en cuenta la seguridad durante todo el ciclo de desarrollo	G	6	L1-L5
[SW65113] Mecanismos de registro y auditoría	G	6	L2
[SW65114] Soporte de la confidencialidad requerida	G	6	L1
[SW653] Código fuente	G	7	L0-L4
[SW6536] Se controla la realización de copias de seguridad del código fuente	G	6	L2
[SW6537] El código fuente no está accesible en los sistemas en producción	G	6	L1

[SW655] Entorno de pruebas (pre-producción)	G	6	L1-L5
[SW6556] Pruebas de penetración	G	6	L1
[SW8] Se aplican perfiles de seguridad	T	8	L1-L3
[SW9] Explotación / Producción	G	7	0
[SWa] Cambios (actualizaciones y mantenimiento)	G	6	L0-L4

4.5. [HW] Protección de los Equipos Informáticos (HW)

salvaguarda	**aspecto**	**recomendación**	**[1Y]**
[HW7] Aseguramiento de la disponibilidad	G	7	L1-L4
[HW72] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	G	6	L1
[HWa] Operación	G	6	L0-L4
[HWa5] Protección de los dispositivos de red	G	6	L0-L4

4.6. [COM] Protección de las Comunicaciones

Salvaguarda	**aspecto**	**recomendación**	**[1Y]**
[COM6] Se aplican perfiles de seguridad	T	8	L1
[COM63] Se eliminan, o modifican, las cuentas estándar de administrador	T	8	L1
[COM64] Los servicios activados se configuran de forma segura	T	7	L1
[COM7] Aseguramiento de la disponibilidad	G	8	L1
[COM71] Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)	G	8	L1
[COM72] Se dimensiona holgadamente y se	G	6	L1

planifica la adquisición de repuestos			
[COM73] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	G	6	L1
[COM74] Se monitorizan enlaces y dispositivos de red	G	6	L1
[COM78] Se hacen copias de seguridad de las claves de autenticación	G	7	L1
[COM79] Se hacen copias de seguridad de las claves de descifrado	G	7	L1
[COM7a] {xor} Garantías de disponibilidad	T	7	L1
[COM7a1] Se dispone de conexión redundante (mediante doble tarjeta de red) de los dispositivos críticos	T	7	L1
[COM7a2] Redundancia de los enlaces con esquema activo-pasivo, incluyendo los dispositivos de red	T	7	L1
[COM7a3] Redundancia de los enlaces con reparto de carga, incluyendo los dispositivos de red	T	7	L1
[COM7a4] Redundancia de los enlaces, con dispositivos de red tolerantes a fallos (doble CPU, doble fuente de alimentación, y doble interfaz de red)	T	7	L1
[COM7a5] Dispositivos de red tolerantes a fallos (doble CPU, doble fuente de alimentación)	T	7	L1
[COMf] Seguridad Wireless (WiFi)	G	7	L1-L4

4.7. [SI] Protección de los Soportes de Información

No existen recomendaciones

4.8. [AUX] Elementos Auxiliares

Salvaguarda	**aspecto**	**recomendación**	**[1Y]**
[AUX4] Suministro eléctrico	F	7	L1-L3
[AUX44] Interruptor general de la alimentación del sistema situado en la entrada de cada área	F	7	L1
[AUX45] Interruptores etiquetados y protegidos frente a activaciones accidentales	F	7	L2
[AUX46] Alimentación de respaldo	F	7	L1-L2
[AUX5] Climatización	F	7	L1
[AUX52] Control de temperatura	F	7	L1
[AUX53] Control de humedad	F	7	L1
[AUX55] Sistema de climatización redundante	F	7	L1
[AUX6] Protección del cableado	F	8	L1
[AUX61] La gestión está centralizada	F	6	L1
[AUX62] Se utiliza una herramienta de gestión	F	6	L1
[AUX66] Se realiza un mantenimiento regular del cableado	F	6	L1
[AUX67] Se ha segregado el cableado de alimentación del de comunicaciones para evitar interferencias	F	7	L1
[AUX68] Se evitan rutas a través de áreas públicas	F	7	L1
[AUX69] Se controlan todos los accesos al	F	8	L1

cableado			
[AUX6a] Hay protección prevista contra daños o interceptaciones no autorizadas (conductos blindados, cajas o salas cerradas, ...)	F	8	L1
[AUX6b] Se protegen los cuadros de distribución	F	6	L1
[AUX6c] Se protejen antenas y repetidores	F	6	L1
[AUX6d] Se emplean recubrimientos que no son inflamables ni tóxicos	F	6	L1
[AUX6e] El cableado es tolerante a fallos (redundancia de líneas críticas, etc.)	F	8	L1
[AUX7] Contenedores de seguridad	F	7	L1
[AUX72] Cajas fuertes	F	7	L1
[AUX73] Cámaras acorazadas	F	7 (o)	L1
[AUX74] Armarios ignífugos	F	7	L1

4.9. [L] Protección de las Instalaciones

salvaguarda	**aspecto**	**recomendación**	**[1Y]**
[L2] **Se** dispone de un inventario de instalaciones	F	6	L2
[L25] Las áreas no se identifican en directorios telefónicos y vestíbulos	F	6	L2
[L26] El personal sólo conoce la existencia de estas áreas, o de sus actividades, si lo necesita para su trabajo	F	6	L2
[L3] Entrada en servicio	F	7	L1-L2
[L33] Se han determinado las acreditaciones o certificaciones pertinentes	F	7	L2

[L35] Plan de Protección	F	6	L1
[L353] Plan de Emergencia	F	6	L1
[L3533] Acceso físico a las instalaciones en caso de emergencia	F	6	L1
[L35332] Sólo se pueden utilizar los accesos autorizados	F	6	L1
[L4] Diseño	F	8	L1-L3
[L49] Se evita que el acceso físico para operación y mantenimiento abra el acceso a otros activos	F	8	L1
[L4e] Las instalaciones son discretas minimizando indicaciones sobre su propósito	F	6	L2
[L5] Control de los accesos físicos	F	8	L1-L3
[L51] Control de los accesos	F	7	L1-L3
[L516] Se investiga cualquier sospecha o intento de acceso físico no autorizado	F	7	L1
[L54] Los accesos permanecen cerrados fuera de las horas de trabajo	F	8	L1
[L55] Las áreas de trabajo se cierran y controlan periódicamente cuando están vacías	F	7	L1
[L56] Se exige que los puestos de trabajo están despejados	F	6	L1
[L57] Se evita el trabajo no supervisado	F	7 (o)	L1
[L58] Se prohiben equipos de registro (fotografía, video, audio, telefonía, etc.) salvo autorización especial	F	7	L1
[L9] Protección frente a desastres	F	8	L0-L3
[L92] Protección frente a incendios	F	8	L0-L1

[L922] Las áreas están compartimentadas (por sectores)	F	6	L0
[L923] Existen vías de evacuación	F	6	L1
[L925] Se dispone de un sistema de iluminación de emergencia	F	6	L1
[L926] Se dispone de un sistema de evacuación de humos	F	6	L0
[L92a] Se dispone de un plan de autoprotección	F	6	L0
[L92b] Se dispone de pulsadores de alarma	F	6	L1
[L92c] Se dispone de un sistema automático de detección de incendios	F	8	L1
[L92e] Se dispone de un sistema automático de extinción de incendios (sprinkler, etc.)	F	7	L0
[L92h] Se notifica automáticamente a los servicios de ayuda exterior de cualquier activación del sistema automático de detección de incendios	F	7	L0
[L92i] Se garantizan las condiciones adecuadas de aproximación para las fuerzas de ayuda exterior	F	6	L0
[L94] Protección frente a accidentes naturales e industriales	F	7	L1
[L943] Se selecciona el emplazamiento para minimizar el riesgo de accidentes naturales o industriales	F	7	L1
[L944] Se mantienen contactos periódicos con los responsables de las fuerzas de apoyo exterior	F	7	L1
[La] Continuidad de operaciones	F	8	L2-L3
[Lc] La seguridad de la instalación no es responsabilidad de un único guarda	F	8	L2

4.10. [P] Gestión del Personal

Salvaguarda	aspecto	recomendación	[1Y]
[P9] Aseguramiento de la disponibilidad	P	6	L1-L3
[P93] {or} Redundancia	P	6	L2
[P931] Otro personal propio ya formado	P	6	L2

4.11. [G] Organización

No existen insuficiencias con recomendación igual o mayor a 6

4.12. [E] Relaciones Externas

Salvaguarda	Aspecto	recomendación	[1Y]
[E1] Acuerdos para intercambio de información y software	G	6	L1-L3

5. Equipamiento de respaldo

Activo	[1Y]
[SIS] Sistema Integrado de Seguros	[2d] / L4
[KREA] Sistema Administrativo-Financiero	[1d] / L4
[DC] Servidor de archivos (N)	[1d] / L4

5.1.1. [SIS] Sistema Integrado de Seguros

[1Y] plan de seguridad

- [D.e-.lcl] copia local
- [SI.alt_prp] Equipo alternativo propio
- [SW.backup] Copia de seguridad
- [S.e_alt.prp] propio

5.1.2. [KREA] Sistema Administrativo-Financiero

[1Y] plan de seguridad

[S.e_alt.prp] propio

[SW.alt] Paquete informático alternativo

[D.e-.ext] copia externa en instalaciones propias

5.1.3. [DC] Servidor de archivos (N)

[1Y] plan de seguridad

[HW.prp.stored] dedicado (almacenado)

[D.e-.ext] copia externa en instalaciones

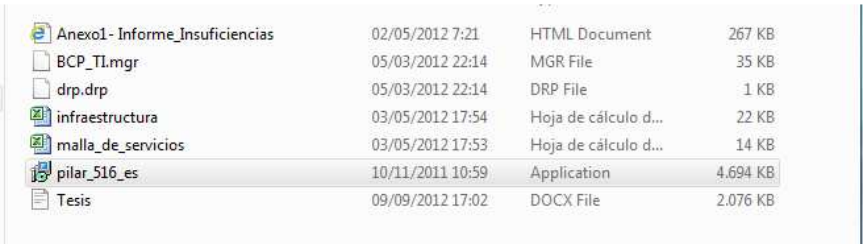
Anexo 2: Análisis y Gestión de Riesgos con Software MAGERIT PILAR

El análisis y la gestión del riesgo está realizado en el software MAGERIT PILAR, para lo cual se anexa a este documento los siguientes archivos digitales:

- ✓ Software de instalación MAGERIT PILAR: pilar_516_es.exe
- ✓ Análisis y Gestión de Riesgos y Análisis del Impacto en el negocio: **BCP_TI.mgr** con password **ingridtesis**
- ✓ Plan de recuperación de desastres: **DRP.drp** con password **Ingridtesis**

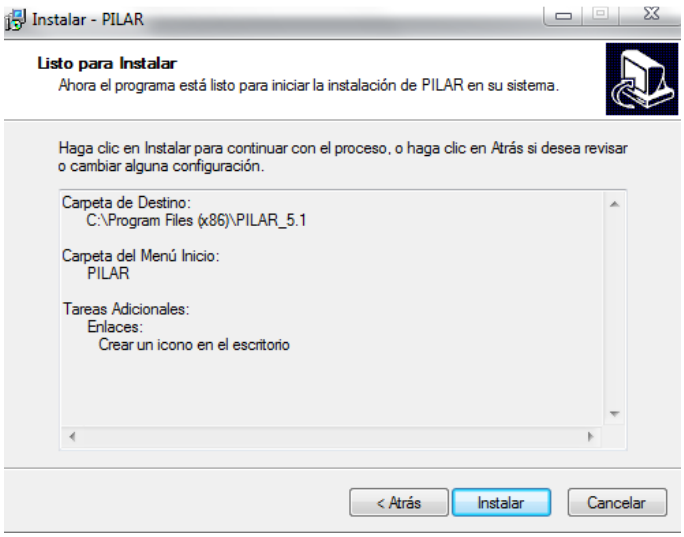
Instalación del Software MAGERIT PILAR

1. Dar doble clic en el instalador

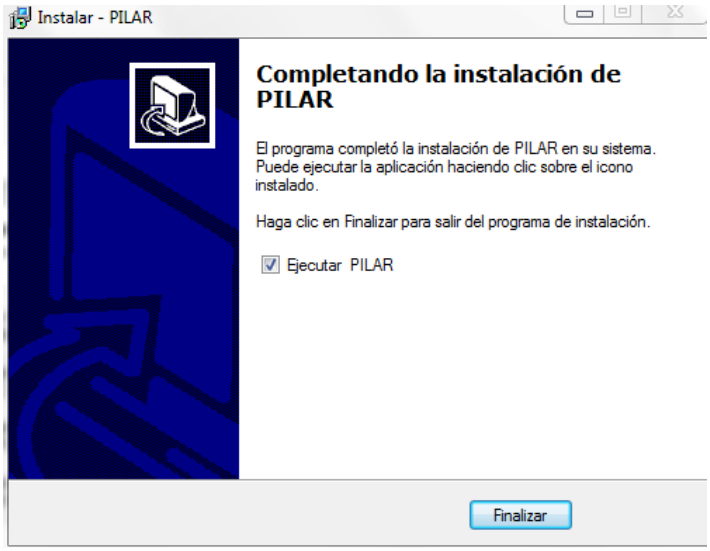


2. Dar clic en siguiente dejando todos los valores por defecto

3. Dar clic en instalar



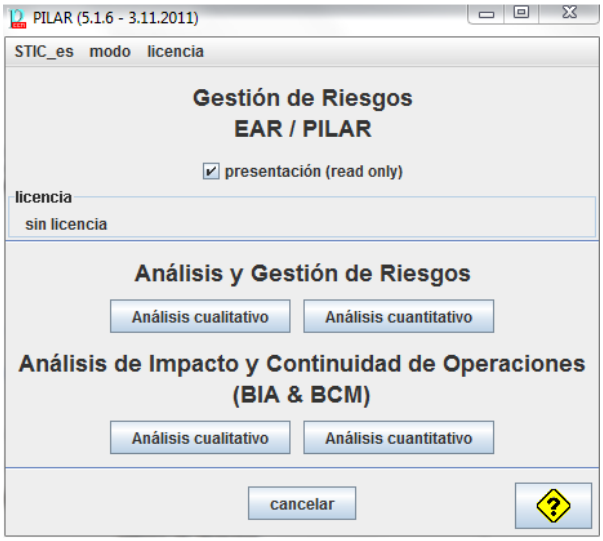
4. Dar clic en finalizar



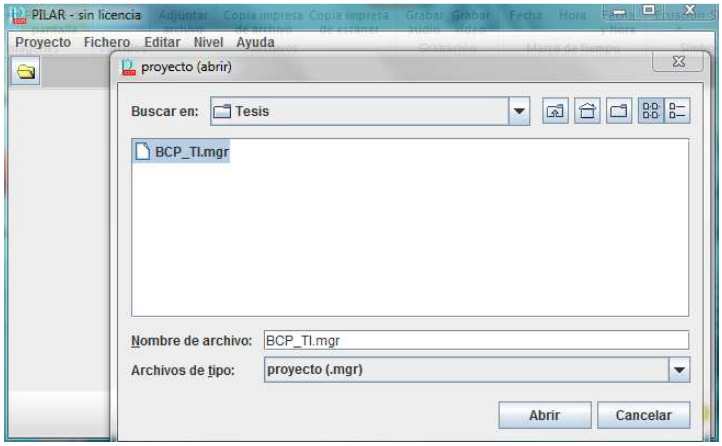
Análisis y Gestión de Riesgos con MAGERIT PILAR

1. Dar clic en el ícono de MAGERIT PILAR

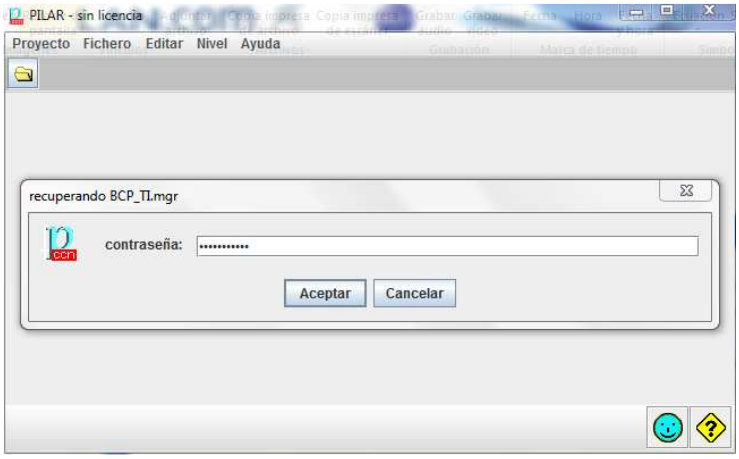
2. Seleccionar la opción de presentación (read only) y escoger la opción que se va a revisar sea Análisis y Gestión de Riesgos (análisis cualitativo).



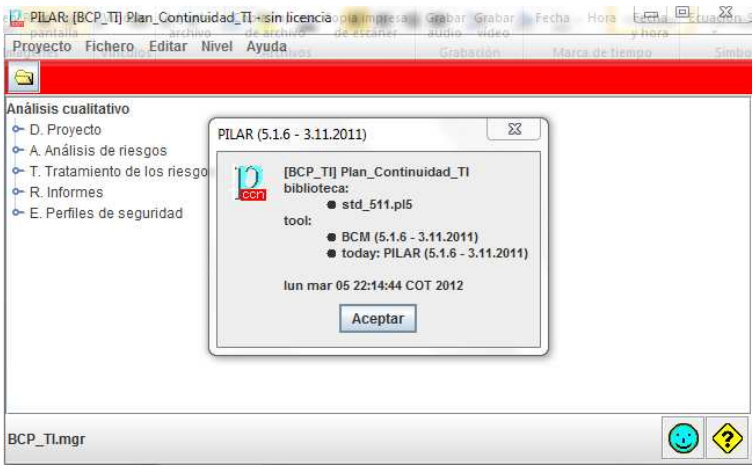
3. Escoger el archivo que se va a abrir **BCP_TI.mgr** y dar clic en abrir



4. Colocar la clave del archivo **tesisingrid**



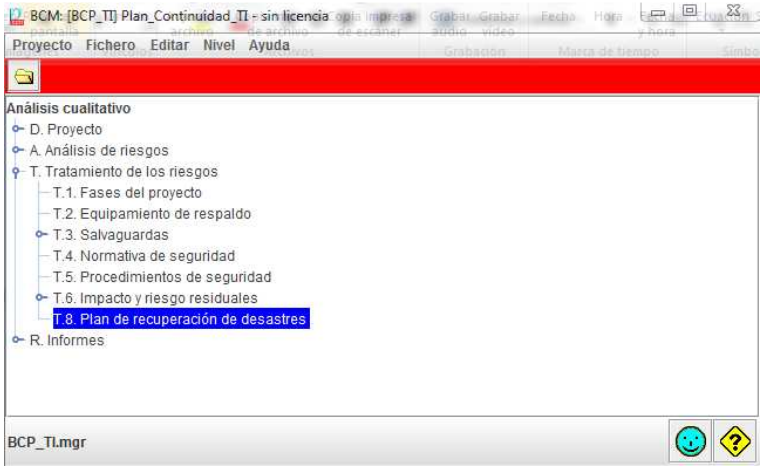
5. Dar clic en aceptar y luego se podrá revisar el análisis y la gestión de riesgos



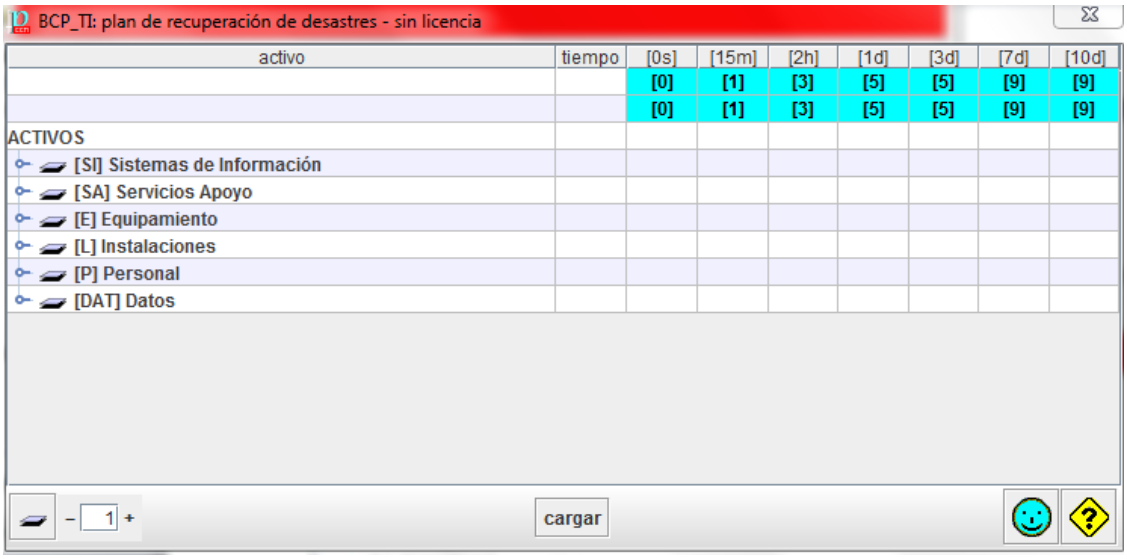
Análisis del Impacto al Negocio con MAGERIT PILAR

Realizar los mismos pasos que en el análisis y gestión de riesgos, excepto que en el paso 2 escoger la opción Análisis de Impacto y Continuidad en las Operaciones (análisis cualitativo).

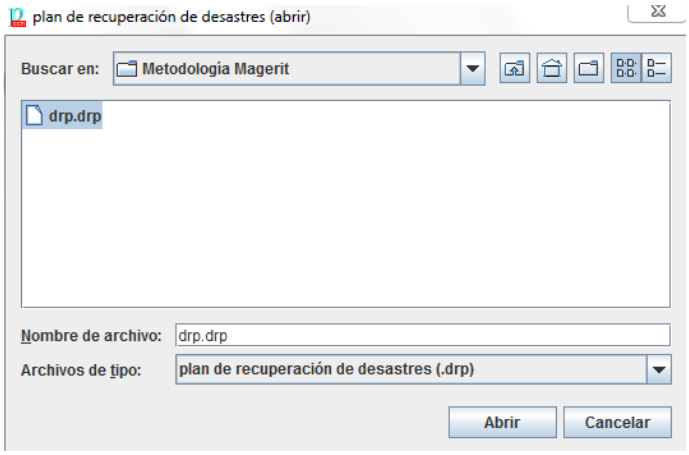
Adicionalmente para poder visualizar el plan de recuperación ante desastres debemos ir a la opción **T.8. Plan de recuperación de desastres.**



Luego damos clic en cargar



Escogemos el archivo en el cual está grabado el plan de recuperación ante desastres **drp.drp** e ingresamos la clave **tesisingrid**.



Y finalmente se puede revisar el plan de recuperación ante desastres.

activo	tiempo	[0s]	[15m]	[2h]	[1d]	[3d]	[7d]	[10d]
[SI] Sistemas de Información								
[SIS] Sistema Integrado de Seguros					objetivo			
[KREA] Sistema Administrativo-Financiero						objetivo		
[DM] Datamart								
[SA] Servicios Apoyo								
[mail] Correo electrónico								
[CI] Centro de Impresión								
[DC] Servidor de archivos (N)					objetivo			
[E] Equipamiento								
[SW] Aplicaciones								
[SOFEX] Microsoft Exchange								
[SOFSQL] SQL Server 2000								
[SOFMO] Microsoft Office 2007	1d				disponible			
[SOFORA] Oracle Developer 6	2d					disponible		
[SOFORADB] Oracle Standar Data Base 10g	1d				disponible			
[SOFUF] Uniface	1d				disponible			
[SOFORACL] Oracle Client 8	2h			disponible				
[SOFSOL] Solid	1d				disponible			
[HW] Equipos								
[SA] Filesrv			listo		requerido			
[SD] Domsrv			listo		requerido			
[SCE] Mailsrv			listo					
[CIF] Servidor de Impresión Facturas					listo			
[CIC] Servidor de Impresión Contable					listo			
[SBD] DBsrv	1d		listo		disponible			
[EC] Equipos de Computación	1d				disponible			
[SREP] DBMsrv	1d		listo		disponible			
[SDM] Datamartsrv			listo					
[SSL] Sislocalidadessrv			listo		requerido			
[COM] Comunicaciones								
[SEGP] Seguridad Perimetral			listo		requerido			
[LAN] Red local			listo		requerido			
[ADSL] Conexión a internet	2h			disponible				
[VPN] Canal virtual privado					listo			
[CD] Canal de Datos	2h			disponible				
[L] Instalaciones								
[CDD] Centro de Datos	15m		disponible					

Anexo 3: Plan de Continuidad de Servicios de TI para una Empresa de Seguros en Ecuador

El plan de continuidad de servicios de TI para una empresa de seguros en Ecuador se anexa digitalmente como documento adjunto con el nombre **Plan de Continuidad.docx**

Anexo 4: Evaluación del Plan de Continuidad de Servicios de TI

El este anexo se colocan todas las plantillas que apoyarán las actividades para la evaluación de un plan de continuidad para servicios de TI.

Planificación de Pruebas del Plan de Continuidad de Servicios de TI

Planificación: _____ **Fecha planificación:** _____

				Fechas de pruebas			
No.	**Tipo de Prueba**	**Activo/Servicio a probar**	**Escenario**	**Inicio**	**Fin**	**Responsable**	**Comentarios**

Realizado por: _____ Aprobado por: _____

Ingrid Cadena

Registro de Pruebas del Plan de Continuidad de Servicios de TI

No.	Tipo de Prueba	Activo/Servicio a probar	Escenario	Fecha pruebas	Responsable	Modificó el plan	Fue efectivo el plan	Comentarios

Ingrid Cadena

Documentación de Pruebas del Plan de Continuidad de Servicios de TI

Fecha de pruebas: _____

Responsable: _____

Número de prueba: _____

No.	Problemas encontrados	Soluciones dadas	Observación final

Ingrid Cadena

Glosario de Términos

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

Probabilidad: posibilidad de que una cosa se cumpla o suceda.

Controles: conjunto de operaciones manuales o automáticas para vigilar el estado de un sistema dirigido con el fin de elaborar las acciones de mando.

Análisis de riesgos: proceso complejo que parte de la determinación de las entidades autónomas (los Activos del Dominio y las Amenazas actuantes en él) y prosigue con la estimación de las entidades derivadas de aquéllas (las Vulnerabilidades y los Impactos).

Gestión de riesgos: es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Amenazas: son los eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Salvaguardas: es la acción que reduce el Riesgo; el Mecanismo de salvaguarda es el procedimiento o dispositivo, físico o lógico que lo reduce.

Riesgo inherente: referente a la valoración del riesgo sin ningún tipo de control.

Riesgo residual: referente a la valoración del riesgo que persiste luego de haber establecido medidas de control.

Riesgo repercutido: toma en cuenta el valor propio del activo combinándolo con la degradación causada por una amenaza y la frecuencia estimada de la misma.

Riesgo acumulado: toma en cuenta el valor propio de un activo y el valor de los activos que dependen de él, combinándolo con la degradación causada por una amenaza y la frecuencia estimada de la misma.