MAESTRÍA EN GERENCIA DE SISTEMA DE INFORMACIÓN MGSI

DISEÑO DE UN PLAN DE CONTINGENCIAS DE TICs PARA LA EMPRESA ELECTRICA CENTROSUR.

TESIS DE MAESTRIA | ING. ANDREA GRANDA

1 Contenido

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO 1

1. INTRODUCCION Y ESTADO DEL ARTE

Hoy en día, la mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto período. En caso de un desastre, la interrupción prolongada de los servicios de TI puede llevar a pérdidas financieras significativas, lo más grave es que se puede perder la credibilidad del público o de los clientes y, como consecuencia, la imagen corporativa de la empresa lo que conllevaría a un fracaso total.

Cabe preguntarse "¿Por se necesita un plan de contingencia para desastres si existe una póliza de seguro para esta eventualidad?" La respuesta es que si bien el seguro puede cubrir los costos materiales de los activos de una organización en caso de una calamidad, no servirá para recuperar el negocio. No ayudará a conservar a los clientes y, en la mayoría de los casos, no proporcionará fondos por adelantado para mantener funcionando el negocio hasta que se haya recuperado. [1]

En un estudio realizado por la Universidad de Minnesota, se ha demostrado que más del 60% de las empresas que sufren un desastre y que no tienen un plan de recuperación ya en funcionamiento, saldrán del negocio en dos o tres años. Mientras vaya en aumento la dependencia de la disponibilidad de los recursos informáticos, este porcentaje seguramente crecerá. [1]

Por lo tanto, la capacidad para recuperarse exitosamente de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan estratégico de seguridad para una organización. [1]

Todos los planes de contingencia informática apuntan a las actividades a desarrollar para evitar o minimizar el impacto de una contingencia y a recuperar el mayor porcentaje posible de nuestra plataforma informática dañada por alguna razón.

Esto es muy importante ya que una contingencia mal enfrentada puede conducir a pérdidas monetarias importantes e incluso el cierre de la empresa.

1.1. MOTIVACION

La motivación para este tema de tesis, es por la gran importancia que tiene, la adecuada y oportuna gestión de riesgos de TI, la cual permita contar con una respuesta estructurada, ante la eventualidad de incidentes, accidentes y/o estados de emergencias, que pudieran ocurrir tanto en las instalaciones de la empresa como fuera de ella, pudiendo interrumpir su normal funcionamiento y la pérdida de unos de los principales activos de la empresa que es la información.

Por este motivo, el diseñar y preparar un plan de contingencias, como una herramienta valiosa que proporcione la capacidad para restablecer las operaciones de TI y de negocio y salvaguardar su información, es una de las principales preocupaciones de las empresas, quienes reconocen la necesidad de auxiliarse con herramientas que le permitan garantizar una rápida vuelta a la normalidad ante la presencia de cualquier eventualidad.

El objetivo del plan no es evitar los riesgos en su totalidad, sino minimizar el impacto que las incidencias podrían producir en la organización. Así como también no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, identificar los mecanismos de seguridad que buscan proteger a la información de las diversas amenazas a las que se ve expuesta y supone un importante avance a la hora de superar todas aquellas adversidades que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos prolongado. Todo esto conlleva a que la función de definir los planes a seguir en cuestión de seguridad se conviertan en una tarea realmente compleja y costosa.

Por otro lado, el costo de detectar de manera temprana las amenazas a las que se encuentran expuesto los procesos críticos de la empresa y los recursos de TI involucrados, ayudarán a minimizar el impacto y costos.

Por este motivo es necesario que se tenga establecido dentro de cualquier empresa el proceso de mantenimiento y ejecución de Planes de Contingencia, en el que no solo la parte de TI tenga claro lo que se debe realizar sino también el resto de personal de la empresa. Para que este proceso sea realizado de una manera ordenada.

1.2. PLANTEAMIENTO DEL PROBLEMA

La empresa ELECTRICA CENTRO SUR, ha realizado en el año 2008 un diagnóstico sobre el Cumplimiento de la Norma ISO27001V.1. El resultado de esta evaluación es un Informe del Estado de Situación de la Empresa respecto a la norma; dentro de los puntos analizados se menciona la necesidad de crear, implementar y mantener un proceso para garantizar la continuidad del negocio.

Dentro del área de TI, la empresa cuenta con algunos controles de seguridad y de recuperación de ciertos recursos de TI, pero sin haber realizado un previo análisis de riesgos y sin contar con un proceso formal de prevención y recuperación de desastres (Plan de Contingencia). Por este motivo se ha visto la necesidad de diseñar un Plan de Contingencia de TI como parte del Plan de Continuidad del Negocio (BCP).

1.3. JUSTIFICACION DE LA TESIS

La empresa contará con una solución estructurada para mantener operativas las funciones que son fundamentales para la organización, cuando una contingencia afecte la infraestructura en TI instalada. Le ayudará a determinar acciones preventivas, reduciendo el grado de vulnerabilidad y exposición al riesgo, así como dimensionar el riesgo potencial y tomar decisiones rápidas ante fallas.

1.4. OBJETIVOS DE LA TESIS

General

- Desarrollar un Plan de Contingencias de TI para la Empresa Eléctrica Centro Sur.

Específicos

- Evaluar los riesgos de TI que impacten a la continuidad del negocio.
- Gestionar los riesgos que podrían dar lugar a eventos desastrosos y, por tanto, minimizarlos.

- Determinar las métricas Punto de Recuperación (RPO) y tiempo de recuperación (RTO) para los procesos de negocio que son soportados por las TI.
- Crear estrategias, procedimientos y políticas para la recuperación de la continuidad de las operaciones de TICs.
- Identificar los recursos necesarios para ejecutar el plan de contingencias.
- Establecer el proceso para el mantenimiento del Plan de Contingencias.

1.5. ALCANCE DE LA TESIS

El alcance del diseño del Plan de Contingencia abarcará lo referente a las TICs, involucradas en los procesos críticos para la continuidad del negocio, con respecto al Centro de Datos principal de la empresa.

Para el desarrollo de este Plan se abarcarán los siguientes aspectos:

- La gestión de Riesgos para prevenir un desastre. Esto se hace mediante la identificación y evaluación de los riesgos en TI que enfrenta la empresa.
- La gestión de incidentes que permita reducir su impacto, es decir, las acciones correctivas que se deben realizar para que el impacto sea mínimo.
- La gestión rápida y eficiente para la reanudación de las operaciones esenciales de la empresa.

1.6. ORGANIZACIÓN DE LA TESIS.

El contenido de esta tesis estará conformado de la siguiente manera:

El capitulo dos abarca todo lo relacionado con el Análisis y Evaluación de Riesgos utilizando la Metodología Magerit. El capítulo tres trata sobre el Análisis e Impacto en el negocio. El capitulo cuatro presenta el Diseño del Plan de Contingencias. El capitulo cinco presenta el Presupuesto requerido para ejecutar el plan. El capitulo seis específica los procesos y procedimientos. El capítulo siete las conclusiones y recomendaciones.

1.7. ESTADO DEL ARTE.

En esta sección se realiza una breve presentación sobre el estado actual del Análisis y Evaluación de Riesgos, Plan de Contingencia TI, la metodología para desarrollar el Plan de Contingencia y el estándar ISO 27001 relacionadas con las contribuciones propuestas en esta tesis de maestría.

1.7.1. METODOLOGÍA DE ANALISIS DE RIESGOS

Actualmente existen algunas metodologías de análisis de riesgos para abordar una certificación ISO/IEC 27001. Entre las que destacan: OCTAVE, MAGERIT, MEHARI y FAIR. El proceso de certificación de un Sistema de Gestión de Seguridad de la Información ISO/IEC 27001 requiere la elaboración de un Análisis de Riesgos como medio de diseñar el Plan de Gestión de Riesgos del sistema, e identificar la aplicabilidad de los controles a implantar en una organización.

Hoy en día la serie de normas ISO 27000 cuenta con una nueva norma para la elaboración del análisis de riesgos, dicha norma es la ISO/IEC 27005:2008 (Information technology, Security techniques, Information security risk management), la misma que establece un criterio sobre la gestión del riesgo y proporciona un marco normalizado que ayuda a definir nuestra propia metodología. Soporta los conceptos definidos en la ISO/IEC 27001 y está diseñado para ayudar a la implementación de un sistema de seguridad de la información basado en la gestión del riesgo.

Debido a la ausencia de una metodología propia para la certificación ISO/IEC 27001 se ha encontrado, debido a sus diferentes funcionalidades, a las herramientas en las que se soporta, a los estándares y normativas a las que da conformidad, como la metodología idónea a MAGERIT II.

MAGERIT

Magerit es una metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. Actualmente está en su versión 2.

El análisis de riesgos propuesto por MAGERIT II es una aproximación metódica que permite determinar el riesgo siguiendo unos pasos:

- Determinar los activos relevantes para la Organización
- Determinar a qué amenazas están expuestos aquellos activos
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Valorar dichos activos en función del coste que supondría para la Organización recuperarse ante un problema de disponibilidad, integridad, confidencialidad o autenticidad
- Valorar las amenazas potenciales.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

El método propuesto por MAGERIT II da cumplimiento en lo establecido en la ISO 13335, en el epígrafe 4.2.1.d Identificar Riesgos, 4.2.1.e Analizar y evaluar riesgos de la ISO /IEC 27001:2005, y además garantiza conformidad respecto los estándares:

- ISO/IEC 27001 / 2005 “Sistemas de Gestión de Seguridad de la Información”
- ISO/IEC 15408 / 2005 “Criterios de Evaluación de Seguridad de la Información”
- ISO/IEC 17799 / 2005 “ Manual de Buenas Prácticas de Gestión de Seguridad de la Información”
- ISO/IEC 13335 / 2004 “Guía para la Gestión de Seguridad TI”

1.7.2. GENERALIDADES SOBRE UN PLAN DE CONTINGENCIAS.

Sistemas de Información

Un sistema de información (SI) es un conjunto organizado de elementos, los cuales pueden pertenecer a alguna de las siguientes categorías: Personas, datos, procesos, recursos materiales (incluyendo recursos informáticos y de comunicación).

Todo ese conjunto de elementos interactúan entre sí para procesar los datos e información y distribuirla para que la empresa pueda alcanzar sus objetivos satisfactoriamente.

Contingencia

Se conoce como contingencia a la alteración en la continuidad de negocio, que impacte en forma relevante el normal desarrollo de un servicio considerado crítico, teniendo su origen en la falla de un componente o la interrupción de una tarea, sin estar necesariamente prevista [2].

Plan de Contingencia

Un plan de contingencias es una herramienta de gestión necesaria para dar una respuesta planificada ante eventos sobre TI que pudieran interrumpir el normal funcionamiento de la empresa, dotándole de la capacidad para restablecer las operaciones de TI y de negocio.

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad de negocio aplicado al departamento de informática o tecnologías.

Ciclo de Vida de un Plan de Contingencia

El plan de contingencias sigue el conocido ciclo de vida iterativo PDCA (plan-do-check-act), es decir, planificar-hacer-comprobar-actuar.

Este inicia con el análisis de riesgos donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio. Luego de determinar el impacto en el negocio y la priorización de procesos críticos, se seleccionan las contramedidas más adecuadas entre diferentes alternativas, siendo plasmadas en el plan de contingencias junto con los recursos necesarios para ponerlo en marcha.

El plan debe ser revisado periódicamente, generalmente, la revisión será consecuencia de un nuevo análisis de riesgos. En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.
- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa del fallo y proponer nuevas contramedidas.
- Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos. Es posible que las contramedidas adoptadas fueran eficaces para una amenaza no prevista. No obstante, esto no es excusa para evitar el análisis de lo ocurrido.

Finalmente, se modifica el plan de contingencias de acuerdo a las revisiones aprobadas y, de nuevo, se inicia el ciclo de vida del plan.

Metodología de un Plan de Contingencia

La metodología aplicada para el desarrollo del proyecto es la que en la mayoría de textos utiliza o recomienda para la elaboración del Plan de Contingencia, basados en el BCI (Instituto de Continuidad del negocio) y DRII (Instituto Internacional de recuperación de Desastres), así como en la observación de estándares y prácticas internacionalmente aceptadas (CobiT DS4, ITIL Service Delivery 2.4, ISO IEC 17799:2005 Ch 14).

La metodología a seguir consta de las siguientes actividades:

1. **Realizar el Análisis de Impacto en el Negocio (BIA).** El BIA ayuda a identificar y dar prioridad a los componentes y sistemas críticos de TI. Esto se logra mediante la identificación y evaluación de riesgos, la asignación de prioridades a los componentes críticos de TI, identificación de umbrales (Lapsos de tiempo que es posible no prestar el servicio sin la ocurrencia de grandes trastornos).

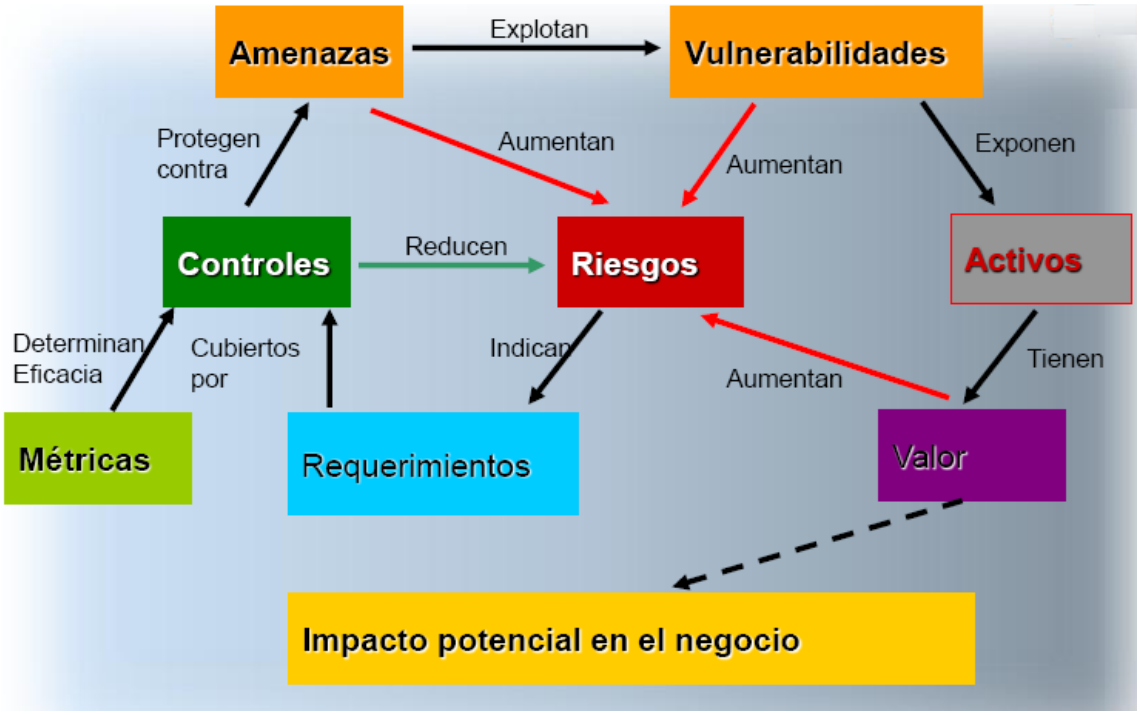


Figura 1.1 Análisis del Impacto del negocio. [6]

2. **Identificar los controles preventivos.** Contempla las medidas tomadas antes de que la amenaza se materialice, para reducir los efectos de las fallas en el sistema, permitiendo incrementar la disponibilidad del sistema y reducir los costos de las contingencias del ciclo de vida.
3. **Identificar los controles de respuesta.** Contempla las medidas requeridas durante la materialización de una amenaza, o inmediatamente después, permitiendo contrarrestar los efectos adversos de la misma.
4. **Identificar los controles de recuperación**. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.
5. **Desarrollar el plan de contingencia.** El plan de contingencia debería contener guías detalladas y procedimientos para restaurar un sistema averiado.
6. **Evaluar el plan y entrenar al personal.** Evaluar el plan identifica brechas en la planificación, mientras que el entrenamiento prepara al personal de respaldo para la activación del plan; ambas actividades mejoran la efectividad del plan y la preparación global de la agencia.
7. **Mantenimiento del plan.** El plan debe ser un documento vivo que se actualiza regularmente para permanecer al corriente de las mejoras del sistema.

Figura 1.2 Metodología para Elaborar el Plan de Contingencia.

1.7.3. CONCEPTOS DE TI SOBRE CONTINUIDAD [3].

En esta sección de la tesis se hará una breve presentación sobre principios de continuidad que sirvieron como fundamento para el desarrollo de esta tesis.

Redes de Misión Crítica

Misión crítica se refiere a la infraestructura y operaciones que son absolutamente necesarias para que una organización lleve a cabo su misión. Cada organización debe definir el significado de misión crítica sobre la base de su necesidad.

Cada organización debe determinar qué aspectos de su red de TI es de misión crítica para ellos. Esto incluye recursos tales como: switches, routers, gateways, plataformas de servicios, dispositivos de seguridad, aplicaciones, instalaciones de almacenamiento, y medios de transmisión. Los recursos de misión crítica son aquellos que son absolutamente necesarios para que los componentes y procesos críticos lleven a cabo su función. Porque cualquiera de estos elementos puede fallar debido a un mal diseño, factores ambientales, defectos físicos, o errores de los operadores. Las contramedidas deben ser elaboradas para que la operación continúe aunque los recursos claves no estén disponibles. Los recursos de front-end pueden tener mayor precedencia sobre los recursos de back-office, que tienen una influencia poco pronunciada en el éxito de la misión.

Características Deseables de una plataforma de misión critica

Las características de una plataforma de misión crítica deberían incluir:

- **Simplicidad:** La regla general “cuanto más simple, mejor”, también recae en las plataformas. Cuanto menor número de componentes tengan y que sean modulares, es mucho mejor, porque facilitan su reemplazamiento. La redundancia es algo que podría afectar esta característica, en las plataformas, porque aumenta el número de componentes, para dar mayor fiabilidad en el funcionamiento. Se tiene que buscar la manera óptima de balancear la fiabilidad, a través de la redundancia, con la simplicidad.
- **Económico:** El costo es un factor importante al momento de elegir un producto, pero este tiene que ser análizado, en base a los objetivos y

estrategias de disponibilidad y mejoramiento de desempeño en las aplicaciones y servicios que la empresa necesita.

- **Enfriamiento del Equipo:** La plataforma debe de tener un buen sistema de ventilación que garantice que el calor generado por los diferentes procesadores, unidades de disco duro, fuentes de poder, no afecten el funcionamiento del sistema.
- **Capacidad de Servicio:** Los sistemas con buena capacidad de servicio puede reducir significativamente el tiempo medio de recuperación (MTTR), permiten accecibilidad a los componentes, así como una fácil instalación y desinstalación. Uno debe ser capaz de acceder a componentes interiores y tener que reemplazarlos sin impactar a otros componentes para su recuperación. Por ejemplo una buena gestión de manejo de cables en un rack o gabinete puede ayudar en la prestación de servicios.
- **Fácil Intercambio:** Este término hace referencia a la rapidez con la que los componentes son reemplazados y asimilados dentro de un sistema, sin tener que reiniciarlo.
- **Memoria**: Debería tener suficiente memoria para poder llevar a cabo el procesamiento de aplicaciones y procesos en background. Mejora el desempeño y prolonga la vida útil de la plataforma.
- **Redundancia:** Identifica componentes redundantes dentro de un sistema, permitiendo que si el componete primario falla, el secundario entre en funcionamiento automáticamente. Esto incluye componentes de hardware y software.
- **Tolerancia a Fallos:** El uso de sistemas redundantes, implica que la plataforma tendrá mecanismos de failover, los cuales permitan que continúe operando, mientras dure la falla y la reparación.
- **Alto nivel de compatibilidad:** La capacidad de interactuar con componentes de diferentes proveedores y ejecutar aplicaciones propias o comerciales.
- **Certificaciones:** Las cuales garanticen el cumplimiento de estándares, en su funcionamiento, calidad y seguridad.
- **Funcionalidad:** Este atributo conlleva, que la plataforma debe satisfacer las necesidades de la organización como: requerimientos operacionales, de red y aplicación.
- **CPU:** La plataforma debe tener una velocidad de CPU que esté acorde con el resto de componentes, de lo contrario, será un desperdicio, si los otros componentes no operan a una velocidad correspondiente.
- **Almacenamiento:** Este es un atributo que se debe de tener en cuenta, al momento de seleccionar una plataforma. Su capacidad y tipo, medio de comunicación, canales de E/S.

- **Sistema Operativo:** La elección del sistema operativo con el que va a operar, es un atributo importante, sea comercial o de código abierto. Conocer qué SO se han certificado para trabajar con qué tipo de CPU, garantizará compatibilidad y soporte por parte del vendedor del software, si se necesitara [3].

Plataformas de Tolerancia

FAULT TOLERANCE o TOLERANCIA A FALLOS (FT)

La tolerancia a fallos (FT) es la capacidad que tiene una plataforma para recuperarse automáticamente de un problema. En una red la tolerancia a fallos debe diseñarse a través de su infraestructura y operaciones. Para hacer esto, una organización debe identificar y entender qué falla es tolerable. Para esto, se requiere determinar los procesos informáticos y de telecomunicaciones que son fundamentales para un proceso u operación. Además, se necesita tener claro cómo debe comportarse la red durante eventos adversos, a fin de que pueda ser diseñada para comportarse de forma previsible.

Las plataformas de tolerancia a fallos están diseñadas de manera que un fallo no cause daño a todo el sistema, permitiendo continuar procesando las solicitudes sin afectar al usuario, servicios, red o sistema operativo. En general, la tolerancia a fallos del sistema o de la operación deben cumplir los siguientes criterios [3]:

- Debe ser capaz de identificar rápidamente los errores o fallos.
- Debe ser capaz de proporcionar el servicio a pesar que los problemas persistan. Esto significa el aislamiento de problemas de manera que no afecten al funcionamiento del resto del sistema. Esto podría implicar temporalmente la eliminación de los componentes problemáticos del servicio.
- Debe ser capaz de corregir el problema o ser reparado y recuperado mientras se encuentra en operación.
- Debe ser capaz de preservar el estado de los trabajos y operaciones durante el fallo.
- Debe ser capaz de volver al nivel original de la operación después de la reanudación.

FT se puede lograr de varias maneras.

- Mediante hardware y software
- Utilizando componentes redundantes,

- comprobación continua de errores,
- mecanismo de recuperación automática.

Estas son las formas más utilizadas. Con frecuencia incluyen cosas como la doble fuente de alimentación redundante del CPU, discos de copia de seguridad, y software de failover automático, todos diseñados con la intención de eliminar la interrupción del servicio.

Es importante tener presente que la notificación (alerta o mesajes de error) que la plataforma genera por una auto recuperación o regeneración de un fallo es obligatoria, para descubrir las causas del mismo. De lo contrario, podrían ocultarse problemas críticos que conllevarían a daños mayores.

FAULT RESILIENCE O RESISTENCIA A FALLOS (FR)

Las plataformas de resistencia a fallos son similares a las plataformas de tolerancia a fallos, también se caracterizan por tener componentes redundantes, mecanismos de tolerancia a fallos, pero se diferencian en que estas no garantizan, la no perdida de transacciones. Sin embargo es una estrategia de bajo costo, que garantiza una disponibilidad similar a una plataforma de tolerancia a fallos [4]. Mientras en una plataforma de tolerancia a fallos la ocurrencia de un fallo, se observará en el usuario final, como un posible retraso poco perceptible, en el funcionamiento normal, en la plataforma de resistencia a fallos, este fallo afectará con un tiempo de inactividad notable.

HIGH AVAILABILITY O ALTA DISPONIBILIDAD (HA)

Las plataformas de alta disponibilidad no proporcionan el mismo nivel de supervivencia como las plataformas de tolerancia a fallos y resistencia a fallos [3]. Estas están diseñadas para corregir proactivamente fallos o defectos en los componentes pero no disponen de mecanismos de recuperación. La redundancia de los componentes garantiza que el fallo de uno de ellos, no afecte el funcionamiento de todo el sistema. Son de menor costo que las plataformas tolerancia a fallos y resistencia a fallos.

Principios de Redundancia

La redundancia es una característica de la arquitectura de red en donde varios elementos son utilizados, de manera que si uno no puede prestar el servicio, el otro lo haga. La redundancia puede aplicarse a varios niveles dentro de una red, con el fin de lograr la continuidad del negocio. El acceso a la red, distribución de servicios, rutas alternas, plataformas de sistemas, recuperación de centros de datos, almacenamiento, todas pueden ser implementadas con alguna forma de redundancia. La redundancia debe ser aplicada a los recursos críticos necesarios para el funcionamiento de las operaciones esenciales de red.

La redundancia puede recargar el costo de inversión en componentes de red y gastos de operación, por lo que debe ser eficaz, más allá de los propósitos de continuidad. No tendría sentido invertir en una solución de redundancia, si la inversión requerida cuesta más de lo que se perdería en dinero, reputación y horas de trabajo, si el sistema fallara. Es más rentable cuando está intrínseca en el diseño de una red que apoye las necesidades de disponibilidad y rendimiento.

La administración puede mejorar la justificación del costo de una solución redundante, cuando agrega valor en las operaciones cotidianas, además de reducir el riesgo minimizando el impacto en la infraestructura actual y sus operaciones. Los sistemas redundantes de conectividad y red, destinados para la recuperación pueden ser utilizados para otros fines durante el funcionamiento normal, en lugar de estar inactivos. Podrían utilizarse para descargar el tráfico de elementos primarios durante períodos picos o mientras están en mantenimiento.

Actualmente en un sistema informático, existen muchos componentes necesarios para su funcionamiento, cuantos más componentes, mas probabilidad hay de que algo falle. Estos problemas pueden presentarse en el servidor como: fallos de discos, fuentes de alimentación, tarjetas de red, etc. y en la infraestructura necesaria para que el servidor pueda utilizarse como: componentes de red, acceso a internet, sistema eléctrico.

A continuación se presenta un breve resumen de las técnicas y configuraciones de redundancia

REDUNDANCIA DE COMPONENTES EN PLATAFORMA PARA SERVIDOR Y EQUIPOS DE RED

Los componentes redundantes más usuales en un servidor son: los discos, las tarjetas de red y las fuentes de alimentación. Existen servidores con múltiples

CPUs que siguen trabajando sin problemas con alguna CPU o módulo de memoria estropeado.

Discos Duros

El fallo más común en un servidor es el fallo de un disco duro. Si el servidor dispone solamente de un disco y éste falla, fallará todo el servidor, ya que no se podrá acceder a los datos contenidos en el mismo. Existen por esto técnicas que ayudan a minimizar este problema, permitiendo que el servidor siga funcionando y que no se pierdan datos. También se pueden sustituir los discos que fallan sin necesidad de apagar el servidor (HotSwap)

La técnica más común es la llamada RAID (redundant array of independent disks). La cual consiste en crear un conjunto de discos redundantes que pueden ayudar, tanto a aumentar la velocidad y el rendimiento del sistema de almacenamiento, como a que el sistema siga funcionando aunque algún disco falle. Existen implementaciones por software y hardware y diferentes configuraciones RAID, siendo las más comunes RAID1, RAID5 y RAID10.

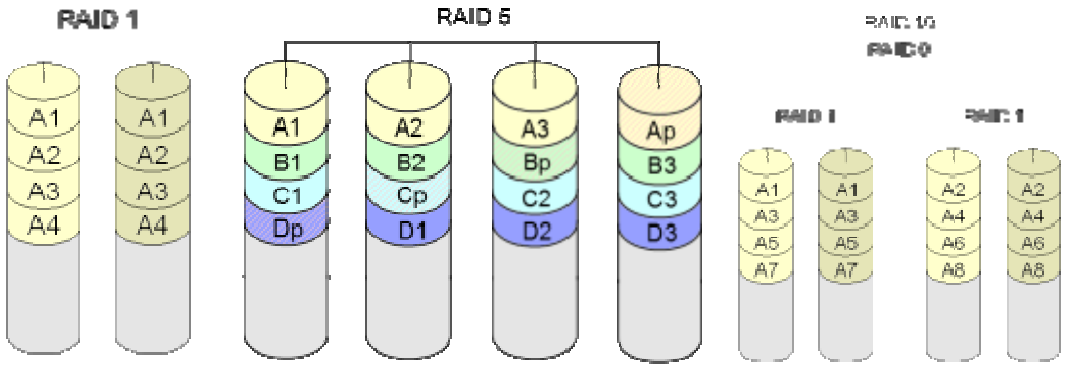


Figura 1.3 Ejemplo de configuraciones RAID. [3]

Tarjetas Adaptadores de Red

La tarjeta de red conocida como NIC, es el dispositivo que permite a un equipo host comunicarse con otros dispositivos de red. Es por ello muy común que los servidores tengan como mínimo 2 tarjetas de red, para garantizar que esta comunicación no se corte en caso de fallo de una de las tarjetas. Este nivel de redundancia se aplica en la capa 2 del modelo OSI.

En Linux existe una técnica llamada 'Bonding", por la cual se utilizan 2 o más tarjetas de red como si fueran un único dispositivo, sumando las capacidades de las mismas y teniendo redundancia en el caso que alguna de las tarjetas falle.

El uso de una NIC multipuertos o redundante va acompañada de un software especial, que permite que si la NIC primaria falla la de respaldo entre a funcionar. Un clúster, son varias NICs agrupadas, donde si una falla otra toma el control del clúster. Esta técnica reduce la necesidad de tener una aplicación especial que maneje la tolerancia a fallos. El software de tolerancia a fallos que viene con este tipo de dispositivos, incorpora características adicionales como: la asignación de una dirección de red a múltiples NICs, balanceo de carga entre las múltiples NICs.

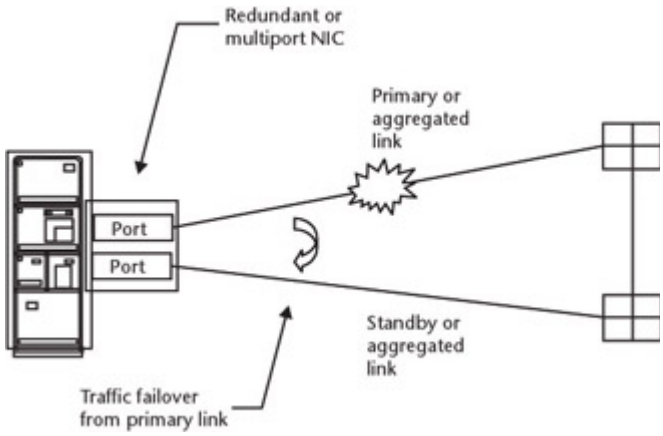


Figura 1.4 Uso de NICs redundantes [3].

Otra ventaja que se destaca con una NIC multipuertos es el ahorro de una ranura, debido a que el uso de una tarjeta adicional puede consumir un espacio en el servidor. La NIC multipuertos, en general, puede enmascarar múltiples direcciones MAC en uno, evitando la necesidad de volver a calcular las rutas. También pueden aumentar el rendimiento mediante la agregación de enlaces, lo que supone la agregación de múltiples puertos de un único adaptador, resultando en un mayor rendimiento.

Fuentes de alimentación

La fuente de alimentación es la encargada de proporcionar electricidad al host o servidor. Es común que los servidores tengan 2 o más fuentes de alimentación conectadas a diferentes sistemas eléctricos, para garantizar el suministro en el caso que una de las fuentes o uno de los sistemas eléctricos fallen. Lo usual es que se puedan sustituir las fuentes de alimentación que fallan sin necesidad de apagar el servidor (HotSwap). Otros componentes del sistema como routers, switches, cabinetes de discos, etc suelen utilizar la misma técnica de redundancia.

Suministro eléctrico

Todo componente eléctrico, necesita un suministro constante de electricidad para funcionar. Fallos en este suministro, aunque sean por periodos muy cortos de tiempo, pueden producir impactos importantes en la continuidad del sistema. Y no solo se necesita un suministro constante, también se necesita que no tenga subidas y bajadas bruscas que puedan estropear componentes electrónicos.

Para conseguir esto se pueden utilizar diferentes componentes según el grado de protección que se necesita.

- **SAI (UPS):** Son baterías más o menos avanzadas que se conectan entre el servidor y la fuente de suministro eléctrico. Garantizan un suministro constante y estable por un tiempo, dependiendo de la capacidad de las mismas.
- **Generadores eléctricos:** Funcionan generalmente con diesel y se conectan entre los UPS y la red de suministro eléctrico. Solo entran en funcionamiento cuando el suministro se corta por más de un determinado tiempo. Pueden suministrar electricidad por un tiempo indefinido siempre que tengan carburante en el tanque.
- **Líneas independientes de suministros:** En centros de datos grandes, se suelen tener al menos 2 conexiones diferentes e independientes a la red de suministro eléctrico.

La redundancia en el sistema eléctrico es aplicable a todos los componentes del sistema que utilicen electricidad, para evitar que queden incomunicados grupos de servidores con redundancia, porque uno de los otros componentes no disponía de un sistema redundante de suministro eléctrico.

REDUNDANCIA EN NODOS DE RED

No sirve de nada tener plataformas con componentes redundantes y un suministro eléctrico constante y equilibrado si algunos de los componentes de la red fallan y no se puede acceder al servidor.

Los componentes más comunes en una red son:

Routers (enrutador): Es un dispositivo que interconecta segmentos de red o redes enteras.

Switch (Conmutador): Es un dispositivo que interconecta dos o más segmentos de red.

Cables de red: Para interconectar los diferentes componentes, existen muchos y variados tipos, siendo los más comunes el cable de par trenzado y el de fibra óptica.

Líneas de conexión: a la red de área amplia, WAN (por ejemplo Internet).

Se puede producir alguna falla en los componentes anteriormente listados, dejando al sistema incomunicado. Existen técnicas para evitar que esto ocurra, lo que se suele hacer es configurar la red, para que al menos existan 2 caminos diferentes entre dos componentes A y B. En el grafico se tiene un esquema ejemplo, de cómo configurar una red con redundancia doble desde el servidor hasta Internet. De esta manera se puede dañar un router, un switch y una tarjeta de red a la vez sin que perdamos conectividad.

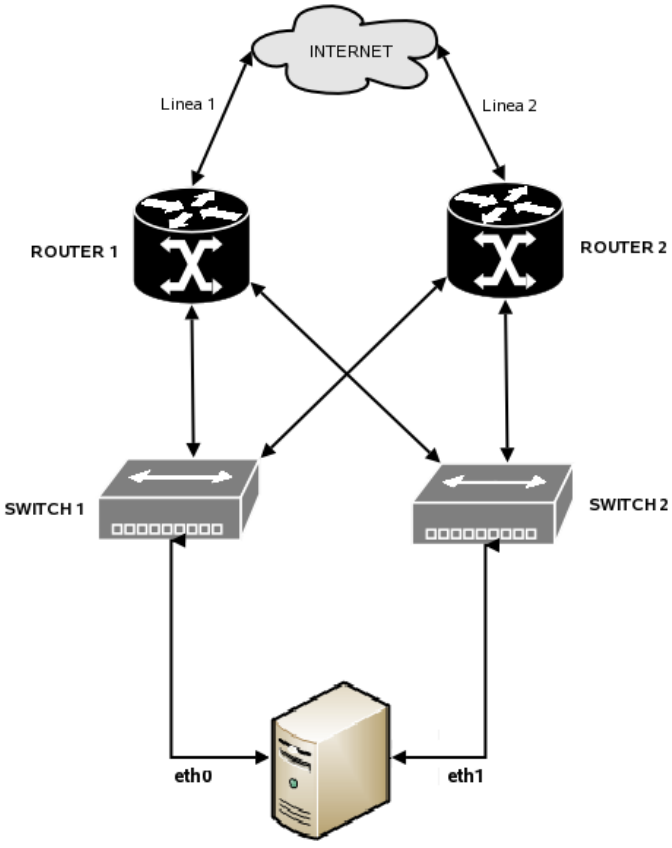


Figura 1.5 Redundancia de componentes de red.

Redundancia de Servidores con Balanceo de Carga

Este tipo de redundancia se aplica para evitar el riesgo que falle todo el servidor, si alguno de sus componentes, que no disponen de redundancia falla.

Existen diferentes tipos de configuraciones con varios servidores, que pueden ayudar con este problema. Esto se conoce como clúster. El fundamento principal detrás del clúster es que varias computadoras redundantes trabajan juntas como un único recurso, permitiendo hacer más trabajo que una sola computadora y puede proporcionar mayor confiabilidad. Físicamente, un clúster abarca varios dispositivos computacionales que se interconecten para comportarse como un solo sistema. Otras computadoras en la red ven y trabajan con un clúster como si fuera un solo sistema. Los elementos computacionales que forman un clúster se pueden agrupar de diferentes maneras para distribuir la carga y eliminar los puntos de fallo. La pérdida de un dispositivo individual o nodo de clúster no causa la perdida de datos o no disponibilidad de las aplicaciones. La transición de un nodo que falla a otro de respaldo, debe ser lo más transparente posible, tal que la pérdida de datos y la interrupción de las aplicaciones sean mínimas.

Las soluciones de clúster son utilizadas también para mejorar el procesamiento o balanceo de carga, así se logra evitar los cuellos de botella en el procesamiento. Si se requiere un alto desempeño en el procesamiento, un trabajo puede ser dividido en varias tareas y distribuido entre los nodos del clúster. Si uno de los procesadores o servidores está sobrecargado, falla, o está fuera de servicio por mantenimiento, otro nodo del clúster puede relevarlo. Esta situación requiere que los nodos tengan acceso a los datos de cada uno para mantener la consistencia.

El clúster puede mejorar la escalabilidad porque la sobrecarga puede distribuirse entre diferentes máquinas. Los nodos individuales pueden ser actualizados o pueden agregarse nuevos nodos para incrementar la unidad central de proceso (CPU) o memoria, para cumplir con requisitos de tiempos de respuesta y mejoramiento de desempeño.

Hay diferentes maneras de implementar el clúster. Servidores conectados a través de una red soportando TCP / IP es un enfoque común. Otro enfoque es conectar los procesadores de cálculo a través de un backplane de alta velocidad. Ellos pueden estar conectados en diferentes topologías, incluyendo estrella, anillo o bucle. Invariablemente, en cada uno de los enfoques los nodos tienen asignadas tareas principales y los nodos secundarios asumirán automáticamente la ejecución de esas tareas, si falla el nodo principal. El nodo secundario puede realizar tareas para que se mantenga útil durante el funcionamiento normal o mantenerse inactivo como en modo de espera. Un acuerdo de reciprocidad se puede establecer entre los nodos para que hagan las mismas tareas. Tales acuerdos se pueden lograr en varios niveles incluyendo hardware, sistema operativo, o aplicaciones.

El clúster requiere un software especial que puede hacer que varios ordenadores se comporten como un sistema. Este software suele ser organizado de manera jerárquica para una gestión operativa a nivel local o global sobre el clúster. La sofisticación del software ha crecido hasta el punto en que puede administrar un conjunto de sistemas, almacenamiento y comunicación. *Un ejemplo de ello es la tecnología de IBM Parallel Sysplex, que se destina a proporcionar una mayor disponibilidad. Sysplex paralelo es una tecnología que conecta varios procesadores a través de largas distancias (40 km) utilizando un mecanismo de acoplamiento especial que les permite comunicarse y compartir datos* [3].

A continuación se tiene una serie de ejemplos de cómo se pueden organizar estos clúster, en donde el fallo de un servidor, no interrumpe el funcionamiento de un servicio. Cuando falla uno o varios servidores en el clúster, la capacidad de proceso del mismo se reduce, por lo que es importante tener siempre cierta capacidad sin usar para que en el caso de un fallo no se reduzca mucho el tiempo de respuesta.

Clúster Múltiprocesamiento: Consisten en varios CPUs internos agrupados para un único sistema, que permite mejorar el desempeño y la disponibilidad. Los sistemas Standalone (sistemas independientes) tienen esta característica y se los llama también como sistemas multiprocesador o escalables. Los nodos del clúster, utilizan procesamiento paralelo e intercambian información a través de la memoria compartida, mensajes y almacenamiento de entrada y salida. Los nodos están conectados a través de una red de área de sistema, que es generalmente un backplane de alta velocidad. Frecuentemente utilizan software especial, como sistemas operativos, manejadores de bases de datos y software de administración de la operación. Por consiguiente este tipo de clúster es costoso de implementar, por lo que es empleado para propósito de alto desempeño.

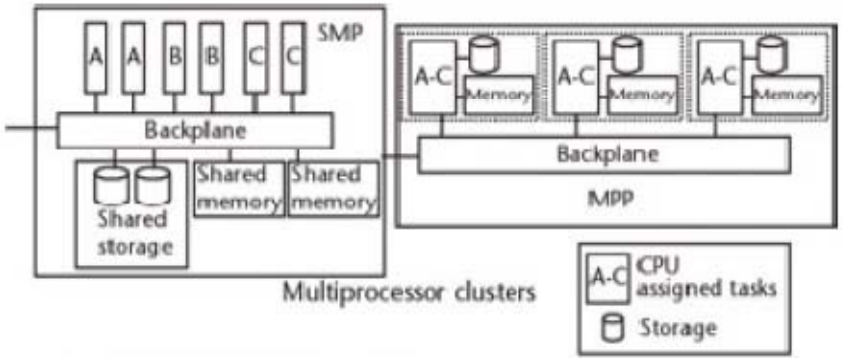


Figura 1.6 Tipos de Cluster Multiprocesamiento[3].

Hay dos tipos básicos de este clúster: El SMP Symmetric Multiprocesing Clúster, en el cual cada nodo ejecuta diferente tarea al mismo tiempo. El MPP Massively parallel procesing, tiene para cada CPU interna su propia memoria y almacenamiento. Esta modularidad le permite al MPP ser más escalable que el SMP, porque el SMP puede verse limitado por la arquitectura de la memoria, mientras que con el MPP estarán limitados por la capacidad de la red.

Clúster con Tolerancia a fallos: Son una versión de hardware simplificada del clúster multiprocesador. Estos sistemas suelen utilizar dos o más procesadores redundantes y software para mejorar el desempeño y la administración de cualquier fallo en el sistema. El software generalmente es complejo, tanto el sistema operativo como las aplicaciones son diseñadas para la plataforma de hardware. Este tipo de sistemas son generalmente utilizados en telecomunicaciones y plantas operativas donde la alta disponibilidad y confiabilidad son necesarias. Estos sistemas pueden ejecutar por sí mismos procesos de software para corrección de fallas o automáticamente aplicar tolerancia a fallos a otro procesador si una falla en hardware o software es catastrófica. Generalmente vienen con alarmas que son ejecutadas para alertar al personal para asistencia o reparación dependiendo del caso. Se caracterizan por ser costosos y son menos escalables que los sistemas multiprocesador.

Clúster de Servidores: Es un enfoque de menor riesgo y menos costo, para proveer desempeño y confiabilidad. A diferencia de los sistemas multiprocesador o tolerancia a fallos, este tipo de clúster se componen de dos o más servidores de menor costo, que se conectan mediante tecnología de red convencional. Los nodos (servidores), son añadidos a la red como se requiera, dotando de mejor escalabilidad. Los clústeres de grandes servidores, utilizan generalmente la estrategia de no compartir nada, es decir que cada servidor tiene su propia memoria, almacenamiento, sistema operativo. Esto evita los cuellos de botella en memoria o recursos de Entrada o salida. Sin embargo esta estrategia debe basarse en alguna técnica de espejo o almacenamiento en red para tener una vista consistente de los datos de las transacciones, si ocurre una falla.

A continuación se lista algunas de las amplias categorías de servicios de clústeres que deben considerarse. Cada una de estas categorías se puede lograr mediante la combinación de configuraciones y tecnologías de clúster antes presentadas.

Clústeres administrativos: Están diseñados para ayudar en la administración y gestión de los nodos ejecutando diferentes aplicaciones, no necesariamente iguales. Algunos van más allá, permitiendo la integración de paquetes de software a través de los diferentes nodos.

Clústeres de alta disponibilidad: Proveen capacidades para tolerancia a fallos. Cada nodo actúa como un único servidor, con su propio sistema operativo y aplicaciones. Cada nodo tiene una imagen replicada, que entra a funcionar si el nodo falla. Dependiendo del nivel, sobrecarga, disponibilidad requerida hay varias políticas de tolerancia a fallos que pueden aplicarse. Configuraciones en caliente o frío pueden aplicarse para asegurar que el nodo de replica esté siempre disponible para asumir el trabajo del otro nodo. Las configuraciones en frío, pueden requerir un tiempo de tolerancia a fallos extra para iniciarse mientras que las configuraciones en caliente pueden asumir el procesamiento con un poco o casi nada de retraso.

Clústeres de alto desempeño: Son diseñados para proveer un poder de procesamiento extra y alta disponibilidad. Generalmente son utilizados en ambientes donde se requiere procesamiento de gran volumen y alta confiabilidad, con son las telecomunicaciones y las aplicaciones científicas. La carga de trabajo de las aplicaciones es dividida entre los nodos, ya sea uniformemente o por tarea específica. Son algunas veces llamados clústeres de aplicaciones en paralelo o balanceo de carga. Por esta razón, esta clase configuraciones de clústeres son las más confiables y escalables.

Clústeres de Área Amplia: Son clústeres utilizados en empresas de gran diversidad y gestión. Están diseñados para procesar aplicaciones simultáneamente sobre todos los nodos del clúster en todos los sitios. Las aplicaciones funcionan sin tomar en cuenta la ubicación física de la plataforma. Si se produce una interrupción en un sitio, continúan las operaciones en el otro sitio. El acceso concurrente a los mismos datos es alcanzado a través de una variedad de técnicas de mirroring y redes de almacenamiento. Los sitios están conectados a través de una red WAN. Este tipo de clúster también requiere de mecanismos para detectar fallos en la ubicación remota y tolerancia a fallos. Esto requiere el uso sincronizado de software de gestión de clústeres, enrutamiento de red, balanceo de carga, y tecnologías de almacenamiento.

Principios de Diseño

Particionado

Un diseño particionado es el mejor enfoque para una red de misión crítica, sistema u operación. La arquitectura particionada involucra separar una red o sistema en zonas, o módulos. Un módulo es el más bajo nivel aceptable de funcionamiento independiente. Pudiendo ser un único componente hasta un segmento de red. Aunque el diseño modular es clave para la sustitución rentable, no implica necesariamente una recuperación rápida. Un proceso de gestión debe ser necesariamente empleado para inducir la tolerancia a fallos y

la recuperación del módulo con fallo. El diseño particionado reduce el riesgo, al limitar el impacto de un problema a un módulo o grupo de módulos, a veces llamado grupo de fallo. De esta manera un acontecimiento adverso en un grupo no afecte la operación de la red entera o del sistema. La figura 1.6 ilustra estos conceptos:

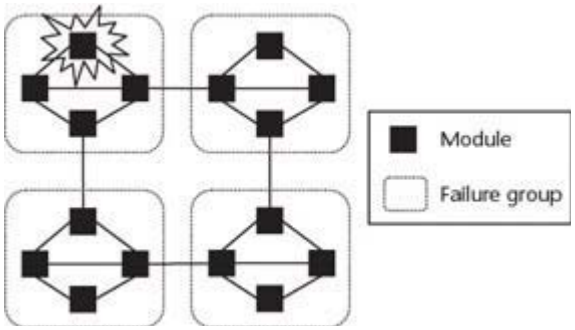


Figura 1.7 Ejemplo de diseño de red particionado [3].

Balance.

El mejor diseño de red es el que equilibra la distribución de los recursos con los costos. Esto significa proporcionar una arquitectura que no es ni centralizado ni descentralizado, pero tiene suficiente redundancia para su supervivencia y rendimiento [3]. Las siguientes secciones describen las ventajas de cada enfoque.

- Centralizado

La centralización es un enfoque que consolida los recursos de la red en una sola ubicación, ya sea un nodo, plataforma, o centro de datos, para reducir el costo y la complejidad (Figura 1.8). Ofrece un uso más eficiente de los recursos y reduce los costes operativos. Pero la consolidación conlleva a una menor flexibilidad y mayor riesgo. Por ejemplo la pérdida de un recurso consolidado puede resultar en la pérdida de un servicio.

En consecuencia, los clientes de un servicio con diseño centralizado requieren mayores garantías de servicio. La pérdida de nodos de redes centralizadas o altamente interconectados puede degradar o eliminar el efectivo desempeño de toda la red.

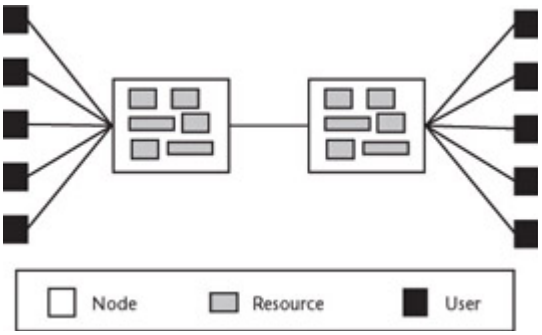


Figura. 1.8 Arquitectura de Red Centralizada [3]

- Descentralizado

En los últimos años, la utilización de arquitecturas de mainframes centralizadas ha disminuido en la creación de redes, dando lugar a una mayor descentralización de las arquitecturas incluyendo sistemas distribuidos (Figura 1.9) [3].Antes se utilizaba un servidor que procesaba diferentes funciones, ahora muchas funciones específicas utilizan diferentes servidores. A pesar de la tendencia hacia la computación distribuida, las empresas están físicamente en un sitio, centralizando todos los recursos, como es el caso de granjas de servidores con grandes número de servidores en un único sitio. En cualquier caso, las arquitecturas distribuidas implican más interfaces de red y conectividad, requieren la integración de muchos sistemas dispares, y, en consecuencia, da lugar a mayores gastos operacionales. Por otra parte, la informática distribuida ofrece una mayor flexibilidad con la posibilidad de utilizar sistemas de múltiples proveedores con diferentes Sistemas operativos, aplicaciones y hardware.

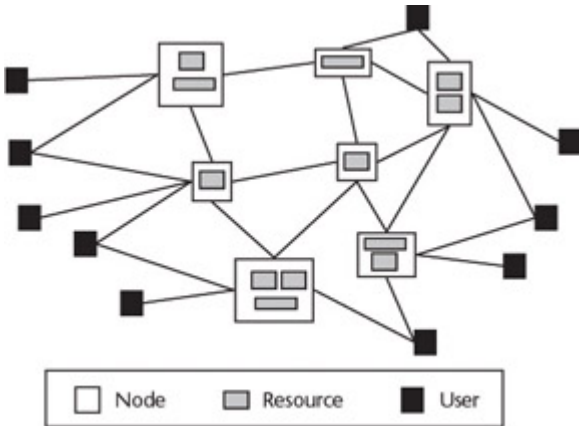


Figura 1.9 Arquitectura de Red Centralizada [3]

A primera vista, una arquitectura descentralizada podría implicar una mayor supervivencia y rendimiento en una red. Una interrupción en un lugar puede ser compensado por los sistemas en otros lugares. Siempre que la redundancia, tolerancia a fallos, y las medidas de recuperación se lleven a cabo con la utilización de otros sistemas de manera correcta. De lo contrario una falsa

sensación de seguridad existirá. De hecho, las arquitecturas distribuidas pueden aumentar el número de puntos de fallo en una red [3]. Cuanto mayor sea el número de nodos, mayor será la probabilidad de fallas o defectos en la estructura general de la red [3]. Redes descentralizadas requieren diseños compartidos para limitar el efecto de fallos en nodos.

- Redes Escalables

Una arquitectura de red escalable tiene la capacidad de adaptarse al cambio de una manera rentable para dar cabida a un aumento en la demanda. La escalabilidad implica principalmente el rendimiento aceptable, bajo condiciones y patrones de tráfico cambiantes. Pero una red escalable tiene consecuencias sobre la vulnerabilidad de fallos.

La escalabilidad es una medida del número de usuarios finales o los nodos de usuarios atendidos por una red. El alcance de una red es el número de usuarios finales y la ubicación de los nodos de usuarios a los que presta servicios (ej. aplicaciones). Un factor de escala (σ) puede ser estimado como la escalabilidad por unidad de alcance, o el porcentaje promedio de los usuarios atendidos por el servicio:

$$\sigma = 1/N$$

Donde N es el número de nodos (alcance o scope) y la escalabilidad el número de usuarios finales.

σ puede ser aplicado en casi cualquier contexto. Puede medir la densidad de carga de un servicio o aplicación por nodo, o la densidad de la conectividad. Redes que tengan una pequeña s (sigma), a veces denominado redes scale–free, disponen de más nodos de servicios que soportan a un puñado de usuarios. S (sigma) es para ser utilizado como un número bruto, transparente a la distribución de los usuarios a través de los nodos de servicio. Una red con una distribución uniforme de usuarios donde cada nodo de servicio maneja el mismo número de usuarios es a veces denominada una red exponencial. Figura 1.10 ilustra estos conceptos

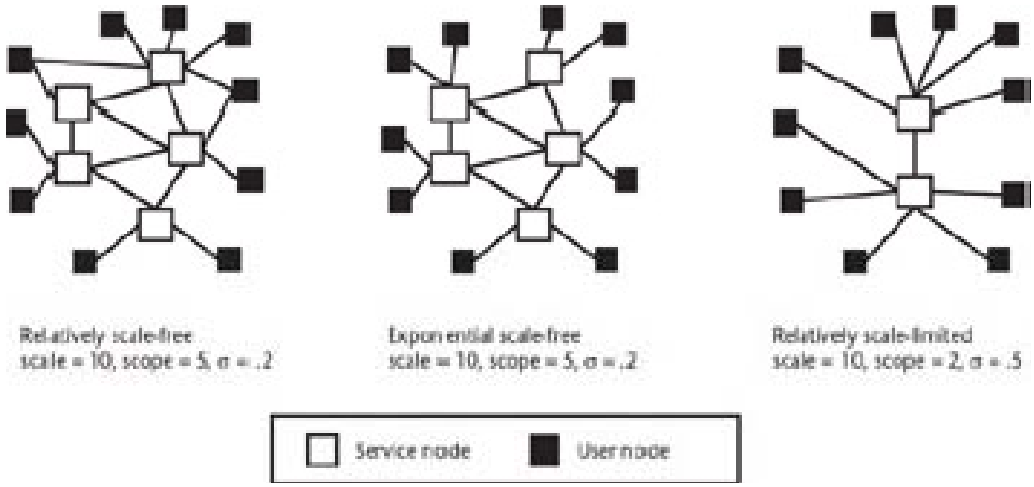


Figura 1.10 Factor escala de red. [3]

Redes que tengan altos valores de s (sigma) se dice que son de escala limitada y son difíciles de proveer un crecimiento rentable para dar cabida a la demanda. El fenómeno del efecto neto, expresado en La Ley de Metcalfe, establece que el valor potencial de una red es proporcional al número de nodos de usuario activo. Más precisamente, la utilidad de una red para los usuarios nuevos y existentes es igual al cuadrado del número de nodos de usuario. Aunque las redes con altos factores de escalabilidad proporcionan mayor valor potencial por nodo, son menos económicos para crecer [3].

s sigma tienen implicaciones sobre riesgos en la red. En general, las redes de escala libre (scale-free) implican arquitecturas distribuidas, que tienen una mayor probabilidad de interrupción. Pero como hay pocos usuarios servidos por nodo, la pérdida prevista en una interrupción nodal es menor. En una red de escala limitada, donde los usuarios están más concentrados en cada uno de los nodos, puede ocurrir un daño mayor.

Estos puntos pueden ilustrarse mediante la estimación de la mínima pérdida esperada en una red de N nodos, cada uno con un fallo posible p, igual a la probabilidad de un fracaso. La probabilidad de f fallos que ocurran en N nodos es estadísticamente caracterizada por la bien conocida Distribución binomial [3]:

$$P(f) = N!p^{f}(1-p)^{n-f} / f!(N-f)!$$

donde P(f) es la probabilidad de que se produzcan f fallos. Si P(0) indica el porcentaje del tiempo que no se producen fallos (f = 0), entonces 1 - P (0) es el porcentaje de tiempo en que uno o más fallos ocurrirán. Si nosotros aproximamos la suposición de que s sigma es el promedio de pérdidas nodal por fallo, medido en términos de porcentaje de usuarios ,entonces, sobre una amplia red de base, el riesgo mínimo (o porcentaje esperado de perdidas mínimas). En una red está dada por:

$$p = \sigma [1-P(0)]$$

En la figura 1.11 se demuestra gráficamente cómo varía con la escalabilidad de red en las diferentes interrupciones potenciales en los nodos P. Demuestra que invirtiendo para reducir las interrupciones potenciales en los nodos, sin importar la escalabilidad, puede en última instancia todavía dejar un porcentaje de usuarios en riesgo. La expansión del tamaño de la red para reducir el riesgo es justificada cuando la escalabilidad (número de nodos de usuarios) es limitada o, es decir los usuarios son concentrados (ver figura 1.10). La concentración dominará el riesgo hasta cierto punto, más allá de el cual el tamaño puede influenciar con mayor riesgo a la red.

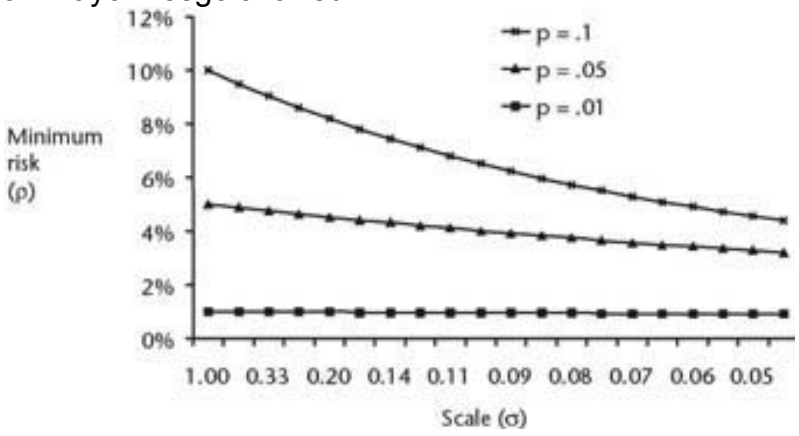


Figura 1.11 Ejemplo de Riesgo. [3]

Este análisis asume uniformidad en la distribución de usuarios, las potenciales interrupciones son aleatorias en cada nodo. Por supuesto, esta suposición puede no ser verdad en redes con una distribución de usuarios no uniforme y las potenciales interrupciones en los nodos es aleatoria. Una interrupción intencional contra una interrupción aleatoria no intencional en un nodo concentrado de usuarios, puede causar un gran daño. Sobre todo, las redes de escala-libres con menos funcionalidad concentrada por nodo son menos vulnerables a las interrupciones dirigidas, o no aleatorias que redes de escala limitada [3].

1.7.4. MÉTRICAS DE CONTINUIDAD

Métrica

La métrica debe estar vinculada al tema que se está midiendo. Además, un indicador debe estar vinculado a un objetivo de servicio. Debe ser utilizado para expresar el grado en que un objetivo ha sido cumplido.

Se debe tener presente, que el cálculo de un indicador debe ser coherente cuando se repite en el tiempo, de lo contrario, la comparación de los cambios relativos en los valores no tendría sentido. Los cálculos repetidos se deben basar en el mismo tipo de datos, el mismo rango de datos, y el mismo enfoque

de muestreo. La mayoría de las veces, los sistemas o servicios de red son comparados sobre medidas bases previstas por un vendedor o proveedor de servicios. La comparación de diferentes fabricantes o proveedores utilizando las medidas que cada uno de ellos ofrecen es a menudo difícil y muchas veces infructuosos, ya que cada uno desarrolla su métrica basada en sus propias metodologías [3].

Métricas de Recuperación

La recuperación implica todas las actividades que se necesitan para ejecutar desde el momento que se produce una interrupción del servicio, hasta que el mismo haya sido restaurado. Estas variaran entre organizaciones y, en función del contexto de uso, dentro del entorno de una red de misión crítica. Las actividades implicadas para recuperar un componente son un poco diferentes, que las que se necesitan para recuperar un centro de datos entero. Pero en cualquier caso, el significado general sigue siendo el mismo. Generalmente, las actividades de recuperación incluyen la declaración de que un evento adverso ha ocurrido (o está a punto de ocurrir), la inicialización de un proceso de tolerancia a fallos; actividades de restauración o de reparación del sistema; y reinicio, traslado, reanudación del servicio. Dos son las métricas de recuperación clave que se describen en las secciones siguientes.

RTO (RECOVERY TIME OBJECTIVE)

El objetivo del tiempo de recuperación (RTO) es una métrica para medir el tiempo transcurrido entre la ocurrencia de un evento adverso y la restauración del servicio. Es decir, el RTO debe medirse desde el momento en que la interrupción se produjo hasta que se reanude la operación. En entornos de misión crítica, esto significa que el funcionamiento debe ser básicamente el mismo, que antes que el evento ocurra. Algunas organizaciones de TI pueden alterar esta definición, disminuyendo algunos de los requisitos del estado de funcionamiento después de la reanudación y de aceptar un funcionamiento parcial como un estado de reanudación.

El RTO es un objetivo, especificado en horas y minutos el cual es determinado por la gerencia de una organización, como el tiempo aceptable de recuperación. El valor que una organización asigne como "aceptable", estará influenciada por una variedad de factores, entre ellos tenemos la importancia del servicio y la consiguiente pérdida de ingresos, la naturaleza del servicio, y la capacidad interna de la organización. En los sistemas, incluso puede ser especificada en milisegundos.

Un RTO puede ser aplicado a un componente de la red, como a todo un centro de datos. Las empresas definirán diferentes RTO para diferentes aspectos de su negocio. Para definir un RTO los administradores deben determinar cuanta interrupción del servicio puede tolerar el negocio. Ellos deben determinar cuánto tiempo una entidad funcional como es un proceso de negocio puede estar sin funcionamiento. Uno puede ver a menudo RTOs en el radio de acción

de 24 a 48 horas para grandes sistemas, sin que estos números reflejen ningún estándar de la industria. Las tiendas virtuales son poco probables a tolerar altos RTO sin una pérdida significativa de ingresos. Algunos mercados verticales, tales como la banca, deben atenerse a las exigencias de la industria financiera para la interrupción de las operaciones [2].

El costo finalmente es quien dirige la determinación del RTO. Un alto costo es requerido para alcanzar un bajo RTO de un particular proceso u operación. Para alcanzar RTOs cercanos a cero se requiere recuperación y redundancia automatizadas [3]. Un RTO de larga duración requiere menos redundancia costosa y más operación manual para la recuperación. Sin embargo, esto está relacionado directamente con la pérdida de negocio. Según muestra la figura 1.10 la pérdida se relaciona directamente con el RTO, a más largo RTO, mayor pérdida. En un cierto punto, hay RTO cuyos costes pueden compensar totalmente las pérdidas durante la recuperación [4, 5].

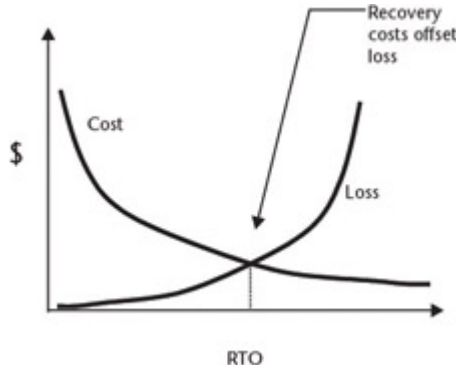


Figure 1.12 RTO versus pérdida y costo [3].

Resulta evidente que la definición de un RTO como única medida no tiene sentido sin una idea de qué nivel de servicio se debe proporciona para la recuperación. Para cada sistema se tendrá diferentes curvas de RTO. Los sistemas críticos tendrán más pequeños los valores de RTO, que los sistemas que no son críticos. Los sistemas que no son críticos tendrán RTOs que son tolerantes a la perdida.

Para esto se deben definir niveles de servicio para los sistemas críticos y asignar un valor a cada RTO. Por ejemplo tres niveles de servicio.

Nivel 1—restaurar al mismo nivel de servicio;
Nivel 2—restaurar al 75% del nivel del servicio;
Nivel 3— restaurar al 50% del nivel del servicio.

Un intervalo de tiempo se puede asociar a cada nivel así como también un descriptor del nivel de servicio proporcionado. Por ejemplo, un sistema es asignado a un nivel 2, RTO de 1 hora para terminar la recuperación dentro de ese marco de tiempo y una interrupción no más del 25% de servicio. A un

sistema se puede asignar un nivel 1, RTO de 1 hora también, pero debe restaurarse al mismo nivel de servicio. El nivel 1 podría requerir procedimientos de tolerancia a fallos o la recuperación a un sistema secundario.

Asumiendo que el nivel de servicio es proporcionalmente lineal al tiempo, RTOs a través de diversos niveles se pueden comparar en una misma escala de tiempo. Un tiempo equivalente RTO, RTO_E puede ser calculado:

RTOE = RTO / 1- (nivel de interrupción de servicio máxima)

En el ejemplo anterior para un RTO de nivel 2, requiere de un 75% de servicio que no se puede interrumpir, el cual equivale a un RTOE de 80 minutos.

TIEMPO DE RECUPERACIÓN DE COMPONENTES

Es el tiempo requerido por cada una de las actividades involucradas en la restauración de un servicio. Una falla en cualquiera de los componentes de las actividades podrían conducir a una violación significativa del RTO. Con este fin, a cada componente de la actividad se puede asignar un RTO también. La sumatoria de cada uno de los RTOs de estos componentes no necesariamente equivale al RTO del servicio, porque las actividades pueden ser llevadas a cabo en paralelo.

La funcionalidad de la red o la complejidad de un sistema por lo general plantean un mayor riesgo. En redes complejas, se puede requerir que el RTO sea pequeño, esto incluiría que el tiempo para diagnóstico y reparación sea pequeño, pero en algunos casos, esto no podría ser tan pequeño como se desearía. La tolerancia a fallos a sistemas redundantes es la contramedida más apropiada, ya que puede ahorrar el tiempo para el diagnóstico y reparación.

La figura 1.13 ilustra la serie continua de actividades de las áreas concernientes a una red de misión crítica. Por supuesto, éstos pueden variar pero son aplicables a la mayoría de las situaciones. Las áreas incluyen el siguiente:

- Recuperación de la red. Es el tiempo para restaurar la comunicación de datos y voz después de un evento adverso. Esta posiblemente tendrá impacto sobre otras actividades.
- Recuperación de datos. Es el tiempo para extraer los datos de respaldo del soporte de almacenamiento y enviarlos al sitio de recuperación, sea físicamente (mediante trasporte) o electrónicamente (via red). Incluye el tiempo de cargar los datos desde el medio (cinta, disco), instalar o reiniciar la aplicación de base de datos.
- Recuperación de aplicaciones. Es el tiempo para corregir una aplicación en mal funcionamiento.
- Recuperación de Plataforma. Es el tiempo para restaurar una plataforma problemática para la operación de servicios.

- Recuperación del servicio. Este representa el tiempo acumulado para restaurar el servicio desde la perspectiva del usuario final. Esto es en resumen el resultado de todos los tiempos de recuperación precedidos.

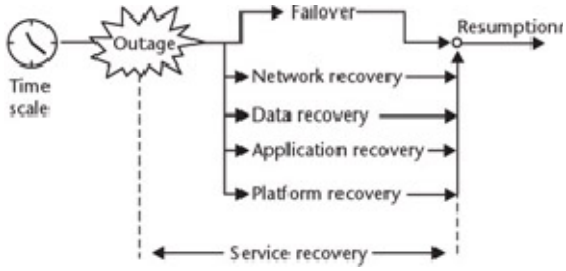


Figura 1.13 Continuidad en las actividades de recuperación. [3]

OBJETIVO PUNTO DE RECUPERACIÓN (RPO)

El objetivo del punto de recuperación (RPO) se utiliza como métrica para la recuperación de los datos. También se mide en términos de tiempo, pero hace referencia a la edad o a la frescura de los datos requeridos para restaurar la operación que sigue a un acontecimiento adverso. Los datos, en este contexto, pueden también incluir la información con respecto a las transacciones no registradas o no capturadas. Como el RTO, cuanto más pequeño es el RPO, más alto son los costos de la recuperación prevista de los datos. La recarga de una cinta de respaldo diaria puede satisfacer una tolerancia en la perdida de datos de no más de 24 horas. Sin embargo, una tolerancia de sólo un minuto de pérdida datos o de transacciones puede requerir métodos más costosos de transferencia de datos, tales como mirroring.

Algunos confunden el RPO como el tiempo transcurrido desde que ocurrió el evento adverso hasta la recuperación de los datos (pero éste se conoce como TTD). El RPO es el punto en el tiempo, al cual los datos deben ser recuperados, a veces designado la ventana de frescura. Es el máximo tiempo tolerable transcurrido entre el último respaldo seguro y el punto de recuperación. Una organización que no puede tolerar ninguna pérdida de datos (es decir, RPO = 0) implica que los datos tendrían que ser restaurados instantáneamente después de un acontecimiento adverso y tendrían que emplear un sistema de respaldo continuo.

Métricas de Costo

La diferencia entre riesgos y pérdidas, el riesgo abarca la incertidumbre, mientras que el costo es determinista. Los cambios repentinos en las circunstancias
producen incertidumbre. El cambio inesperado en la operación de una red produce la desafortunada posibilidad de incurrir en costos. El costo es el cálculo del pago de la interrupción de un único servicio. El coste de una interrupción (también denominados costes de inactividad) puede ser de gran

alcance. Este es presentado y normalizado de diversas maneras. Muchos cuantifican en términos de costo por hora del servicio no disponible. Otros especifican como el costo de no disponibilidad por usuario o por empresa. En E-business se ha fijado en términos de costes por hora por aplicación o el costo por transacción. La actual unidad de medida para determinar los costos, dependerá del contexto de uso y de la situación. Aunque las unidades monetarias puedan parecer la unidad de medida más universal, otras unidades pueden utilizarse. Por ejemplo, las unidades que miden la producción, tales como las operaciones, llamadas, widgets, y megabytes son utilizadas a menudo por las organizaciones operacionales para la ejecución o planificación de gastos. Esto elimina muchas de las ambigüedades asociadas a los costes y determina el costo en términos más precisos.

Los costos de degradación del servicio o tiempos lentos no deben pasarse por alto. La aparición de la lentitud, que es la degradación del servicio por debajo de niveles aceptables, a menudo es más frecuente que la interrupción del servicio. Aunque el servicio se ha degradado, no fue interrumpido. Sin embargo, la productividad y el rendimiento del sistema se ven afectados negativamente. Los tiempos lentos son a menudo más caros que el tiempo de interrupción: a menudo no se reportan, pero en entornos básicamente transaccionales, por ejemplo, puede ser debilitante. Un enfoque conservador para la asignación de valores de métrica de costos debería implicar una cierta especificación de rendimiento-sobre los niveles que constituyan umbrales aceptables de la disponibilidad y de la interrupción del servicio.

Los costos de inactividad varían entre las organizaciones. Muchos estudios se han realizado para cuantificar los costos por hora de inactividad a través de diferentes industrias. Los costes por hora pueden variar desde miles a millones de dólares, dependiendo del tipo y el tamaño de la empresa. Por ejemplo, para empresas financieras y de corretaje, los costos de inactividad están directamente relacionados con los desastres abruptos. En E-business, por otro lado, se enfocan en la interrupción y la disponibilidad transaccionales del sitio Web. Además de los costes por pérdida de transacciones, son muy sensibles a la imagen corporativa, a los costes judiciales resultantes de litigios, a la devaluación de valores, a la erosión de la marca de fábrica, y al descontento del cliente. Al final, cada industria pondrá énfasis sobre los componentes particulares del coste de inactividad.

Algunos de los resultados de los estudios de coste de tiempo de interrupción no son cantidades reales del coste, sino la identificación de qué factores tienen un efecto pronunciado sobre este coste para diversos tipos de organizaciones. Algunos de estos factores incluyen [24]:

- La dependencia de la tecnología. Las empresas que son impulsadas por la tecnología, tales como telecomunicaciones, energía, industria manufacturera que depende de tecnologías, y las industrias financieras a menudo muestran altos costos de inactividad.

- Intensidad de Trabajo. Las empresas que dependen menos de la infraestructura de TI y necesitan más mano de obra, tales como la atención de la salud y las industrias de servicios, son menos propensos a los costes de inactividad.
- Intensidad de capital. Empresas intensivas en capital pueden presentar menores costes directos de inactividad, pero altos costos indirectos, reflejando la capacidad de protección, pueden cargar la rentabilidad.
- Intensidad de Margen. Las empresas, de bajo margen y alto volumen de capital, son propensas a graves costes de inactividad. Estas a menudo representan a las empresas, tales como el comercio minorista. En este tipo de empresas, hay poco margen para que los incentivos permitan recuperar de nuevo a clientes perdidos a raíz de una interrupción. Estas empresas exhiben altos costes indirectos de inactividad.
- Mercado cautivo. Las empresas que tienen una base exclusiva de clientes, ya sea a través de un producto o servicio especializado o general, un monopolio, pueden soportar la posibilidad de continudad en las operaciones de negocio debido a interrupciones del servicio. La experiencia ha demostrado que es poco probable que los clientes deserten después de una interrupción, estas empresas suelen ser objeto de controles normativos y jurídicos.

Realmente no hay estándares relacionados con la categorización de los costos de inactividad. Las diferentes industrias, países, políticas de compañías, y las prácticas contables han dado lugar a distintas formas de expresar los costes. Hay generalmente tres tipos de costos asociados con la inactividad: directos, indirectos y costos intangibles. Los costes directos son aquellos que de inmediato se materializan como resultado de una interrupción. Los costos indirectos son aquellos que representan los efectos secundarios y pueden ser a menudo bastante significativos. Los costos directos e indirectos que sean cuantificables, se consideran los costos tangibles, mientras que los costos intangibles son los de índole cualitativa o no fácilmente cuantificable. Costos Avoided (costos que se evita incurrir cuando se produce la falla) son los que no son ocasionados por la interrupción. El verdadero costo de inactividad, C, se obtiene de la suma de estos costes:

C = C (direct) + C (indirect) + (intangible) – C (avoided)

A continuación se listan algunos de los componentes que conforman los costes de inactividad [25]. La definición de estas categorías y la inclusión o exclusión de determinados costes en el coste global de tiempo de inactividad ha sido el tema de mucho debate.

Costos directos:

- Costos de Recuperación. Está relacionado con el tiempo y costos asociados con la restauración del servicio de red a su operación normal. Los costes de la recuperación generalmente se relacionan directamente con el grado y alcance de la interrupción del servicio. Cuanto más larga

es la interrupción, es menos probable una recuperación y más alto es el coste de recuperación

- Pérdida de ingresos. Este es el valor de la pérdida de ventas que de otro modo habría, si no se hubiera producido una interrupción. Indicando un valor monetario de la pérdida de las transacciones, o alguna otra unidad de producción, a menudo supone una tasa constante de las ventas por hora que es aplicado a la hora de la interrupción. Debido a que esta pérdida no es vista como un coste de "reserva", su inclusión como un costo directo es discutible.
- Daños a Activos. Este es el costo para recuperar los activos que han sido destruidos, dañados, o extraviados como resultado de una interrupción. Estos costos están asociados con la pérdida o daño de datos, software, sistemas, equipos, materiales, y otros relacionados con la infraestructura de TICs.
- Costos de Solución. Estas son las devoluciones, créditos, sanciones, y tarifas asociadas con incumplimiento de los compromisos de servicio a los clientes u otras entidades como consecuencia de una interrupción.
- Exposiciones de regulación. Estas son las multas, sanciones, y tarifas como resultado de violaciones de leyes o reglamentos del gobierno o de los organismos reguladores.

Costos Indirectos

- Costos de Capacidad de protección. Son el capital y gastos operativos asociados con las medidas de protección para evitar la interrupción del servicio. Puede incluir personal extra, sistemas, piezas de repuesto, y capacidad de infraestructura. Estos costos son típicamente realizados sobre una base anual frente a la hora exacta de una interrupción.

- Pérdida de productividad. Esto representa el costo de pagar por los activos que de otro modo producirían servicios si no ocurriera la interrupción. Esta es dividida en dos categorías:
    - Costos que representan el tiempo por empleado que no es productivo, porque su trabajo útil, es afectado por la interrupción, así como tiempos de gestión improductiva. Este costo debe incluir también el tiempo extra de los empleados, para recuperar el trabajo que no se ha realizado durante la interrupción.
    - Costos que representan la no utilización de los sistemas, software y equipos que de otro modo brindarían servicios que producen ingresos.
- Exposición Legal: Estas son las tasas y los costos para la solución de controversias con los clientes, proveedores, accionistas, u otras entidades en torno a la interrupción del servicio. Esto también puede ser visto como un coste directo en función de la circunstancia.
- Exposición de Responsabilidad. Este es el aumento de las primas de seguros y los costes resultantes de la interrupción del servicio.
- Capitalización de mercado. Esto incluye la devaluación y la pérdida de valores de los inversores como resultado de la interrupción del servicio.

Costes intangibles:

- Percepción del mercado. Una interrupción del servicio, particularmente importante, puede ser una indicación de que hay algo malo en general con una operación. Otros en la industria se preguntaran sobre la integridad en la gestión y del personal, e incluso vacilaran en realizar negocios. La publicidad, la reputación, la imagen pública, la confianza de los clientes, y la identidad de la marca pueden ser afectadas negativamente.
- Desgaste de clientes. La insatisfacción de los clientes como resultado de una interrupción del servicio, genera pérdida de los mismos. Los clientes existentes que representan las ventas actuales, así como clientes potenciales que representan las ventas futuras, son motivados a realizar sus negocios en otros lugares.
- Retención del cliente. Los costos para retener a los clientes pueden manifestarse de varias maneras. Estos incluyen costos tales como los servicios para atender el incremento de las quejas de los clientes en términos de denuncias, llamadas de servicio, costos para soporte de servicios, e incentivos para que los clientes esperen.
- Perdida de financiamiento. Además de perjudicar a una empresa en el balance final, muchos de los factores antes mencionados pueden afectar también a las empresas en su calificación crediticia y la capacidad de buscar financiación.
- La moral de los empleados. La cultura de la organización puede verse afectada, si muchos de los factores antes mencionados impactan a una empresa, en el balance final y por consiguiente causa la pérdida posterior de personal. Una baja moral afecta la calidad del servicio y el rendimiento.
- Posición en el mercado. Pérdida de cuota de mercado y la posición relativa respecto de los competidores podrían afectar la competitividad global.
- Utilización de activos. El no uso de los activos productivos durante una interrupción de servicio en última instancia, afecta la rentabilidad de los activos en un balance. Sistemas, aplicaciones, redes, servicios de tecnología y la infraestructura se consideran activos.

CAPITULO 2

2. ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para realizar un análisis de los riegos, se procede a identificar los recursos de TICs que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la empresa, y su importancia dentro del funcionamiento de la misma. Es necesario reconocer y reducir los riesgos potenciales que afecten a los productos y servicios; es por ello que se considera dentro de un Plan de Contingencia, como primer paso la Reducción de Riesgos, para favorecer el cumplimiento de los objetivos institucionales.

Para realizar el Análisis y Evaluación de Riesgos se dividen en dos grandes procesos que a continuación se detallan.

2.1. ANALISIS DE RIESGOS

Un análisis de riesgos es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. El análisis de riesgos permite tomar decisiones de inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro alternativo para asegurar la continuidad de la actividad, pasando por las decisiones de adquisición de salvaguardas técnicas, selección y capacitación del personal.

Para realizar el proceso de Análisis de Riesgos se ha identificado las siguientes tareas:

- Identificación de los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Identificación de las amenazas significativas sobre aquellos activos, y la valoración en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Identificación de salvaguardas existentes y la valoración de la eficacia de su implantación.
- Estimación del impacto y el riesgo al que están expuestos los activos del sistema.
- Interpretación del significado del impacto y el riesgo.

2.1.1. IDENTIFICACIÓN DE ACTIVOS

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado “modelo de valor” ver Libro de trabajo de la empresa eléctrica. El resumen de esta valoración se encuentra en las tablas 2.1, 2.2, 2.3, 2.4.

2.1.1.1. IDENTIFICACIÓN DE LOS ACTIVOS

OBJETIVO DE LA ACTIVIDAD

Identificar los activos que componen el dominio, determinando sus características, atributos y clasificación en los tipos determinados.

PRODUCTOS DE ENTRADA

Los productos de entrada que se utilizaron en este punto para la identificación de activos son:

- Los procesos de Negocio principales de la empresa, los cuales se encuentran descritos detalladamente en el anexo A-3.
- Levantamiento del Inventario de Datos en el Libro de trabajo
- Levantamiento de Inventarios de Equipos físicos en el Libro de trabajo
- Levantamiento de Inventarios de Software en el Libro de trabajo
- Levantamiento de Inventarios de Equipo de Comunicaciones en el Libro de trabajo.
- Diagramas de red.
- Mediante entrevistas.

ACTIVOS IDENTIFICADOS

Para la identificación de los activos se utilizaron los datos proporcionados por el administrador de la red, y para facilitar el análisis y gestión de riesgos se han dividido los activos en cinco categorías de información, a continuación se detalla cada una de las cinco categorías:

Información

Activos Auxiliares
Descripción: Otros dispositivos que ayudan al funcionamiento de la organización soporte estático no electrónico que contiene datos.
Activos

- Suministros de Oficina

Documentación y Registros
Descripción: Soporte estático no electrónico que contiene datos.
Activos • Actas • Documentación de Procesos (Plan Operativo Anual POA) • Contrato con Proveedores • Contrato con Clientes • Memos • Oficios • Reglamento SRI • Manuales de los sistemas y de usuario. • Informes de Consultorias • Reglamentos de la empresa.

Software

Sistemas Operativos:
Descripción: Esta denominación comprende todos los programas de una computadora que constituyen la base operativa sobre la cual se ejecutarán todos los otros programas (servicios o aplicaciones). Incluye un núcleo y funciones o servicios básicos. Dependiendo de su arquitectura, un sistema operativo puede ser monolítico o puede estar formado por un micronúcleo y un conjunto de módulos del sistema. El sistema operativo abarca principalmente todos los servicios de gestión del hardware (CPU, memoria, discos, periféricos e interfaces redes), los servicios de gestión de tareas o procesos y los servicios de gestión de usuarios y de sus derechos.
Activos • Windows Server 2003 Enterprise Edition SP1,SP2 • Aix V5.1 • OS/400 5.3 (ESTÁNDAR) • WIN 2000 SERVER • Linux version 7.3 • Windows XP Profesional SP 2 • Windows NT

Paquete de programas o software estándar
Descripción El software estándar o paquete de programas es un producto comercializado como tal (y no como desarrollo único o específico) con soporte, versión y mantenimiento. Presta un servicio « genérico » a los usuarios y a las aplicaciones pero no es personalizado o específico como la aplicación profesional.
Activos • Antivirus F-Security Cliente. • Software de declaraciones para el SRI. • Software de atención al cliente mediante el call center • Microsoft office 2003 • Microsoft office 2010 • Nero Suite • Genexus • Microsoft Project • Software menejador de base de datos Oracle • Software menejador de base de datos DB2 • Lotus Note y Dominio.

Software de Aplicación
Descripción Datos y servicios informáticos compartidos y privados, que utilizan los protocolos y tecnologías de comunicación (por ejemplo, tecnología de Internet).
Activos • Aplicación SICO • Sistema Administrativo Financiero • Sistema de Recursos Humanos • Sistema de Atencion al Cliente Interno y Externo • Sistemas Documentales y Correo Electrónico • Portal Web

Activos Físicos

Hardware Portátil
Descripción Hardware informático diseñado para poder ser transportado manualmente con el fin de utilizarlo en lugares diferentes.
Activos • Portátiles

PC's de Oficina
Descripción. Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo.

Activos
• Estaciones de trabajo.

Equipos de Oficina
Descripción. Hardware para la recepción, la transmisión o la emisión de datos.
Activos
• Impresoras, Copiadoras, Teléfonos, Fax.

Servidores
Descripción. Hardware informático que pertenece al organismo y maneja información importante de la empresa y clientes.
Activos
• Servidor de Base de datos • Servidor de Correo electrónico • Servidor de Dominio y DHCP • Servidor de Aplicaciones • Servidor de Bases de Conocimiento • Servidor de Respaldos • Servidor de Antivirus

Soporte electrónico
Descripción. Soporte informático conectado a una computadora o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos sin modificar su pequeño tamaño. Se utiliza a partir de equipo informático estándar.
Activos
• CD-ROM, disco duro extraíble, memoria extraíble, cintas

Medios de comunicación
Descripción. Los medios o soportes de comunicación y telecomunicación pueden caracterizarse principalmente por las características físicas y técnicas del soporte (punto a punto, difusión) y por los protocolos de comunicación (enlace o red – capas 2 y 3 del modelo OSI de 7 capas).
Activos
• Cableado Estructurado, tecnología Ethernet, cables, Switch, MODEM, Firewall Nokia, fibra óptica.

Establecimiento
Descripción. El tipo establecimiento está formado por el conjunto de lugares

que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.
Activos • Edificio, centro de datos del séptimo piso, oficinas, zona de acceso reservado, zona protegida.

Servicios

Comunicación
Descripción. Servicios y equipo de telecomunicaciones brindados por un prestador
Activos • Línea telefónica, central telefónica, redes telefónicas internas, internet.

Energía
Descripción. Servicios y medios (fuentes de energía y cableado) necesarios para la alimentación eléctrica del hardware y los periféricos.
Activos • Entrada de la red eléctrica • UPS • Generadores de energía eléctrica.

Correo Electrónico
Descripción. Dispositivo que permite, a los usuarios habilitados, el ingreso, la consulta diferida y la transmisión de documentos informáticos o de mensajes electrónicos, a partir de computadoras conectadas en red. .
Activos • Correo electrónico interno, correo electrónico vía web, sistema documental.

Portal Externo
Descripción. Un portal externo es un punto de acceso que encontrará o utilizará un usuario cuando busque información o un servicio del organismo. Los portales brindan un gran abanico de recursos y de servicios.
Activos • Portal de información (Página Web de la empresa)

Personas

Empleados
Descripción. Es el personal que manipula elementos delicados en el marco de su actividad y que tiene una responsabilidad particular en ese tema. Puede disponer de privilegios particulares de acceso al sistema de información para cumplir con sus tareas cotidianas .
Activos • Personal del Área de Informática

2.1.1.2. DEPENDENCIAS ENTRE ACTIVOS

OBJETIVO DE LA ACTIVIDAD

Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

PRODUCTOS DE ENTRADA

- Identificación de Activos
- Procesos de negocio

METODO UTILIZADO

El método utilizado para analizar la dependencia entre activos, es el top-down, el cual parte desde los procesos de negocio, los servicios, software de sistemas y aplicaciones, datos, equipos, comunicaciones, personal.

RESULTADOS DEL ANALISIS DE DEPENDENCIA

Para determinar la dependencia que existen entre los activos identificados, se realizaron diagramas de dependencia, que sirvan de base para obtener los resultados. Los cuales se encuentran en el anexo 8.4.

2.1.1.3 VALORACIÓN DE LOS ACTIVOS

OBJETIVO DE LA ACTIVIDAD

- Identificar en qué dimensión es valioso el activo
- Identificar los escalones de Interrupción para recuperar el activo.

- Valorar el impacto que para la Organización supondría la destrucción del activo

PRODUCTOS DE ENTRADA

- Identificación de Activos
- Dependencia de los Activos
- Identificar en qué dimensión es valioso el activo

ESCALONES DE RECUPERACION

Los escalones de recuperación que se utilizaron para valorar los activos en la dimensión disponibilidad son los siguientes:

Escalones de Recuperación	Descripción
45 min	Se dispone de máximo 45 mi para dar una primera respuesta a un incidente de nivel de error crítico, que ha surgido sobre un activo crítico (de prioridad 1 para la escala que maneja Centro Sur, y de valor 5 para la metodología magerit). Son aquellos activos altamente críticos para la continuidad del negocio.
60 min	Este tiempo es para activos de prioridad media (2 para la escala que maneja Centrosur, y de valor 4 para metodología Magerit) y el error es de nivel medio.
90 min	Este tiempo de respuesta se aplica para sistemas de nivel crítico (5 para Magerit o 1 para escala de CentroSur) y el error es medio o cuando el sistema tiene una prioridad de nivel bajo (escala de 3 para magerit o 3 para Centrosur) y el error es crítico.
120 min	Tiempo de respuesta para sistemas de nivel de prioridad (7-8 para la metodología magerit o 2 para la escala que maneja Centrosur) y el nivel de criticidad del incidente es medio.
1 día	Este tiempo se aplica para activos cuya prioridad es baja (menor a 6 en la escala de Magerit o 3 para la

	escala que maneja Centrosur) y el error tiene un nivel de criticidad bajo.

Nivel de Error sobre los activos

Nivel de Error	Descripción
Nivel 1: Crítico	Cuando la aplicación o el servicio están fuera de operación y ninguno de los usuarios puede trabajar.
Nivel 2: Medio	Cuando la aplicación o el servicio está operando, pero algunas de las funciones más críticas no están disponibles y por ende, no todos los usuarios pueden seguir trabajando.
Nivel 3: Bajo	Cuando la aplicación o el servicio presentan algún problema que no afecta significativamente al trabajo del usuario, es decir, éste puede continuar con sus tareas.

ESCALA DE VALORACION

Valor	Categoria	Descripción
5	**Muy alto**	daño muy grave a la organización
4	**Alto**	daño grave a la organización
3	**Medio**	daño importante a la organización
2	**Bajo**	daño menor a la organización
1	**Despreciable**	irrelevante a efectos prácticos

RESULTADOS DE LA VALORACION

La valoración utilizada en esta tesis es una valoración cualitativa, facilitando una rápida valoración y estimación de costes abastractos, como la pérdida de la credibilidad.

Los criterios de valoración que se utilizaron, son los propuestos por la metodología de Magerit v 1.2, el cual utiliza una escala de valoración cualitativa detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). En el anexo A-2 se encuentra la escala de valoración detallada.

Para la valoración de los activos de la empresa, se empezó por la valoración de los procesos de negocio críticos, tomando de las dimensiones de seguridad la disponibilidad [D], como la dimensión para la valoración del riesgo que afecte la continuidad de este tipo de activo.

Categoría Activos	Activo	Valoración Margerit	Valoracion CentroSur
Procesos de Negocio	Facturación	5	1
	Lecturas	5	1
	Recaudación	5	1
	Consumos	5	1
	Servicios	3	2
	Cartera	3	2
	Contabilidad	3	2
	Compras	3	2
	Nomina	3	2
	Inventarios	3	2
	Gestión Tributaria	3	2

Tabla 2.1 Valoración de los Procesos de Negocio de la Empresa Eléctrica Centro Sur.

En base a los resultados presentados en la tabla 2.1 se puede determinar que estos son los procesos críticos para la continuidad del negocio de la empresa sobre los cuales se va a trabajar en el diseño del Plan de Contingencias. El resto de procesos serán incluidos posteriormente en una segunda etapa de evaluación de continuidad del Negocio de la empresa. Para este tipo de activos solo se tiene en cuenta el valor Individual del mismo, ya que no tiene elementos superiores que dependan de este.

A partir de esto se procede a valorar los servicios y sistemas informáticos que soportan cada uno de estos procesos.

Categoría Activos	Activo	Valoración Margerit	Valoracion CentroSur
Servicios	Comunicaciones o Red	5	1
	Intranet	3	2
	Atención al Cliente	5	2
	Web	3	2
	Correo electrónico y documentales	4	2

	Help Desk	5	2
	Antivirus	3	2
	Internet	3	3

Tabla 2.2 Valoración de los Servicios de la Empresa Eléctrica Centro Sur.

Cada uno de los servicios que se listan en la tabla 2.2, corresponden a los servicios que se proveen tanto al usuario final (cliente de la empresa eléctrica), así como a los usuarios de los servicios de TICs. Las dimensiones de seguridad que se tomaron en cuenta para esta valoración según la sugerencia de la metodología de Magerit v 1.2 es la disponibilidad [D].

A continuación se presenta la valoración de los Sistemas Informaticos, que ayudan como backend de los procesos y servicios críticos del negocio.

Categoría Activos	**Activo**	**Valoración Margerit**	**Valoracion CentroSur**
Sistemas Informáticos/ Aplicaciones	Sistema de Comercialización	5	1
	Sistema Administrativo Financiero	3	2
	Recursos Humanos	3	2
	Sistemas de Atención al Cliente Interno y Externo	5	2
	Portal Web	3	2
	Sistemas Documentales y Correo Electronico	4	2
	Sistema Comercial de Telecomunicacion	5	1

Tabla 2.3 Valoración de los Sistemas Informaticos de la Empresa Eléctrica Centro Sur.

Finalmente, en la siguiente tabla se listan los activos de tipo hardware críticos del centro de datos principal, que dispone la empresa eléctrica, sobre los cuales se ejecutan los principales Sistemas informáticos y servicos para la continuidad de la empresa eléctrica.

Categoría Activos	Activo	Valoración Margerit	Valoracion CentroSur
Servidores y Equipos de comunicación del centro de datos principal	Servidor Blade	5	1
	i-series MODELO 520 Servidor de Pruebas	5	1
	i-series MODELO M25 Servidor de PRoduccion	5	1
	SERVIDOR HP DL140	5	1
	Computador COMPAQ PIII	5	1
	SERVIDOR HP 2110	5	1
	AS/400 MODELO 270	5	1
	SERVIDOR HP PROLIANT ML530	5	1
	SERVIDOR COMPAQ 530	5	1
	i-Serie 520 8203-EA4	5	1
	pseries 610C1	5	1
	pSeries 510	5	1
	PC HP	5	1
	FIREWALL NOKIA IP350	5	1
	Itanium	5	1

Tabla 2.4 Valoración de los Servidores y Equipos de comunicación

La valoración se enfocó en este tipo de activos que son los puntos críticos en el negocio, que en caso de fallo o interrupción, pueden provocar problemas a la organización.

2.1.2. IDENTIFICACIÓN DE AMENAZAS

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por la frecuencia estimada de ocurrencia y la estimación de daño (degradación) que causarían sobre los activos.

El resultado de esta actividad es el informe denominado “mapa de riesgos”.

2.1.2.1. IDENTIFICACIÓN DE LAS AMENAZAS

OBJETIVOS DE LA ACTIVIDAD

- Identificar las amenazas relevantes sobre cada activo

PRODUCTOS DE ENTRADA

- Criterios de evaluación
- Caracterización de los activos

RESULTADOS

Las amenazas identificadas para cada uno de los tipos de activos, los cuales son críticos para la continuidad del negocio, se encuentran listadas a continuación. Estas amenzas están sacadas del catálogo de la Metodología de Magerit v 1.2, identificadas de otras fuentes y entrevistas realizadas al personal de la empresa Eléctrica Centro Sur:

Amenazas de Desastre naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. [6]

Dentro de los Desastres naturales [N.*], se entienden otros incidentes que se producen sin intervención humana como: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras. Se excluyen desastres específicos tales como incendios e inundaciones, porque estos ya se los identifica específicamente, en las amenazas (ver [N.1]) y (ver [N.2]) en la tabla 2.5. Se excluye al personal por cuanto se ha previsto una amenaza específica [E.28] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. [6]

[N] Desastres naturales	
[N.1]	Fuego
[N.2]	Daños por agua
[N.*]	Desastres naturales

Tabla 2.5 Amenazas de Desastres Naturales

Amenazas de Origen Industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada. [6]

Dentro de los Desastres industriales [I.*] se incluyen otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico. Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]) porque de igual manera estas se identifican individualmente en la tabla 2.6. Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.28] que se encuentra en la tabla, para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. [6]

[I] De origen industrial	
[I.1]	Fuego
[I.2]	Daños por agua
[I.*]	Desastres industriales
[I.3]	Contaminación mecánica
[I.4]	Contaminación electromagnética
[I.5]	Avería de origen físico o lógico
[I.6]	Corte del suministro eléctrico
[I.7]	Condiciones inadecuadas de temperatura y/o humedad
[I.8]	Fallo de servicios de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales
[I.10]	Degradación de los soportes de almacenamiento de la información
[I.11]	Emanaciones electromagnéticas

Tabla 2.6 Amenazas de Origen Industrial

Errores y Fallos no intencionados

Fallos no intencionales causados por las personas [6]. La secuencia en la numeración de estos errores se encuentra combinada, con la secuencia de los ataques intencionados (ver tabla 2.8). Esto es una manera en que la metodología de Margerit lo establece.

[E] Errores y fallos no intencionados	
[E.1]	Errores de los usuarios
[E.2]	Errores del administrador
[E.3]	Errores de monitorización (log)
[E.4]	Errores de configuración
[E.7]	Deficiencias en la organización
[E.8]	Difusión de software dañino
[E.9]	Errores de [re-]encaminamiento
[E.10]	Errores de secuencia
[E.14]	Escapes de información

[E.15]	Alteración de la información
[E.16]	Introducción de información incorrecta
[E.17]	Degradación de la información
[E.18]	Destrucción de información
[E.19]	Divulgación de información
[E.20]	Vulnerabilidades de los programas (software)
[E.21]	Errores de mantenimiento / actualización de programas (software)
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)
[E.24]	Caída del sistema por agotamiento de recursos
[E.28]	Indisponibilidad del personal

Tabla 2.7 Errores y Fallos no intencionados

Ataques intencionados

Fallos deliberados causados por las personas. [6]

[A] Ataques intencionados	
[A.4]	Manipulación de la configuración
[A.5]	Suplantación de la identidad del usuario
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino
[A.9]	[Re-]encaminamiento de mensajes
[A.10]	Alteración de secuencia
[A.11]	Acceso no autorizado
[A.12]	Análisis de tráfico
[A.13]	Repudio
[A.14]	Interceptación de información (escucha)
[A.15]	Modificación de la información
[A.16]	Introducción de falsa información
[A.17]	Corrupción de la información
[A.18]	Destrucción la información
[A.19]	Divulgación de información
[A.22]	Manipulación de programas
[A.24]	Denegación de servicio
[A.25]	Robo
[A.26]	Ataque destructivo
[A.27]	Ocupación enemiga
[A.28]	Indisponibilidad del personal
[A.29]	Extorsión
[A.30]	Ingeniería social

Tabla 2.8 Ataques Intencionados.

2.1.2.2. VALORACION DE LAS AMENAZAS

OBJETIVOS DE LA ACTIVIDAD

- Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

PRODUCTOS DE ENTRADA

- Identificación de las amenazas
- Series históricas de incidentes
- Antecedentes: incidentes en la Organización

RESULTADOS DE LA VALORACION

De la valoración de los activos se procede a analizar las amenazas a los que están expuestos. Para cada amenaza sobre cada tipo de activo se ha registrado la siguiente información:

- estimación de la frecuencia de la amenaza
- estimación del daño (degradación) que causaría su materialización
- explicación de las estimaciones de frecuencia y degradación
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- **degradación:** cuán perjudicado resultaría el activo, siendo 0 una degradación despreciable y 1 una degradación total del activo.
- **frecuencia:** cada cuánto se materializa la amenaza.

Frecuencia de Ocurrencia	**Categoria**	**Descripción**
5	Muy alta	Frecuencia diaria
4	Alta	Frecuencia mensual
3	Media	Frecuencia Normal una vez al año

2	Baja	Poco Frecuente cada varios años
1	Muy Baja	Infrecuente

Tabla 2.9 Escala de Frecuencia de ocurrencia de una amenaza. [7]

Impacto	Categoria	Descripción	Rango de Valores
1	Muy baja	El evento no provoca un impacto en los procesos. La interrupción de los servicios de TI afecta a uno o algunos usuarios, pero no dura lo suficiente para provocar un impacto en sus procesos	menor que 10.000
2	Baja	El evento genera un leve impacto en los procesos, pero no ocasiona una interrupción importante en las operaciones. La interrupción de los servicios de TI afecta a menos de un 30% de los usuarios y dura lo suficiente para afectar levemente sus operaciones.	menor que 100.000
3	Media	El evento provoca una interrupción en los servicios de TI y esto afecta los procesos, pero las actividades críticas no son interrumpidas.	menor que 1.000.000
4	Alta	El evento provoca una interrupción entre parcial y completa de la Tecnología en Informática y afecta a todos sus procesos	menor que 10.000.000
5	Muy Alta	El evento provoca una interrupción completa de la Tecnología en Informática y de todas sus operaciones. Los procesos críticos del negocio no tienen acceso a las instalaciones y tampoco a los recursos de información.	mayor que 10.000.000

Tabla 2.10 Escala de Impacto de una amenaza. [7]

MAPA DE RIESGOS

FECHA:

VERSION:

DESCRIPCION:

PROPIETARIO:

ORGANIZACIÓN:

AMENAZAS PARA EL TIPO DE ACTIVO HARDWARE

ACTIVOS POR AMENAZA

AMENAZAS PARA EL TIPO DE ACTIVO HARDWARE

Amenazas:	Porcentaje de degradación	Frecuencia de la amenaza:	Justificación:
Incendio o Fuego (N.1, I.1)	1	Muy Bajo (1)	Como resultado de la valoración de la amenaza sobre los activos identificados, se puede ver que esta amenaza no ha sido contemplada por ninguno de los entrevistados, sin embargo, el impacto en caso de ocurrir es muy alto y no debe ser obviado. En otros Centros de cómputo de la misma empresa, no cuenta con un extintor, ni con sistemas de detección de humo, por ello el riesgo residual de estos activos es mayor, pero sigue siendo mínima la frecuencia. En el centro de datos principal se cuenta con un sistema de detección de incendios para los servidores y equipos de comunicación principal, pero para las otras áreas donde se encuentra equipos de comunicación no se dispone de este sistema. Además no se tiene el conocimiento ni se encuentra documentado el funcionamiento de este sistema de detección de incendios. Por este motivo, si bien es cierto que la empresa a nivel tecnológico no requiere adquirir ningún otro tipo de herramienta tecnológica, para disminuir la amenaza, si se debería incluir un software que permita a una persona responsable monitorear y documentar su funcionamiento y asegurarse que si se presenta la amenaza este funcionando. De lo contrario sería como no tener nada que mitigue este evento.

Desastres Naturales (N.*)	1	Muy Baja(1)	La última década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, derrumbes u otro tipo de desastre natural, que afecte la infraestructura y funcionamiento de la empresa. Potencialmente existe la probabilidad de sufrir inundaciones por las fuertes lluvias en época de invierno, por cambios climáticos. Pero, la ubicación del cuarto de servidores es apropiada, porque no existen tuberías de agua que pasen cerca del mismo, tampoco existen otro tipo de medios por donde se filtre agua. No se dispone de ningún plan frente a desastres naturales si es que se presentara, de cómo se debería actuar.
Corte del suministro eléctrico (I.6)	1	Baja (2)	Este tipo de amenaza ha sido calificada como poco frecuente, casi nula su frecuencia de ocurrencia, de igual manera la degradación sobre este tipo de activos es mínima. De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos. En épocas de estiaje que afectan a nuestro país, el corte de suministro eléctrico tiene una frecuencia diaria por varias horas, pero en este último estiaje, la empresa eléctrica no se vio afectada. Otros aspectos por los que se daría un corte de energía serían por: placas de pared, usos de extensiones eléctricas, supresores de pico, reguladores

			de voltaje y ups en mal estado, que afecten el correcto suministro eléctrico a los equipos informáticos que estén conectados a estos.
Desastres Industriales: Sobrecarga y fluctuaciones eléctricas (I.*)	0.6	Media (3)	Este tipo de amenaza se presenta muy frecuente en las redes eléctricas, con una degradación en el funcionamiento de los equipos de hardware del 60%. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del Hardware y la información podría perderse. La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico.
Avería de Origen físico o lógico de los equipos (I.5)	1	Media (3)	La falla en el hardware de los equipos, se da por muchas causas como fallas en el disco duro, en la memoria, en la tarjeta de red, fallas en los slots PCI, fallas en el mainboard. Causando un impacto en el equipo del 100% de degradación en el funcionamiento del mismo, dependiendo de la gravedad de la falla.
Errores en la configuración y Errores del administrador (E.4, E.2)	0.5	Bajo (2)	Las equivocaciones que se producen en forma rutinaria son de carácter involuntario. No se tiene establecidos procedimientos y estándares técnicos para la instalación y seguridad de servidores. No se disponen de parámetros de configuración claramente identificados que permitan el riesgo de incurrir en errores por desconocimiento de estos parámetros. Estos errores si se han presentado.
Robo (A.25)	1	Muy Bajo (1)	En la empresa Eléctrica no se han presentado casos de robo de equipos. Por lo que se ha estimado la frecuencia como muy baja. No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización entre el Jefe del Área funcional y Jefe del departamento informático. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

			La empresa cuenta con una política de asignación de bienes a cada uno de los empleados, en la cual se establece la responsabilidad que ellos tienen de los mismos.
Acceso no autorizado y Manipulación de la configuración (A.11, A.4)	0.6	Baja (2)	En la empresa eléctrica se tiene controles sobre la seguridad física en los ambientes donde están los principales componentes de hardware. Pero falta definir políticas, normas y procedimientos, que realmente den soporte a las herramientas tecnológicas implementadas. El cuarto de servidores está con llave pero cualquiera puede solicitar el acceso a esta, sin jutificar su ingreso y sin que nadie se de cuenta que esta persona ingreso y qué actividad realizó. El acceso a los equipos se lo realiza mediante identificador de usuario y clave, sin embargo este sistema de seguridad podría dar lugar a numerosos incidentes como: errores al activar y desactivar cuentas de usuarios con privilegios elevados, algunas plataformas tanto servidores como equipos de red tienen las claves de administrador por defecto, poniendo en peligro la seguridad en la configuración de los equipos (Esto es una amenaza identificada en el informe de la ISO 27001 que se entregó a la Centro Sur). Los puertos de diagnostico algunos se encuentran habilitados, poniendo en riesgo el acceso a la red a través de ellos. No se tienen implementadas las respectivas políticas de acceso internas entre los distintos tipos de usuarios, servidores y servicios existentes dentro de la institución, mediante el uso de VLANs que mejoren la seguridad dentro de la infraestructura de la red (Esto es una amenaza identificada en el informe de la ISO 27001 que se entregó a la Centro Sur).

			Los usuarios todavía comparten sus claves de acceso a los recursos de red y aplicaciones. Los usuarios manejan muchas claves de acceso, para los diferentes recursos de red en los que se tienen modulos de seguridad, haciendo que se vuelva complejo el recordar tantas contraseñas. Esto obliga a que muchas contraseñas no cumplan con los requerimientos de seguridad, por lo difícil que se vuelve recordar tantas contraseñas. Los usuarios de las estaciones de trabajo desconocen que deben dejar bloqueados sus equipos cuando dejen sus puestos de trabajo desatendidos.
Caída del sistema por agotamiento de recursos informáticos (E.24)	0.9	Media (3)	Esta amenaza implica que los sistemas estén expuestos a la saturación de los discos duros, la falta de parches, código malicioso oculto (troyanos), etc. Esto provocará un mal funcionamiento de los sistemas y fallos de disponibilidad. La empresa eléctrica, no tiene dentro de sus políticas realizar un monitoreo periódico de los recursos de hardware informáticos de los diferentes Sistemas, para llevar a cabo un mantenimiento apropiado al tamaño y complejidad de los sistemas existentes, de manera que se eviten fallos (Esto es una amenaza identificada en el informe de la ISO 27001 que se entregó a la Centro Sur).
Errores de Mantenimiento y actualización de equipos (E.23)	0.5	Media (3)	Si bien la empresa eléctrica cuenta con un listado de equipos, no dispone de un inventario formal actualizado regularmente de todos los equipos de cómputo críticos de la empresa, requeridos como mínimo para el funcionamiento permanente de cada sistema o servicio. Tampoco se lleva un registro de los mantenimientos/actualizaciones preventivos o correctivos

			realizados a cada uno, y el periodo requerido para realizar estos mantenimientos y el tiempo que cada mantenimiento/actualización tomaría para realizarla. No se tiene como política, ni procedimiento en donde se especifique que para hacer un cambio o actualización se debe hacer un análisis del impacto en el hardware, aplicaciones y otros recursos que dependen del recurso al cual se le va aplicar la actualización o mantenimiento, poniendo en riesgo el funcionamiento del equipo. No se realiza un escaneo regular de puertos de las diferentes plataformas de red para revisar que no existen puertos abiertos que comprometen la seguridad de la red y se puedan detectar así las vulnerabilidades. (Esto es una amenaza identificada en el informe de la ISO 27001 que se entregó a la Centro Sur). Infraestructura física de Red. La institución no cuenta con diagramas actualizados de red. También se pudo detectar que no se lleva un control respecto a los puertos de los switches mediante un etiquetamiento adecuado al cableado. Otro aspecto a resaltar es que la mayoría de los puntos de red están activos, es decir no se lleva un control adecuado en relación a que su activación debe ser estrictamente cuando se necesiten ser usados por un usuario interno autorizado. (Esto es una amenaza identificada en el informe de la ISO 27001 que se entregó a la Centro Sur).
Ataque destructivo (A.26)	1	Muy Baja (1)	La empresa eléctrica se encuentra en una zona donde el índice de vandalismo es bajo. La empresa cuenta con vigilancia las 24 horas del día.

Uso no previsto (A.7)	1	Baja (2)	Este tipo de amenaza no ha sido identificada como posible de ocurrencia, debido a que las plataformas que dispone la empresa tienen las funcionalidades claras y definidas; para las cuales fueron adquiridas y configuradas, aun así, se estimó una frecuencia de esta amenaza como baja.
Condiciones inadecuadas de temperatura y humedad (I.7)	0.3	Baja (2)	Los equipos y las aplicaciones importantes se encuentran habitualmente en áreas seguras y en condiciones adecuadas. Cuentan con sistemas de aire acondicionado y control de temperatura en el centro de datos. Pero este sistema de climatización no es monitoreado por ningún sistema de alarmas.

AMENAZAS PARA EL TIPO DE ACTIVO SOFTWARE

AMENAZAS PARA EL TIPO DE ACTIVO SOFTWARE

Amenazas	Porcentaje de degradación	Frecuencia de la amenaza	Justificación
Errores de los usuarios (E.1)	0.5	Media (3)	Esta amenaza se presenta con una frecuencia media, que consiste en ingreso incorrecto de datos, mal manejo o desconocimiento de las aplicaciones, de las opciones de las aplicaciones, desconocimiento del manejo de las aplicaciones o herramientas informáticas. Los usuarios deben autocapacitarse en el manejo de las herramientas informáticas. Algunas veces la empresa proporciona cursos de capacitación a todos los empleados para ciertas aplicaciones o herramientas informáticas, pero puede que el personal que ingrese luego de la capacitación no la reciba, porque no existe una política que así lo estipule.
Errores del Administrador (E.2)	0.75	Media(3)	Son errores que se producen involuntariamente, por parte del personal responsable de la instalación y operación. En general, los administradores están suficientemente capacitados para ejecutar correctamente su trabajo, pero hay ciertas ocasiones en las que por realizar una actualización o cambio se han producido errores que han afectado el funcionamiento de ciertas aplicaciones o servicios. Por la falta de procedimientos documentados donde se tengan identificados todos los parámetros de configuración que se pueden pasar por alto. Debido a los privilegios de este tipo de usuarios, el impacto es notable.

Errores de configuración (E.4)	0.75	Media (3)	A pesar que la responsabilidad en la configuraciones de los diferentes sistemas informáticos esté definida, de manera que si se produce algún evento indeseado, se sabe a quién recurrir, existe falta de criterios y procesos documentados acerca de los parámetros y pasos que hay que seguir, lo que hace que se dependa indispensablemente de la persona a cargo. Poniendo en riesgo la continuidad de las operaciones de los diferentes sistemas, servicios y procesos informáticos.
Difusión de software dañino (E.8)	0.8	Alta (4)	Esta es una amenaza que puede degradar el rendimiento de los sistemas y aplicaciones informáticas altamente y su frecuencia es alta, debido a que todas las empresas se encuentran expuestas a virus, troyanos, gusanos, etc. mediante el intercambio de información a través de la intranet, internet, correo electrónico, memorias flash, discos externos, etc. Lo que hace que esta amenaza tenga una frecuencia alta. La ventaja que cuenta la empresa eléctrica es que sus sistemas críticos se encuentran implementados con software que no es vulnerable a este tipo de software dañino, haciendo que la amenaza para ellos al realizar el respectivo análisis de riesgo se disminuya a una frecuencia baja.
Errores de secuencia (E.10)	0.9	Media (3)	Este tipo de amenazas se puede dar como consecuencia de un error en la configuración tanto de los equipos, como en las aplicaciones de red.
Escapes de Información (E.14)	1	Muy Baja (1)	Este tipo de amenaza es una consecuencia que se puede dar por otro tipo de amenazas como: accesos no autorizados, errores de configuración, vulnerabilidad en los programas de software, manipulación de la configuración.
Vulnerabilidad en los programas de software	1	Media (3)	Los entrevistados con un perfil más técnico han señalado que un buen desarrollo del código que genere una aplicación de calidad,

(E.20)			sin defectos, es uno de los principales factores que garantizan la seguridad de una plataforma. Sin embargo, este tipo de amenazas se presenta inevitablemente cuando un nuevo módulo de software se pone en producción, trayendo como consecuencia no sólo el mal funcionamiento del sistema sino que se podría incurrir en el ingreso incorrecto de datos. También se analizó la posibilidad de que a través del acceso al código fuente de las aplicaciones que ellos desarrollan, se puede explotar alguna vulnerabilidad que permita el acceso no autorizado a las bases de datos y recursos de red.
Errores de mantenimiento/actualización de programas de software (E.21)	0.4	Media (10)	A pesar de todas las medidas que se tomen, los programas suelen tener fallos que se van descubriendo al utilizarlos, o bien se producen al modificarlos para mejorar sus funcionalidades o su rendimiento. Las plataformas cuentan con numerosos programas y funcionalidades que deben ser adecuadamente mantenidos para evitar costosos incidentes. Otro aspecto a resaltar, es la incompatibilidad que puede producirse con otras aplicaciones, recursos o servicios de red, que afecten a los sistemas informáticos. Por ejemplo versiones de sistemas operativos, bases de datos, exploradores web, controladores de impresoras, etc.
Manipulación de la configuración (A.4)	0.74	Media (3)	Este tipo de amenaza se da como resultado de la realización de otras amenazas como: Errores de Administrador, errores de configuración, difusión de virus, vulnerabilidad en los programas de software, Errores de mantenimiento de aplicaciones.
Suplantación de la identidad de usuario (A.5)	0.74	Baja (2)	Esta amenaza no se ha presentado dentro del historial de incidentes de la emprea, por eso se la califica con una frecuencia baja pero, este tipo de amenaza se da como resultado de la

			realización de otras amenazas como: Errores de Administrador, errores de configuración, vulnerabilidad en los programas de software, Errores de mantenimiento de aplicaciones, acceso no autorizado, abuso de privilegios de acceso. También se puede dar como consecuencia que algún usuario haya dejado su sesión activa, dentro de alguno de los sistemas informáticos, permitiendo que cualquier persona no autorizada tenga acceso a través de su perfil de usuario. No existe una política donde se especifique de que manera a una persona se le asignan los privilegios de acceso a los diferentes aplicaciones informáticas, y si se olvida la clave, cómo volverle a asignar una nueva, sin que la asignación de esta nueva clave sea a la persona correcta y no sufrir una suplantación de identidad. En la organización todavía es neceario trabajar en concientizar que no se presten las claves de usuario, que es algo que todavía se da en algunas áreas de las empresas.
Uso no previsto (A.7)	0.4	Bajo (1)	Las aplicaciones instaladas en los equipos de la empresa están claramente definidas su funcionalidad y las políticas de utilización; aun así, el gran número de usuarios hace factible que ocurran amenazas de este tipo, como por ejemplo que se instale software que genere conflictos con los sistemas informáticos críticos, con los servicios de correo electrónico u otro servicio donde se vea afectada la continuidad del negocio. Debido a las restricciones existentes, se detectará la irregularidad enseguida, y el impacto, en caso de ocurrir, será bajo.
Manipulación de Programas (A.22)	0.5	Muy Bajo (0.1)	Este es un tipo de ataque que no se ha detectado todavía. En el caso de que ocurriera, podría generar daños de importancia dependiendo de cuál fuera la información que se llegara a

			manejar fraudulentamente y cuál fuera el uso que se le diera.

AMENAZAS PARA EL TIPO DE ACTIVO DATOS

AMENAZAS PARA EL TIPO DE ACTIVO DATOS

Amenazas	Porcentaje de degradación	Frecuencia de la amenaza	Justificación
Errores de los usuarios (E.1)	0.1	Media (3)	Equivocaciones que se producen en forma rutinaria de carácter involuntario. Este tipo de amenaza pondría en riesgo la consistencia de la información registrada en las bases de datos de los sistemas de información. Esta amenaza sería la consecuencia en fallos que se producen en el software de las aplicaciones.
Alteración de la Información (E.15)	0.9	Media (3)	Esta amenaza se produce como consecuencia de otras amenazas: Errores de configuración, accesos no autorizados, abuso de los privilegios de acceso, vulnerabilidad en los programas y aplicaciones, errores de usuarios. El entorno en el que se usan ciertas aplicaciones podría aumentar la frecuencia de ocurrencia de esta amenaza, como son las aplicaciones que se encuentran en el portal Web. Hay otros entornos como la intranet que aunque no produzca con frecuencia este evento, el impacto de este tipo puede ser importante
Introducción de Información Incorrecta (E.16)	0.6	Media (3)	Esta amenaza se refiere a que muchos usuarios pueden introducir información en las diferentes bases de datos a través de los sistemas informáticos o aplicaciones, lo que pone en riesgo la integridad de los datos, la frecuencia de que esta amenaza se materialice es considerable y el impacto puede ser importante. Generalmente se puede dar porque los procedimientos de validación de los sistemas no estén bien implementados, los mismos que garanticen el ingreso de datos correctos y válidos. Otra forma de ingresar información a las bases de datos es por procesos batch que se ejecuten en horas de baja carga transaccional, pero que por algún error en la definición del proceso batch se haga un ingreso incorrecto.

Degradación de Información (E.17)	0.7	Baja (1)	Esta amenaza se presenta como consecuencia de la materialización de otras amenazas como es la alteración de la información y la introducción incorrecta de la misma, trayendo como consecuencia que la información se degrade y no se pueda obtener información veraz en el momento requerido, esto es un punto básico que hay que cumplir. Puesto que muchos usuarios pueden introducir información en las diferentes plataformas, la frecuencia de que esta amenaza se materialice es considerable y el impacto puede ser importante
Destrucción de Información (E.18)	0.76	Baja (1)	Esta amenaza se presenta como consecuencia de la materialización de otras amenazas como es el caso de fallos de origen físico y lógico en los equipos de hardware, difusión de software dañino, errores de mantenimiento y actualización de software, errores de actualización y mantenimiento de equipos, manipulación de la configuración.

AMENAZAS PARA EL TIPO DE ACTIVO SERVICIOS

Amenazas	Porcentaje de degradación	Frecuencia de la amenaza	Justificación
Repudio (A.13)	0.4	Baja (1)	Esta amenaza por ahora no se ha presentado dentro de los incidentes detectados en la empresa y no supone un problema mayor, porque la mayoría de transacciones se encuentran respaldadas por documentos por escrito que resguarden las comunicaciones realizadas a través de las plataformas de TI en los servicios que se dan y que son importantes.
Denegación del Servicio (A.24)	1	Media (3)	Esta amenaza se puede presentar como consecuencia de otra amenaza como es la carencia de recursos suficientes para dar soporte al servicio que se provee. Una de las características de las plataformas es el gran número de usuarios que las utilizan, en muchos casos, de manera concurrente, por lo que es importante tener en cuenta esta amenaza, si la aplicación no esté disponible desmotiva a los usuarios para utilizarla.
Indisponibilidad del Personal (E.28, A.28)	0.5	Baja (1)	No es un hecho habitual, pero, al no haber mucho personal a cargo de las plataformas, si falta alguien, puede existir un problema de disponibilidad, quizá solo de alguna función.

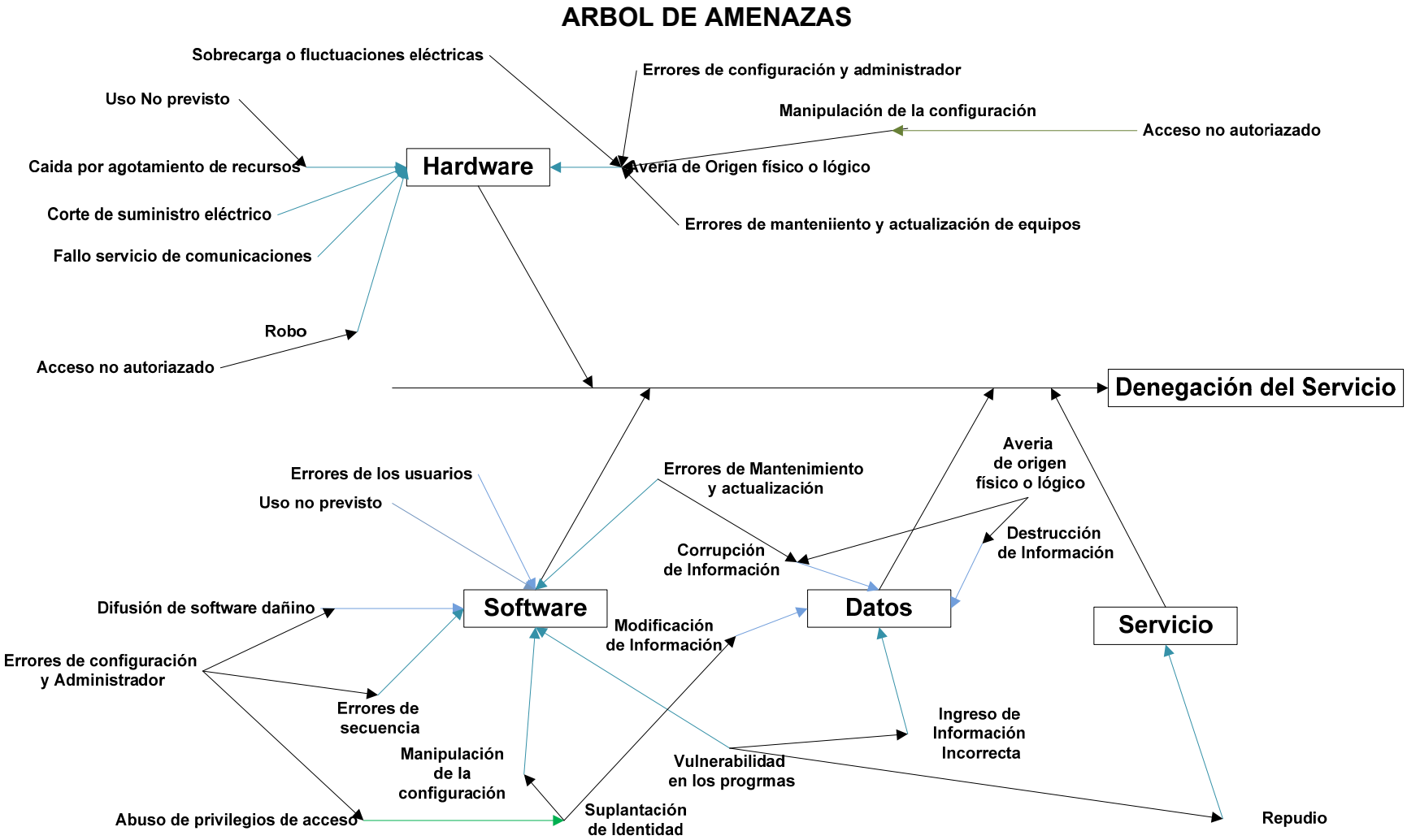


Figura 2.1 Arbol de amenazas.

2.1.3. IDENTIFICACIÓN DE SALVAGUARDAS

2.1.3.1. IDENTIFICACIÓN Y VALORACION DE SALVAGUARDAS EXISTENTES

OBJETIVOS DE LA ACTIVIDAD

- Identificar las salvaguardas, de cualquier tipo, que se han previsto y desplegado a fecha de realización del estudio
- Determinar la eficacia de las salvaguardas desplegadas

PRODUCTOS DE ENTRADA

- Inventario de procedimientos operativos
- Inventario de productos y/o desarrollos hardware o software de soporte a la seguridad de los sistemas
- Plan de formación
- Definición de los puestos laborales
- Contratos
- Acuerdos de externalización de servicios
- Inventario de salvaguardas (Catálogo de Elementos)

RESULTADOS

Para cada salvaguarda se registró la siguiente información:

- descripción de la salvaguarda y su estado de implantación
- descripción de las amenazas a las que pretende hacer frente
- valora la efectividad de las salvaguardas identificadas

Informe de Salvaguardas Existentes

FECHA:

VERSION:

DESCRIPCION:

PROPIETARIO:

ORGANIZACIÓN:

2.1.3.2. VALORACIÓN DE SALVAGUARDAS EXISTENTES

Los controles seleccionados de la Norma ISO 27001, son los que se adjunta en la siguiente lista:

Eficacia	Categoría	Descripción
0	Inexistente	Procedimiento: No se ejecuta. Elemento: No existe. Documento: No existe.
1	Inicial / ad hoc	Procedimiento: La ejecución es de manera esporádica, o sólo lo hacen algunas personas. Elemento: Existe, pero apenas se utiliza. Documento: Se está preparando su desarrollo
2	Reproducible, pero intuitivo	Procedimiento: Informal, se ejecuta pero no está documentado. Elemento: Existe, pero está en proceso de ajuste. Documento: En proceso de desarrollo.
3	Proceso definido	Procedimiento: Formal, se ejecuta y está documentado. Elemento: Existe y funciona correctamente. Documento: Existe
4	Gestionado y medible	Procedimiento: Se obtienen indicadores. Elemento: Se obtienen indicadores. Documento: Se obtienen indicadores
5	Optimizado	Procedimiento: Se revisa el mismo y los indicadores, se proponen mejoras y se aplican. Elemento: Se revisa el mismo y los indicadores, se proponen mejoras y se aplican. Documento: Se revisa el mismo y los indicadores, se proponen mejoras y se aplican.

Tabla 2.11. Niveles de Madurez de las Salvaguardas [7]

SALVAGUARDAS IDENTIFICADAS PARA EL TIPO DE ACTIVO HARDWARE

Controles	Descripción del Control/Salvaguarda	Amenazas Mitigadas	Respuestas
7. 1.1 Inventario de Activos	**1. ¿Hay políticas y procedimientos relativos al uso y protección del hardware de la organización?**	Robo	2
	a) Cuantificación del hardware		
	b) Descripción del hardware (características básicas)		
	c) Distribución del hardware (ubicación física mediante planos por capas por tipo de hardware, prioridad)		
	d) Áreas de informática: departamentos usuarios y áreas locales y remotas.		
	e) Registro del hardware instalado, dado de baja, en proceso de adquisición		
	f) Uso del hardware: desarrollo, operación, mantenimiento, monitoreo y toma de decisiones		
	g) Funciones responsables del control del hardware		
7..1.2 Propiedad de los activos	Los activos tienen asignados personas responsables del uso de los mismos, que se les conoce como propietarios de los activos.		3

7.1.3 Uso aceptable de los activos			
9.1.3 Asegurar las oficinas, habitaciones y medios	El acceso a las instalaciones de la empresa eléctrica, se encuentran vigilados las 24 horas, por guardias de seguridad.		3
	Para personas visitantes, la recepcionista entregará el credencial de visitante para ingresar a las diferentes áreas de la empresa, y registra la entrada con el documento de identificación de la persona que ingresa, y al momento de salir se le devuelve dicho documento, asegurando que cada persona que ingresa después de cierto período debe de abandonar las instalaciones.		3
9.2.1 Ubicación y Protección del Equipo, 9.2.7 Retiro de propied	**Mencione si existen políticas relacionadas con el ingreso y salida del hardware que aseguren al menos lo siguiente**		
	a. Revisada (contenido, cantidad, destino)		3
	b.Justificada (compra, pruebas, reemplazo, devolución, dado de baja,otro)		3
	c. Aprobada por el responsable de informática que va a recibirlo		3
	d. Registrada (responsables, hora, motivo, etc.)		3

ad	e. Devuelta (comparar con la fecha estimada de salida)		2
	f. Devuelta en las mismas condiciones de entrada		3
	g. Devolución autorizada por medio de un responsable de informática		3
	Se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno.		2
	Se realizan chequeos inesperados de los equipos para detectar retiro de propiedad no autorizada. Estos chequeos deben realizarse bajo la autorización de requerimientos legales y politicas definidas en la empresa.		2
	Procedimientos y controles de seguridad para la evaluación, selección y adquisición de hardware.	Agotamiento de recursos	1
11.5.1 Procedimientos para un registro seguro	**Al adquirir el hardware se debe considerar:**	Manipulación de la Configuración	
	a) Acceso al hardware (llaves de seguridad, por ejemplo).		3

	b) uso del hardware (facilidades de monitorear la operación).		3
	c) bitácoras de uso del hardware quién, cuándo, para qué, entre otros puntos)		3
10.1.2 Gestion del Cambio (Actualización del Hardware)	**Políticas orientadas a confirmar que el hardware actualizado cubra los siguientes puntos**	Fallos o Averias de Origen fisico o logico (I.5)	
	a) Autorización de la actualización del hardware por medio de la justificación.		2
	b) Impacto de la implantación del hardware en el medio de informática: aplicaciones, software y costos		2
	c) Procedimientos de emergencia y respaldo ante una falla en la aplicación del cambio		3
	d) Registro de los cambios realizados (fecha, hora, respondable, motivo, autorización, tareas realizadas, errores o fallas detectadas durante el cambio)		2

10.1.2 Gestion del Cambio (Reemplazo del Hardware)	f) Autorización del nuevo hardware por medio de la justificación del reemplazo (errores incompatibilidades de drivers)		2
	g) Impacto del reemplazo del hardware en el medio de informática: aplicaciones, software y costos		2
9.2.2 Servicios Públicos de Soporte	Se ha considerado necesario un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada.		2
	Se cuenta con un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado		2
	El equipo UPS y los generados son revisados regularmente para asegurar que tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante		2
	Se debiera proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal		3

	El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de voz. Los servicios de voz debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia		3
	El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de internet. Los servicios de internet debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia		3
12.6.1 Control de las vulnerabilidades técnicas	¿Hay procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de desastres o contingencias?		2
9.2.4 Mantenimiento hardware	Los equipos de informática reciben el respectivo proceso de mantenimiento en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor	Errores de mantenimiento / actualización de equipos (hardware)	2
	Sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio de mantenimiento a los equipos		3

	Se dispone de registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo		2
	Tener presente el cumplir con todos los requerimientos impuestos por las pólizas de seguros.		3
9.1 .1 Permimetro de Seguridad Fisica	Indique si se cuenta con controles y procedimientos para la clasificación y justificación del personal con acceso a los centros de cómputo del negocio y a las oficinas donde se encuentra papelería o accesorios relacionados con informática.	Acceso no autorizado	1
	Restringir el acceso a los centros de cómputo sólo al personal autorizado.		3
9.1.2 Controles de Ingreso Fisico	Definición y difusión de las horas de acceso al centro de cómputo		1
	Uso y control de bitácoras de acceso a los centros de cómputo		
	Definir la aceptación de la entrada a visitantes		
	Manejo de bitácoras especiales para los visitantes a los centros de cómputo		
9.2.1 Úbicación y Protecci on del	¿La ubicación física del equipo de cómputo en el edificio es la más adecuada pensando en los diversos desastres o contingencias que se pueden presentar (manifestaciones, huelgas, inundaciones, incendios u otros)?	Desastres Naturales (N.*)	2

Equipo	Sistema para Controlar y Monitorear la temperatura y humedad del Centro de Datos		2
	Sensores de humo y un sistema de alarma de incendio en el centro de datos	Amenaza Fuego	2
	Cuentan con extintores tipo C [1]cercanos al data center y el personal ha recibido la capacitación respectiva para su manejo		2
	Cuentan con racks y archivadores de material ignifugo para proteger los equipos y documentacion critica		2
	Existen políticas establecidas que prohiban fumar cerca de los equipos informáticos		3
	La empresa cuenta, con un programa de creación de brigadas, las que están encargadas de todo lo referente a seguridad, primeros auxilios, control de evacuación, ayuda en caso de incendio, etc		3
	Mantenimiento periódico a las instalaciones eléctricas		2
	Dispone de sensores de detección de inundaciones a niveles de ras del suelo	Amenaza Inundaciones	1
	Se tiene medidas preventivas de mantenimiento del edificio, revisión de conductos de agua y drenaje		1

[1] El extintor tipo C hace referencia a la clase de fuego tipo C (Inflamación de equipos energizados eléctricamente), el agente extintor (Dióxido de Carbono (CO_2) o Polvo químico seco ABC-BC) para mayor información revisar documento http://www.chilearq.com/bloques/bloques.php?f=2009-02-04-7209PCI1744.pdf.

	En los PCs de Usuarios	Cortes de Suministro de Energía	
	La mayoría de computadores y equipos clientes disponen de enchufes de pared para las conexiones, limitando el uso de extensiones eléctricas. Las extensiones eléctricas están fuera de las zonas de paso, siempre que sea posible.		3
	Se comprueba periódicamente cada seis meses, el estado de las extensiones eléctricas, placas de pared y resto de equipos eléctricos a los que se encuentran conectados los equipos informáticos críticos, para evitar cortes inesperados de energía eléctrica por falla de alguno de ellos		2
	Cada computadora tiene su propio UPS que las protege durante 5 minutos aproximadamente para poder resguardar los datos y apagar el computador durante una falla de energía.		3
	En el Centro de Datos		
	UPS: (Uninterruptible Power Supply) en el centro de cómputos hay un UPS que pueden mantener los servidores funcionando por aproximadamente 1 hora.		3
	Se debiera proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal		3
	La Red de Servidores en la Centrosur cuenta con una red eléctrica estabilizada	Desastres Industriales:	3

	Cada computadora se encuentra conectados a dispositivos que los protegen de las sobrecargas eléctricas como: supresores de picos, reguladores de voltaje, UPS	Sobrecarga y fluctuaciones eléctricas (I.*)	3
	Tanto las tomas de corrientes de pared como las extensiones eléctricas disponen de toma a tierra.		3
9.2.3 Seguridad del Cableado	Los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia	Ataque destructivo	3
	Se utiliza marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados		3
	La instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación		2
	El uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada		2
	La iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves		2
	Acceso controlado para empalmar los paneles y los cuartos de cableado		3
10.1.1 Procedimientos	Se disponen de procedimientos documentados de los sistemas criticos de la empresa como:	Errores de configuración, Errores del	2
	Bases de datos		

de operación documentados	Servidor de aplicaciones	administrador, errores de mantenimiento /actualización (hardware y software)	
	Servidor de Correo		
	Servidor Web		
	Sacar copias de seguridad y respaldo de datos e informacion		
	Se tienen documentados las interdependencias con otros sistemas para al darse un error identificar que procesos y sistemas del core del negocio se verán afectados		1
	Los tiempos que les tomaría realizar cada uno de los procedimientos operacionales requeridos para levantar los sistemas y sus respectivos componentes		2
	Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.		2
	Se tiene documentado los contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas		1
	Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema		2

10.1.3 Segregación de los deberes	Se tienen debidamente identificado y establecidos los responsables y las funciones a desarrollar para cada uno de los sistemas criticos de la empresa		3

SALVAGUARDAS PARA LA PROTECCION DE LA SEGURIDAD DE LAS APLICACIONES

Controles	Descripción del Control/Salvaguarda	Amenazas Mitigadas	Respuestas
	¿Hay políticas y procedimientos relativos al uso y protección del software de la organización?	Errores de mantenimiento / actualización de programas (software)	
7. 1.1 Inventario de Activos	a) los listados y cuantificación del software (original y copias)		2
	b) Descripción (por original)		
	c) Distribución (en qué equipos o dispositivos de almacenamiento secundarios se encuentra, en qué lugar físico se localizan: áreas del negocio, bancos, etc.)		
	d) Registro del software instalado, dado de baja, en proceso de adquisición, etc.)		
	e) Uso del software (tipo de uso, responsables de su uso, entre otros puntos)		
10.1.2 Gestion del Cambio (Actualización del software)	**Procedimientos y controles de seguridad para la evaluación, selección y adquisición de software.**		3
	Políticas orientadas a confirmar que el software actualizado cubra los siguientes puntos		2
	a. Autorización del software por medio de la justificación de la actualización (es decir que los usuarios autorizados acepten el cambio antes de implementarlo)		
	b. Impacto de la implantación del software en el medio de informática: aplicaciones, hardware y costos		

	c. Implicaciones de control en la implantación y uso del software actualizado como errores, agujeros de seguridad, incompatibilidades		
10.1.2 Gestion del Cambio (Reemplazo del Software)	Autorización del software por medio de la justificación del reemplazo		2
	Impacto del reemplazo del software en el medio de informática: aplicaciones, software y costos		2
	Implicaciones de control en la implantación y uso del software nuevo		2
	Asegurar que el conjunto de documentacion del sistema este actualizado al completar cada cambio y que la documentación antigua se archive o se elimine		2
	Mantener un control de la versión para todas las actualizaciones del software		3
	Mantener un rastro de auditoria de todas las solicitudes de cambio		2
	Asegurar que la documentación de operación y procedimientos de usuario sean cambiados según sea necesario para seguir siendo apropiados		1
	Las actualizaciones automáticas no deben estar permitidas en los sistemas críticos de la empresa ya que algunas actualizaciones pueden causar que fallen las aplicaciones críticas (ver 12.6)		3
	La implementación de los cambios se realizann en el momento adecuado y no interrumpen los procesos comerciales involucrados		3
12.4.1 Control del software operacional	Las actualizaciones o reemplazos son realizadas solo por administradores capacitados con la respectiva autorización		3
	Disponen del software operacional critico la información requerida como parámetros, procedimientos, detalles de configuración y software de soporte		2

	Disponen de estratégias de regreso a la situación original "roll back" antes de implementar los cambios		3
	Disponen de un registro de auditoria de las actualizaciones a las bibliotecas del programa operacional		2
	Se mantienen las versiones previas del software de aplicación como una medida de contingencia		3
12.4.3 Control de acceso al codigo fuente del programa	Mantienen politicas de control de acceso a las bibliotecas de codigo fuente de los sistemas operacionales evitando un acceso irrestricto.		3
	Mantienen separado los ejecutables de las bibliotecas de codigos fuentes de los sistemas operacionales		3
Ingreso del software	**Mencione si existen políticas relacionadas con el ingreso y salida del software que aseguren al menos lo siguiente**	Vulnerabilidad en los programas de software (E.20	2
	a) Revisada (contenido, cantidad, destino)		
	b) Justificada (compra, pruebas, reemplazo, devolución, dado de baja,otro)		
	c)Aprobada por el responsable de informática que va a recibirlo		
	d) Registrada (responsables, hora, motivo, etc.)		
	e) Devuelta (comparar con la fecha estimada de salida)		
	f) Devuelta en las mismas condiciones de entrada		
	e) Devolución autorizada por medio de un responsable de informática		
	g) El personal esté comprometido formalmente a no hacer un mal uso del mismo (copiarlo, dañarlo o modificarlo)		

10.3.2 Aceptación del Sistema	**¿Existen procedimientos que verifiquen que la construcción (programación), prueba e implantación de los controles y procedimientos de seguridad sean formalmente aprobados antes de que se utilice el sistema?**		2
	¿Participan funciones de control o evaluación de sistemas, como auditores o consultores, en la aprobación de los controles de seguridad de los sistemas antes de que sean formalmente aprobados por los usuarios?		2
	a) Si es así, ¿en qué etapas del desarrollo participan?		
	b) ¿Se involucran en todos los proyectos de desarrollo?		
	En cuanto a las aplicaciones (sistemas de información) que se desarrollan en la empresa, ¿se tienen los controles y procedimientos necesarios para garantizar la seguridad mínima requerida	Errores de los usuarios (E.1), Acceso no autorizado (A.11)	2
12.2.1 Validación de la unput data	Procedimientos de llenado de documentos fuente		2
	Procedimientos de uso de la computadora		2
	a) Encendido e inicialización del equipo		
	b) Reinicialización del equipo en caso de fallas		
	c) Manejo de bitácoras de uso de la computadora		
	d) Monitoreo de uso de la computadora		

11.1.1 Control de acceso	Niveles de acceso (perfil de usuarios) a los módulos de: Captura, Actualización, Consulta, Generación de reportes, Respaldos, Otros		3
	Procedimientos de uso de los módulos de: Captura, Actualización, Consulta, Generación de reportes, Respaldos, Otros		3
12.2.4 Validación de la output data	**8. Mencione si los controles aseguran que el sistema contemple los procedimientos necesarios para que la información manejada en el mismo sea total, exacta, autorizada, mantenida y actualizada**	Introducción de Información Incorrecta (E.16)	3
	8.1 ¿Existen procedimientos para comprobar que los totales de los reportes de validación del usuario concuerden con los totales de validación del sistema computarizado?		
12.2.3 Validación de la input data	8.2 ¿Los documentos fuente por capturar llevan preimpresos sus números consecutivos o se los asigna el usuario? Si ocurre lo último, ¿hay alguno de los controles mencionados a continuación dentro del sistema que valide la no repetición o exclusión de algún número consecutivo?		4
12.2.2 Control del procesamiento interno	Control de todos los movimientos o transacciones rechazados por el sistema que ayuden a comprobar que los datos erróneos para el sistema sean registrados, corregidos, alimentados correctamente y actualizados).	Errores de Usuario (E.1)	2
	Entendimiento y buen uso de los mensajes del sistema, como manejo de errores.		2
	Uso de bitácoras por parte de usuarios y personal de informática como pistas para auditoria.		2
	Existen procedimientos que permitan realizar chequeos de validación en las aplicaciones para detectar corrupción de la información a través de errores de procesamiento o actos deliberados		1

10.1.4 Separación de los medios de desarrollo, prueba, y operación	Se tienen separados los ambientes de desarrollo de software del ambiente operacional	Manipulación de programas, Alteración de la información,Introducción de información incorrecta, Abuso de privilegios de acceso, Modificación de la información, Introducción de falsa información	3
	Los compiladores, editores, y otras herramientas de desarrollo o utilidades del sistema no debieran tener acceso a los procesos operacionales cuando no se requieren		3
	Deben estar establecidos los responsables que asignan los permisos de acceso al personal de desarrollo, al ambiente operacional		3
10.3.1 Gestión de la capacidad	Existen procedimientos de monitoreo del funcionamiento de los sistemas criticos de la empresa para asegurar su funcionamiento eficiente.	Caída del sistema por agotamiento de recursos, Fallos o Averias de Origen fisico o logico, Indisponibilidad del personal	2
	Se tienen identificados y establecidos los parámetros o criterios requeridos para determinar el comportamiento eficiente del sistema		2
	Disponen de herramientas para el monitoreo y notificación de posibles problemas en los recursos claves de los sistemas		2
	Las proyecciones futuras de crecimiento en las capacidades de los recursos de los sistemas se obtienen basados en las tendencias actuales del monitoreo de los recursos claves de los sistemas		2
10.3.2 Aceptación del Sistema	Se tienen procedimientos y politicas establecidas para la aceptación del traspaso de un nuevo sistema del ambiente de desarrollo y pruebas al ambiente operacional (Esto incluye documentación)	Vulnerabilidades de los programas (software)	2
	Se tiene asignado al personal responsable de definir y verificar los criterios de aceptación para el traspaso del ambiente de desarrollo al ambiente operacional		2

	¿Cómo se aseguran que al estar el sistema en operación se cumplan formal y oportunamente los procedimientos de seguridad contemplados en el desarrollo del mismo? (Con auditoria de sistemas interno,Con revisiones de consultores externos, con revisiones del personal de informática)		2
	¿Cómo se aseguran de que los manuales de usuario, técnicos y de operación cumplan con los estándares de la metodología de CVDS y de que sean completos?		2
	a) ¿Cómo se aseguran de que el personal que va a utilizar estos manuales se encuentre capacitado en el uso de los mismos?		
10.4.1 Controles contra código malicioso	Se tiene establecido una politica formal prohibiendo el uso de software no autorizado	Difusión de software dañino	3
	Se encuentra Instalado y actualizado un software para la detección, eliminación y reparación de codigos maliciosos para la revisión de computadores, medios de almacenamiento, archivos adjuntos de correo electrónico y de accesos a los recursos de red compartidos, paginas web		3
	Disponen de personal encargado de revisar información relacionada con codigo malicioso nuevo y los respectivos procedimientos para mitigar o reparar si se introdujera este codigo en los sistemas criticos de la empresa. Para ello se debe contar con fuentes de información confiables.		1
10.7.4 Seguridad de la documentación del sistema	La documentación del sistema se encuentra almacenada de una manera segura, en un lugar donde no tengan acceso personal no autorizado	Vulnerabilidades de los programas (software), Manipulación de la configuración, incendio o fuego	2
	Se utiliza material ignifugo para almacenar este tipo de documentación		1
	Se dispone de una lista de acceso que ayude a restringir al minimo el acceso a la documentación del sistema, la misma que será adminitrada por el propietario de la aplicación		1

10.9.2 Trasacciones en linea	Los protocolos utilizados para comunicarse entre todas las partes involucradas son seguros	Alteración de la Información (E.15), Degradación de Información (E.17)	2
	Las credenciales de usuario de todas las partes sean válidas y verificadas		2
	El lugar donde se almacenan los detalles de la transacción en linea se encuentran dentro de la plataforma de almacenamiento en la intranet y no dentro de la zona desmilitarizada		3
	Se utilizan firmas electrónicas por cada una de las partes involucradas en la transacción		1
	Se tienen controles de seguridad implementados que garanticen que las transacciones en linea realicen trasmisiones completas, que no se de un ruteo equivocado, alteración no autorizada de los mensajes trasmitidos (paquetes de datos),duplicación o repetición no autorizada del mensaje.		2
10.9.3 Información Públicamente disponible	El acceso al sistema de publicación (Servidor Web) permite el acceso involuntario a las redes con las cuales se conecta el sistema	Acceso no autorizado (A.11), Suplantación de la identidad de usuario (A.5), Alteración de la Información (E.15), Degradación de Información (E.17)	2
10.10.1 Registro de auditoria	Disponen de registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso	Acceso no autorizado	2

	Registros de Accesos Autorizados (Ïds de usuarios, fecha y hora, tipo de eventos, archivos a los cuales se tuvo acceso, programas/utilitarios utilizados)		2
	Registros de todas las operaciones privilegiadas(Uso de cuentas administrador/supervisor, inicio/apagado del sistema, dispositivos I/O para adjuntasy eliminar lo adjuntado		2
	Registros de Intentos de acceso no autorizado (acciones del usuario fallidas o rechazadas que involucran la data y otros recursos de los sistemas claves)		1
	Registros de Violaciones a la politica de acceso y notificaciones para los gateways y firewalls de la red		1
	Registros de Alerta de los sistemas de detección de intrusiones		1
	Disponen de procedimietos para el monitoreo del uso de los medios de procesamiento de la información, los mismos que deben ser revisados periódicamente para tomar decisiones en base a los resultados obtenidos		2
11.1.1 Politica de control de acceso	Existen procedimientos que gestionen los requerimientos para la autorización formal de las solicitudes de acceso		2
	Existen procedimientos que ayuden en la revision periódica de los controles de acceso		2
	Las reglas de acceso tienen la premisa todo esta prohibido a no ser lo que este expresamente permitido		2
	Existen procedimientos establecidos para la revocación de los derechos de acceso		2

11.2.1 Registro de Usuario	Utilizan IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones dentro de los sistemas informaticos y recursos de red críticos		3
	Proporciona a los usuarios un enunciado escrito de sus derechos de acceso		3
	Se elimina o bloquea inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto o trabajo o han dejado la organización		3
	Se tiene incluido en los contratos del personal y contratos de servicio cláusulas que especifiquen las sanciones si el personal o los agentes de servicio intentan un acceso no autorizado		3
11.2.3 Gestión de Claves secretas de los usuarios	Cuando se asignan permisos de acceso a los usuarios a los sistemas o recursos de red se les obliga inicialmente a cambiar la clave secreta temporal que se les proporcionó.		3
	Se tienen establecidos procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta de nueva, sustituta o temporal		3
	Las claves secretas son almacenadas en los sistemas de computo de una manera segura		3
	Las claves secretas predeterminadas por el vendedor son cambiadas después de la instalación de los sistemas o software		3

11.3.2 Equipo del usuario desatendido	Se tiene establecido una politica formal de seguridad que los usuarios una vez que han terminado sus actividades deben cerrar las sesiones activas. (No solo apagar la pantalla de la PC o terminal)		1
	Se dispone de algún mecanismo automático de cierre, que después de unos minutos de inactividad el sistema se bloquee y para volver a activar la sesión se debe ingresar la clave de usuario.		2
11.4.1 Política sobre el uso de los servicios de red	Existe especificamente una política relacionada con el uso de las redes y los servicios de red, la cual indique las redes y los servicios a las cuales se tiene acceso		1
	Se tiene establecido procedimientos de autorización para determinar quién está autorizado a tener acceso a cuáles redes y servicios de red		1

	Los usuarios tienen acceso a los servicios para los cuales hayan sido especificamente autorizados		1
	Se tienen actualizados los diagramas de red que ayuden a tomar decisiones sobre el uso y autorizaciones de las redes y sus servicios		1
	Se tiene establecido los medios utilizados para tener acceso a las redes y los servicios de red (las condiciones para permitir acceso via discado a un proveedor de internet o sistema remoto, acceso mediante wireless).		2
11.4 Protección de puerto de diagnostico y configuración remotos	Existen politicas y procedimentos establecidos para el control de accesos de usuarios remotos		2
	Los puertos de diagnostico y configuracion remotos se encuentran normalmente desactivados y solo se los activa cuando se requiere realizar alguna tarea de mantenimiento en el equipo, mediante un proceso de autorización entre el responsable y el personal de soporte		2

11.4.5 Segregación en redes	Existen dentro de la red de la organización segregación de redes mediante VLANs las cuales se tengan claramente identificados que usuarios pueden compartir recursos y que accesos están autorizados para las diferentes redes y medios. Por ejemplo, sistemas de acceso público, redes internas y activos críticos.		2
	Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, se debiera restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones comerciales ver 11.1		2
	Existen procedimientos establecidos para el monitoreo de controles de seguridad en el routing en las redes para asegurar que las conexiones de las computadoras y los flujos de información no violan la política de control de acceso de las aplicaciones comerciales		2

SALVAGUARDAS PARA LA PROTECCION DE LA SEGURIDAD DE LOS DATOS

Controles	Descripción del Control/Salvaguarda	Amenazas Mitigadas	Respuestas
10.5 Respaldo o Back-Up	Se tiene definido el nivel necesario de respaldo de la información	Errores de los usuarios (E.1),Alteración de la Información (E.15),Introducción de Información Incorrecta,Destrucción de Información (E.18), (E.16),Degradación de Información (E.17)	2
	Se tiene registros completos de la información de los respaldos como: la fecha, hora, el tipo si es diferencial o completo, a que sistema corresponde, el responsable, si fue probado o no, nro de copias, procedimientos documentados de la restauración, si disponde de copias fuera del local)		2
	Los respaldos se almacenan en lugares apartados a una distancia suficiente que garantice que si se produce un desastre en el centro de datos principal, estos no se verán afectados		1
	Los medios de respaldo son probados regularmente para asegurar que se pueden confiar en ellos en el momento que se necesite usarlos, en caso de una emergencia		1
	Los procedimientos de restauración son chequeados y probados regularmente para asegurar que son efectivos y que pueden ser completados en el tiempo asignado en los procedimientos operacionales para la recuperación.		2

	Se tiene establecido el periodo de retención para la información comercial esencial y cualquier otra información o requerimiento para que las copias se mantengan permanentes		2
Datos PC's	Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados.	Avería de Origen físico	1
	Si hacen un backup deberían hacerlo en sus propias máquinas o en DVD's.		1
Documentación del area de sistemas	Los documentos se encuentran en gavetas bajo llave. Pero susceptible a daños por fuerza bruta.	Destrucción de Información (E.18), Robo (A.25)	2

2.2. ESTIMACION DEL ESTADO DE RIESGO

2.2.1. ESTIMACION DEL IMPACTO

OBJETIVOS DE LA ACTIVIDAD

- Determinar el impacto potencial al que está sometido el sistema
- Determinar el impacto residual al que está sometido el sistema

Productos de entrada

- Resultados de la actividad A2.1, Caracterización de los activos
- Resultados de la actividad A2.2, Caracterización de las amenazas
- Resultados de la actividad A2.3, Caracterización de las salvaguardas

Resultados

En esta tarea se estima el impacto al que están expuestos los activos del sistema:

- El impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas

  Probabilidad*Degradación= Impacto
- el impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

2.2.2. ESTIMACION DEL RIESGO

OBJETIVOS DE LA ACTIVIDAD

- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

Productos de entrada

• Resultados de la actividad A2.1, Caracterización de los activos
• Resultados de la actividad A2.2, Caracterización de las amenazas
• Resultados de la actividad A2.3, Caracterización de las salvaguardas

Resultados

En esta tarea se estima el riesgo al que están sometidos los activos del sistema:

- El riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- El riesgo residual, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

		FRECUENCIA				
		Infrecuente (I)	Poco frecuente cada varios años (PF)	Normal una vez al año (FN)	Frecuencia mensual (F)	Muy frecuente a diario (MF)
IMPACTO	Muy Alto	Medio	Alto	Muy Alto	Muy Alto	Muy Alto
	Alto	Bajo	Medio	Alto	Muy Alto	Muy Alto
	Medio	Muy Bajo	Bajo	Medio	Alto	Muy Alto
	Bajo	Inexistente	Muy Bajo	Bajo	Medio	Alto
	Muy Bajo	Inexistente	Inexistente	Muy Bajo	Bajo	Medio

Tabla 2.12 Escala de Impacto de una amenaza.[7]

TIPO DE ACTIVO HARDWARE

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Hardware Portátil	Incendio o Fuego (N.1, I.1)	2	□	1	Inexistente	2	0.20	Inexistente
	Desastres Naturales (N.*)	2	□	1	Inexistente	1	0.30	Inexistente
	Corte del suministro eléctrico (I.6)	2	□	1	Inexistente	3	1.00	Inexistente
	Desastres Industriales: Sobrecarga y fluctuaciones eléctricas (I.*)	2	□	3	Muy Bajo	2	1.00	Inexistente
	Avería de Origen físico o lógico de los equipos (I.5)	2	□	2	Muy Bajo	1	1.00	Inexistente
	Errores en la configuración y Errores del administrador (E.4, E.2)	2	ı	2	Inexistente	1	0.00	Inexistente
	Robo (A.25)	2	□	ı	Bajo	1	0.30	Inexistente
	Acceso no autorizado y Manipulación de la configuración (A.11, A.4)	2	□	1	Inexistente	1	0.00	Inexistente

	Caída del sistema por agotamiento de recursos informáticos (E.24)	2	□	3	Bajo	0	0.00	Inexistente
	Errores de Mantenimiento y actualización de equipos (E.23)	2	ı	1	Inexistente	1	0.30	Inexistente
	Ataque destructivo (A.26)	2	□	1	Inexistente	0	0.00	Inexistente
	Uso no previsto (A.7)	2	ı	2	Inexistente	0	0.00	Inexistente
	Condiciones inadecuadas de temperatura y humedad (I.7)	2	ı	1	Inexistente	1	0.00	Inexistente

Tabla 2.13 Estimación del Impacto y el Riesgo Potencial y Residual para portátiles.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
PC'S DE OFICINA	Incendio o Fuego (N.1, I.1)	2	□	2	Muy bajo	2	0.20	Muy bajo
	Desastres Naturales (N.*)	2	□	2	Muy bajo	2	0.10	Muy bajo
	Corte del suministro eléctrico (I.6)	2	□	2	Muy bajo	3	1.00	Inexistente
	Desastres Industriales: Sobrecarga y fluctuaciones eléctricas	2	ı	3	Bajo	2	1.00	Muy bajo

	(I.*)							
	Avería de Origen físico o lógico de los equipos (I.5)	2	[illegible]	4	Media	1	0.10	Media
	Errores en la configuración y Errores del administrador (E.4, E.2)	2	[illegible]	3	Bajo	1	0.00	Bajo
	Robo (A.25)	2	[illegible]	[illegible]	Inexistente	2	0.30	Inexistente
	Acceso no autorizado y Manipulación de la configuración (A.11, A.4)	2	[illegible]	1	Inexistente	1	0.00	Inexistente
	Caída del sistema por agotamiento de recursos informáticos (E.24)	2	[illegible]	3	Bajo	0	0.00	Bajo
	Errores de Mantenimiento y actualización de equipos (E.23)	2	[illegible]	4	Media	1	0.30	Media
	Ataque destructivo (A.26)	2	[illegible]	1	Inexistente	0	0.00	Inexistente
	Uso no previsto (A.7)	2	[illegible]	2	Inexistente	0	0.00	Inexistente
	Condiciones inadecuadas de temperatura y humedad (I.7)	2	[illegible]	1	Inexistente	1	0.00	Inexistente

Tabla 2.14 Estimación del Impacto y el Riesgo Potencial y Residual PCs de oficina.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual

	Incendio o Fuego (N.1, I.1)	5		2	Alto	2	0.20	Alto
	Desastres Naturales (N.*)	5		2	Alto	1	0.30	Alto
	Corte del suministro eléctrico (I.6)	5		2	Alto	3	1.00	Media
	Desastres Industriales: Sobrecarga y fluctuaciones eléctricas (I.*)	5		3	Media	2	0.60	Bajo
	Avería de Origen físico o lógico de los equipos (I.5)	5		3	Muy alto	2	0.30	Alto
Servidores	Errores en la configuración y Errores del administrador (E.4, E.2)	5		3	Muy alto	2	0.10	Alto
	Robo (A.25)	5			Alto	2	0.50	Media
	Acceso no autorizado y Manipulación de la configuración (A.11, A.4)	5		2	Alto	1	0.00	Media
	Caída del sistema por agotamiento de recursos infqormáticos (E.24)	5		3	Muy alto	2	0.30	Media
	Errores de Mantenimiento y actualización de equipos (E.23)	5		3	Muy alto	1	0.30	Alto
	Ataque destructivo	5		1	Media	2	0.50	Media

	(A.26)							
	Uso no previsto (A.7)	5		2	Alto	2	0.60	Media
	Condiciones inadecuadas de temperatura y humedad (I.7)	5		2	Media	1	0.30	Media

Tabla 2.15 Estimación del Impacto y el Riesgo Potencial y Residual Servidores.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Medios de Comunicación	Incendio o Fuego (N.1, I.1)	3		1	Muy bajo	2	0.20	Inexistente
	Desastres Naturales (N.*)	3		1	Muy bajo	1	0.30	Inexistente
	Avería de Origen físico o lógico de los equipos (I.5)	3		3	Media	1	0.20	Media
	Acceso no autorizado y Manipulación de la configuración (A.11, A.4)	3		1	Inexistente	1	0.00	Inexistente
	Caída del sistema por agotamiento de recursos informáticos (E.24)	3		3	Media	2	0.50	Media
	Errores de Mantenimiento y actualización de equipos (E.23)	3		1	Muy bajo	1	0.30	Inexistente
	Ataque destructivo (A.26)	3		2	Muy bajo	0	0.00	Muy bajo

	Uso no previsto (A.7)	3	˜ı□	2	Muy bajo	0	0.00	Muy bajo
	Condiciones inadecuadas de temperatura y humedad (I.7)	3	˜ı	1	Inexistente	1	0.30	Inexistente

Tabla 2.16 Estimación del Impacto y el Riesgo Potencial y Residual.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Establecimiento	Incendio o Fuego (N.1, I.1)	4	˜□	2	Medio	2	0.20	Medio
	Desastres Naturales (N.*)	4	˜□	1	Inexistente	1	0.30	Inexistente
	Acceso no autorizado	4	˜□	1	Medio	1	0.00	Medio
	Falta de Mantenimiento	4	˜□	2	Bajo	1	0.30	Bajo
	Ataque destructivo (A.26)	4	˜□	1	Bajo	0	0.00	Bajo
	Daños por Agua	4	˜□	1	Bajo	0	0.00	Muy bajo
	Condiciones inadecuadas de temperatura y humedad (I.7)	4	˜□	2	Inexistente	1	0.30	Inexistente

Tabla 2.17 Estimación del Impacto y el Riesgo Potencial y Residual.

TIPO DE ACTIVO SOFTWARE

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Paquetes de Software	Errores de los usuarios (E.1)	2	□̃	3	Medio	3	0.20	Media
	Errores del Administrador (E.2)	2	□̃	3	Alto	2	0.30	Alto
	Errores de configuración (E.4)	2	□̃	3	Alto	2	0.30	Alto
	Difusión de software dañino (E.8)	2	□̃	4	Muy Alto	3	1.00	Bajo
	Errores de secuencia (E.10)	2	□̃	3	Alto	2	1.00	Alto
	Escapes de Información (E.14)	2	□̃	1	Bajo	1	0.00	Bajo

	Vulnerabilidad en los programas de software (E.20)	2			Alto	2	0.50	Media
	Errores de mantenimiento/actualización de programas de software (E.21)	2		3	Alto	2	0.50	Media
	Manipulación de la configuración (A.4)	2		1	Bajo	3	0.70	Inexistente
	Suplantación de la identidad de usuario (A.5)	2		3	Alto	3	0.60	Media
	Manipulación de Programas (A.22)	2		2	Alto	3	0.60	Media
	Uso no previsto (A.7)	2		3	Alto	2	0.40	Media
	Manipulación de Programas (A.22)	2		3	Alto	2	0.60	Media

Tabla 2.18 Estimación del Impacto y el Riesgo Potencial y Residual Paquetes de Software Comercial.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Sistemas Operativos	Errores de los usuarios (E.1)	4		3	Bajo	2	0.60	Muy bajo
	Errores del Administrador (E.2)	4		3	Muy Alto	2	0.50	Alto
	Errores de configuración (E.4)	4		3	Muy Alto	2	0.50	Alto
	Difusión de software dañino (E.8)	4		2	Bajo	3	0.60	Muy Bajo

	Errores de secuencia (E.10)	4		3	Alto	2	0.00	Alto
	Vulnerabilidad en los programas de software (E.20)	4			Alto	2	0.40	Media
	Errores de mantenimiento/actualización de programas de software (E.21)	4		3	Muy Alto	2	0.60	Media
	Manipulación de la configuración (A.4)	4		3	Muy Alto	2	0.60	Media
	Suplantación de la identidad de usuario (A.5)	4		3	Alto	2	0.60	Media
	Manipulación de Programas (A.22)	4		3	Alto	2	0.40	Media
	Falta de Capacidad de Restauración	4		2	Alto	2	0.60	Media
	Uso no previsto (A.7)	4		2	Alto	2	0.40	Media

Tabla 2.19 Estimación del Impacto y el Riesgo Potencial y Residual Sistemas Operativos.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Sistema de Comercialización	Errores de los usuarios (E.1)	5		3	Media	2	0.60	Bajo
	Errores del Administrador (E.2)	5		2	Alto	2	0.50	Media
	Errores de configuración (E.4)	5		2	Alto	2	0.50	Media
	Difusión de software dañino (E.8)	5		1	Media	2	0.70	Bajo
	Errores de secuencia (E.10)	5		3	Alto	2	0.30	Alto
	Escapes de Información (E.14)	5		3	Alto	1	0.30	Alto
	Vulnerabilidad en los programas de software (E.20)	5			Muy alto	2	0.70	Media

	Errores de mantenimiento/actualización de programas de software (E.21)	5		3	Muy alto	2	0.70	Media
	Acceso no autorizado (A.11)	5		3	Muy alto	2	0.65	Media
	Manipulación de la configuración (A.4)	5		2	Alto	2	0.50	Media
	Suplantación de la identidad de usuario (A.5)	5		2	Alto	2	0.30	Media
	Manipulación de Programas (A.22)	5		1	Media	2	0.30	Media

Tabla 2.20 Estimación del Impacto y el Riesgo Potencial y Residual SICO.

Activo	AMENAZA	Valor Activo	Degradacion (0-1)	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Sistema Administrativo Financiero	Errores de los usuarios (E.1)	3	0.50		3	Media	2	0.60	Bajo
	Errores del Administrador (E.2)	3	0.75		2	Alto	2	0.40	Media
	Errores de configuración (E.4)	3	0.75		2	Alto	2	0.40	Media
	Difusión de software dañino (E.8)	3	0.80		1	Muy alto	2	0.60	Media
	Errores de secuencia (E.10)	3	0.90		3	Alto	2	0.30	Alto
	Escapes de Información (E.14)	3	0.30		3	Alto	1	0.30	Alto
	Vulnerabilidad en los programas de software (E.20)	3	1.00			Muy alto	2	0.70	Media

	Errores de mantenimiento/actualización de programas de software (E.21)	3	0.40		3	Muy alto	2	0.70	Media
	Acceso no autorizado (A.11)	3	0.75		3	Muy alto	1	0.65	Media
	Manipulación de la configuración (A.4)	3	0.74		3	Alto	1	0.50	Alto
	Suplantación de la identidad de usuario (A.5)	3	0.74		3	Alto	1	0.30	Alto
	Manipulación de Programas (A.22)	3	0.50		1	Media	1	0.30	Media

Tabla 2.21 Estimación del Impacto y el Riesgo Potencial y Residual Sistema Administrativo Financiero.

Activo	AMENAZA	Valor Activo	Degradacion (0-1)	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Sistema Recursos Humanos	Errores de los usuarios (E.1)	3	0.50		3	Media	2	0.60	Bajo
	Errores del Administrador (E.2)	3	0.75		2	Alto	2	0.40	Media
	Errores de configuración (E.4)	3	0.75		2	Alto	2	0.40	Media
	Difusión de software dañino (E.8)	3	0.80		4	Muy alto	2	0.60	Media
	Errores de secuencia (E.10)	3	0.90		3	Alto	2	0.30	Alto
	Escapes de Información (E.14)	3	0.30		3	Alto	1	0.30	Alto
	Vulnerabilidad en los programas de software (E.20)	3	1.00			Muy alto	2	0.70	Media
	Errores de mantenimiento/actualización de programas de software (E.21)	3	0.40		3	Muy alto	2	0.70	Media

	Acceso no autorizado (A.11)	3	0.75		3	Muy alto	1	0.65	Media
	Manipulación de la configuración (A.4)	3	0.74		3	Alto	1	0.50	Alto
	Suplantación de la identidad de usuario (A.5)	3	0.74		3	Alto	1	0.30	Alto
	Manipulación de Programas (A.22)	3	0.50		1	Media	1	0.30	Media

Tabla 2.22 Estimación del Impacto y el Riesgo Potencial y Residual del Sistema de Recursos Humanos.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Sistemas Documentales y Correo Electronico	Errores de los usuarios (E.1)	3		3	Muy bajo	2	0.60	Muy bajo
	Errores del Administrador (E.2)	3		2	Alto	2	0.40	Media
	Errores de configuración (E.4)	3		2	Alto	2	0.40	Media
	Difusión de software dañino (E.8)	3		4	Muy alto	2	0.60	Media
	Errores de secuencia (E.10)	3		3	Alto	2	0.30	Alto
	Escapes de Información (E.14)	3		3	Alto	2	0.30	Alto
	Vulnerabilidad en los programas de software (E.20)	3			Muy alto	2	0.70	Alto
	Errores de mantenimiento/actualización de programas de software (E.21)	3		2	Alto	2	0.70	Media

	Acceso no autorizado (A.11)	3	~	2	Media	2	0.65	Media
	Manipulación de la configuración (A.4)	3	~	2	Alto	2	0.50	Media
	Suplantación de la identidad de usuario (A.5)	3	~	2	Alto	2	0.50	Media
	Manipulación de Programas (A.22)	3	~	2	Alto	2	0.60	Media

Tabla 2.23 Estimación del Impacto y el Riesgo Potencial y Residual del Sistema Documentales y Correo Electrónico.

TIPO DE ACTIVO SERVICIOS

Activo	AMENAZA	Valor Activo	Degradacion (0-1)	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residu
Servicios Comunicación	Repudio (A.13	5	0.40	~	1	Bajo	1	0.30	Ba
	Denegación del Servicio (A.24)	5	1.00	~	3	Muy alto	2	0.40	Al
	Manipulación de la configuración (A.4)	5	0.90	~	3	Muy alto	2	0.30	Al
	Uso no previsto [A.7]	5	0.90	~	2	Alto	2	0.30	Al
	Caída del sistema por agotamiento de recursos [E.24]	5	0.90	~	3	Muy alto	2	0.30	Al

	Errores del administrador [E.2]	5	1.00			Muy alto	2	0.60		Al
	Indisponibilidad del Personal (A.28)	5	0.40			Muy alto	2	0.70		Al
	Errores de configuración [E.4]	5	0.60		3	Muy alto	2	0.70		Al

Tabla 2.24 Estimación del Impacto y el Riesgo Potencial y Residual Comunicación.

Activo	AMENAZA	Valor Activo	Degradacion (0-1)	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residu	
Servicio de Correo Electrónico	Repudio (A.13)	4	0.40		2	Media	2	0.30		Med
	Denegación del Servicio (A.24)	4	1.00		3	Alto	2	0.40		Al
	Manipulación de la configuración (A.4)	4	0.90		2	Alto	2	0.60		Med
	Caída del sistema por agotamiento de recursos [E.24]	4	0.90		1	Bajo	2	0.30	Muy ba	
	Errores de los usuarios [E.1]	4	0.30		4	Bajo	2	0.60	Muy ba	
	Acceso no autorizado (A.11)	3	0.75		2	Muy alto	2	0.65		Med
	Errores del administrador [E.2]	4	1.00			Alto	2	0.60		Med
	Indisponibilidad del Personal (A.28)	4	0.40			Bajo	2	0.70	Muy Ba	
	Errores de configuración [E.4]	4	0.60		3	Muy alto	2	0.70		Med

Tabla 2.25 Estimación del Impacto y el Riesgo Potencial y Residual Servicio Correo Electrónico.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Servicio Web	Repudio (A.13	3	□̃	2	Media	2	0.30	Media
	Denegación del Servicio (A.24)	3	□̃	3	Alto	2	0.40	Alto
	Manipulación de la configuración (A.4)	3	□̃	2	Alto	2	0.60	Media
	Uso no previsto [A.7]	3	□̃	3	Alto	2	0.30	Alto
	Caída del sistema por agotamiento de recursos [E.24]	3	□̃	3	Muy alto	2	0.60	Alto
	Errores del administrador [E.2]	3	□̃	□	Alto	2	0.70	Media
	Acceso no autorizado (A.11)	3	□̃	3	Muy alto	1	0.65	Media
	Indisponibilidad del Personal (A.28)	3	□̃	3	Muy alto	2	0.70	Media
	Errores de configuración [E.4]	3	□̃	3	Muy alto	2	0.70	Media

Tabla 2.26 Estimación del Impacto y el Riesgo Potencial y Residual del Servicio Web.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Servicio Intranet	Repudio (A.13)	3	□	2	Media	2	0.30	Media
	Denegación del Servicio (A.24)	3	□	3	Alto	2	0.40	Alto
	Manipulación de la configuración (A.4)	3	□	2	Alto	2	0.60	Media
	Uso no previsto [A.7]	3	□	3	Alto	2	0.30	Alto
	Caída del sistema por agotamiento de recursos [E.24]	3	□	4	Muy alto	2	0.60	Alto
	Acceso no autorizado (A.11)	3	□	□	Alto	2	0.70	Media
	Errores del administrador [E.2]	3	□	3	Muy alto	1	0.65	Media
	Indisponibilidad del Personal (A.28)	3	□	3	Muy alto	2	0.70	Media
	Errores de configuración [E.4]	3	□	3	Muy alto	2	0.70	Media

Tabla 2.27 Estimación del Impacto y el Riesgo Potencial y Residual del Servicio Intranet.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Servicio Atencion al Cliente	Repudio (A.13)	5	□̃	1	Media	2	0.30	Media
	Denegación del Servicio (A.24)	5	□̃	3	Muy alto	2	0.40	Alto
	Manipulación de la configuración (A.4)	5	□̃	3	Muy alto	1	0.30	Alto
	Caída del sistema por agotamiento de recursos [E.24]	5	□̃	3	Muy alto	2	0.50	Bajo
	Errores de los usuarios [E.1]	5	□̃	3	Bajo	2	0.60	Muy bajo
	Errores del administrador [E.2]	5	□̃	□	Muy alto	2	0.60	Alto
	Indisponibilidad del Personal (A.28)	5	□̃	□	Alto	2	0.70	Alto
	Errores de configuración [E.4]	5	□̃	3	Muy alto	2	0.70	Alto

Tabla 2.28 Estimación del Impacto y el Riesgo Potencial y Residual.Servicio de Atencion al Cliente

El servicio de atención al cliente tiene la estimación del impacto y riesgo, con el mismo esquema del sistema comercial. Solo se tendría problemas si se cae el servicio de comunicaciones o la intranet.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Servicio Help Desk	Repudio (A.13)	4	□̃	1	Muy bajo	2	0.60	Inexistente
	Denegación del Servicio (A.24)	4	□̃	3	Alto	2	0.40	Alto
	Manipulación de la configuración (A.4)	4	□̃	3	Muy alto	2	0.30	Muy alto
	Uso no previsto [A.7]	4	□̃	3	Media	2	0.30	Media
	Caída del sistema por agotamiento de recursos [E.24]	4	□̃ □̃	3	Media	2	0.30	Media
	Errores de los usuarios [E.1]	4	□̃	3	Bajo	2	0.60	Bajo
	Errores del administrador [E.2]	4	□̃	□	Muy alto	2	0.60	Alto
	Indisponibilidad del Personal (A.28)	4	□̃	□	Muy alto	2	0.70	Alto
	Errores de configuración [E.4]	4	□̃	3	Muy alto	2	0.70	Alto

Tabla 2.29 Estimación del Impacto y el Riesgo Potencial y Residual del Servicio Help Desk.

El servicio de help desk se vería afectado si se cae el servidor de sistemas documentales.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada (0-3)	Eficacia Salvaguarda (0-1)	Riesgo Residual
Internet	Denegación del Servicio (A.24)	3	□	3	Media	2	0.40	Media
	Manipulación de la configuración (A.4)	3	□	3	Media	2	0.30	Media
	Uso no previsto [A.7]	3	□	3	Media	1	0.30	Media
	Caída del sistema por agotamiento de recursos [E.24]	3	□	3	Alto	2	0.50	Media
	Errores de los usuarios [E.1]	3	□	1	Inexistente	2	0.60	Inexistente
	Errores del administrador [E.2]	3	□	□	Muy alto	2	0.60	Alto
	Indisponibilidad del Personal (A.28)	3	□	□	Muy alto	2	0.70	Alto
	Errores de configuración [E.4]	3	□	3	Muy alto	2	0.70	Alto

Tabla 2.30 Estimación del Impacto y el Riesgo Potencial y Residual del Servicio de Internet.

TIPO DE ACTIVO DATOS/INFORMACION

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Soporte electrónico	Incendio o Fuego (N.1, I.1)	1	□	2	Alto	2	0.20	Alto
	Desastres Naturales (N.*)	1	□	2	Alto	1	0.30	Alto
	Corte del suministro eléctrico (I.6)	1	□	2	Media	3	1.00	Bajo
	Desastres Industriales: Sobrecarga y fluctuaciones eléctricas (I.*)	1	□	3	Media	2	0.50	Bajo
	Avería de Origen físico o lógico de los equipos (I.5)	1	□	3	Media	1	0.30	Media
	Robo (A.25)	1	□	□	Alto	1	0.30	Alto
	Acceso no autorizado	1	□	2	Bajo	1	0.00	Bajo
	Ataque destructivo (A.26)	1	□	2	Media	0	0.00	Media
	Uso no previsto (A.7)	1	□	2	Media	0	0.00	Media

	Condiciones inadecuadas de temperatura y humedad (I.7)	1	□	3	Media	1	0.30	Media

Tabla 2.31 Estimación del Impacto y el Riesgo Potencial y Residual de Soporte Electrónico.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Documentacion y Registros	Incendio o Fuego (N.1, I.1)	2	□	2	Alto	2	0.20	Alto
	Desastres Naturales (N.*)	2	□	2	Alto	1	0.30	Alto
	Avería de Origen físico	2	□	2	Alto	1	0.30	Alto
	Robo (A.25)	2	□	□	Alto	1	0.30	Alto
	Acceso no autorizado	2	□	2	Alto	2	0.50	Media
	Ataque destructivo (A.26)	2	□	2	Alto	0	0.00	Alto
	Uso no previsto (A.7)	2	□	2	Alto	0	0.00	Alto
	Condiciones inadecuadas de temperatura y humedad (I.7)	2	□	2	Alto	1	0.30	Alto

Tabla 2.32 Estimación del Impacto y el Riesgo Potencial y Residual de la Documentación y Registros.

Activo	AMENAZA	Valor Activo	IMPACTO	Frecuencia Amenaza	Riesgo Potencial	Nivel Salvaguarda Aplicada	Eficacia Salvaguarda (0-1)	Riesgo Residual
Bases de Datos	Errores de los usuarios (E.1)	5	□̃	3	Muy alto	2	0.60	Media
	Alteración de la Información (E.15)	5	□̃	2	Alto	2	0.60	Media
	Introducción de Información Incorrecta (E.16)	5	□̃	3	Muy alto	2	0.60	Media
	Degradación de Información (E.17)	5	□̃	□	Muy alto	2	0.30	Media
	Destrucción de Información (E.18)	5	□̃	1	Muy alto	2	0.60	Media

Tabla 2.33 Estimación del Impacto y el Riesgo Potencial y Residual Bases de datos.

CAPITULO 3

3. ANÁLISIS E IMPACTO EN EL NEGOCIO

3.1. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA INTRANET CORPORATIVA

En este capítulo se describirá la infraestructura actual de la red de la CentroSur hasta finales de Agosto del 2010, los datos obtenidos son resultado de la información recogida en colaboración del administrador de la red de la Empresa, inventario realizado y revisión de las instalaciones físicas de la red. Esta información nos permitirá realizar el análisis de la situación actual de la red en cuanto a seguridad para determinar el punto de partida para la implementación del Plan de Contingencia.

3.1.1. UBICACIÓN FISICA DELA EMPRESA (LOCALES Y SEDES DE LA ORGANIZACIÓN)

La empresa Eléctrica CentroSur dispone de una Agencia Matriz y varias agencias de recaudación dentro y fuera del cantón Cuenca. Las cuales se listan a continuación:

- Biblián Agencia Empresa Eléctrica
- Cañar Agencia Empresa Eléctrica
  Av. Ingapirca y El Vergel
- Girón Agencia Empresa Eléctrica
- Gualaceo Agencia Empresa Eléctrica
  Av. Sucre y Colón (Esq.)
- Limón Agencia Empresa Eléctrica
- Macas Agencia Empresa Eléctrica
- Méndez Agencia Empresa Eléctrica
- Nabón Agencia Empresa Eléctrica
- Paute Agencia Empresa Eléctrica
- Sigsig Agencia Empresa Eléctrica
- Santa Isabel Agencia Empresa Eléctrica

El local objeto de análisis para este tema de tesis es la Matriz de la Empresa Eléctrica, la misma que se encuentra ubicada en el cantón Cuenca en la dirección Max Uhle y Pumapungo.

El edificio posee siete pisos, distribuidos en áreas, las que se encuentran separadas por las escaleras de acceso junto a los ascensores. El área de Atención al Cliente se encuentra en la planta baja del edificio. Con respecto a la disposición física de los servidores de la Empresa (Centro de Datos), estos

se encuentran ubicados en el séptimo piso del edificio, en el Área de Informática que cuenta con una alarma de seguridad para su acceso.

Los pisos ocupados por la Empresa son de concreto, cuentan con cableado estructurado categoría 6e, lo que facilita la administración física de la red. Cuentan con una red propia de energía eléctrica para los equipos, debidamente separada del cableado de datos.

3.1.2. INFRAESTRUCTURA DE LA RED DE LA EMPRESA

ESTRUCTURA DE LA RED LAN DE LA CENTROSUR

En este punto se presenta un breve análisis de las funciones que desempeñan cada uno de los principales componentes de red, con los que cuenta la empresa como son los routers, switches y módems de acceso, además se especifica el tipo de enlace que ofrecen a las agencias que se encuentran dentro y fuera del cantón Cuenca, así como puntos de recaudación y contratistas. Esta infraestructura está bajo la responsabilidad de la Dirección de Telecomunicaciones (Ditel) de la empresa CentroSur. El cuarto de comunicaciones donde se encuentran la mayoría de los equipos tanto de la red Wan como de la red lan están en la sala de Equipos Principal otros lo conocen como Centro de Datos de la Red WAN ubicado en el último piso del Edificio. Otra parte de los equipos informáticos se encuentran bajo la responsabilidad de la dirección de Control y Supervisión de Operaciones (CSO). Finalmente otros recursos informáticos se encuentran bajo la responsabilidad de la dirección de Distribución.

Las capas que conforman la arquitectura de red de la empresa son las que se describen a continuación:

Capa de Acceso:

Esta capa describe como los host de los usuarios se conectan a la red.

Las conexiones de red de los host de los usuarios, de cada piso del edificio matriz, llegan a los closet de comunicaciones, que se encuentran también en cada piso. Estos closets de comunicaciones, albergan los swichs y racks que a su vez se conectan a la capa de distribución.

El cableado estructurado de la red del edificio es cable UTP categoría 6e, cuentan con un 20% de tomas de datos de exceso para soportar el crecimiento futuro de puestos de trabajo. Para conectar la Bodega General, que se encuentra en el subterráneo, se utiliza fibra óptica. En el subterráneo no se tiene un cuarto de comunicaciones para los equipos.

Las áreas de trabajo cuentan en total con unos 300 Computadores Personales, los cuales se encuentran distribuidos en los diferentes, pisos del edificio matriz. La velocidad de transmisión por la red es de 100 Megabits por segundo.

El cableado estructurado es subcontratado, tanto para instalar nuevos puntos, como para el mantenimiento.

La empresa dispone de varios proveedores de cableado estructurado, pero en situaciones urgentes se tiene identificada una empresa específica, quien proporciona los servicios requeridos.

La empresa tiene dentro de sus políticas realizar un mantenimiento preventivo de ductos, una vez al año.

Capa de Distribución:

Red LAN

Esta capa permite el paso del tráfico de red, de la capa de acceso hacia la capa núcleo. En este nivel se encuentran los dos switchs de capa 3 o administrables, que son el core de la red, porque conectan a cada uno de los cuartos de comunicaciones, que se encuentran en los diferentes pisos que cuenta el edificio, a la plataforma de servicio (servidores). Los dos switches no son respaldo uno del otro, cada uno tiene asignado los componentes de red que debe interconectar. Como se puede ver en el Esquema de la Red LAN, en el libro de trabajo de la empresa. Para conectar cada uno de los pisos del edificio, al cuarto principal de comunicaciones, se tienen cableados rutas redundantes, las cuales no están siendo utilizadas para tal objetivo, pero sí se disponen, si se llegarán a necesitar.

El firewall Nokia IP 390, sirve para interconectar la red interna, con la red WAN de la empresa y con internet. En este equipo se encuentran las reglas de acceso. En el libro de trabajo de la empresa, se encuentra la ficha donde se describe detalladamente los datos de este equipo.

Para el acceso a Internet el firewall se conecta a un router, el cual se conecta directamente con el ISP que es Centronet, el cual está dentro de la misma infraestructura de CentroSur.

Red WAN

La red WAN de la empresa, la conforman las diferentes agencias, puntos de recaudación, entidades financieras, bancos, contratistas.

Para la interconexión con los contratistas, entidades financieras, bancos y puntos de recaudación, actualmente CentroSur es responsanble solo de que

las VPN y puertos del router estén activos. Cada uno de ellos es responsable de los enlaces.

Las agencias están conectadas por microonda la parte backbone y radio la ultima milla.

Capa Núcleo:

La capa núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia la plataforma de servicios. Estos servicios se conocen como servicios globales o corporativos. Algunos de los servicios que dispone la empresa eléctrica CentroSur se detallan a continuación:

PLATAFORMAS DE SERVICIO

Servidor de Base de datos

Los datos de los sistemas informáticos se encuentran centralizados en el servidor HW_ISERIESM25 (Ver libro de trabajo de la empresa), al cual acceden las diferentes aplicaciones de la empresa. Los datos se almacenan en su gran mayoría en un sistema de Base de Datos Relacional DB2, con sistema operativo OS/400 y se explotan generalmente vía Batch o transaccional SICO y otras aplicaciones, tanto directamente como en aplicativos.

Servidor de Aplicaciones

Es una plataforma de arquitectura cerrada, con sistema operativo OS/400 (estándar), en el cual se encuentran almacenadas todas las aplicaciones de sistemas informáticos desarrolladas en Lotus Note, por la misma empresa o por DataCrom (Empresa de desarrollo de software externa). Este se encuentra configurado en el equipo HW_HPDL140.

Servidor de Internet

Unos pocos usuarios utilizan el servidor Proxy de Linux Red Hat 7.5 llamado Squid, ubicado en el servidor de Internet. Este a su vez se conecta al firewall Nokia IP 390, para la conexión a Internet.

Servidor de Antivirus.

Este servidor tiene instalado un antivirus corporativo F-Security, con sistema operativo Windows 2000, mediante el cual provee a los clientes internos de la empresa, las actualizaciones de la base de datos de antivirus así como de las últimas actualizaciones de software.

Servidor de Directorio Activo

Este servidor tiene instalado el sistema operativo Windows 2003 Server y Active Directory, para dar acceso a los recursos del dominio, solo a los clientes internos de la empresa. Para ello se tiene el equipo HW_ITNM1 (ver libro de trabajo de la empresa) en el cual se encuentra configurado el Controlador de Dominio principal y DNS. En el equipo HW_HPML530 se encuentra el controlador de Dominio alterno, así como el DNS y DHCP.

Servidor web

El servidor web se encuentra configurado en el equipo HW_PSERIES510, con plataforma AIX 5.1 en el cual reside el portal Web de la empresa. Este portal fue desarrollado por una empresa externa en Softbuilder. El sitio provee información estática de la empresa, así como también información de cada uno de los clientes de la empresa. Para ello, cada uno de los clientes, tiene asignado un usuario y contraseña, con los cuales pueden acceder a su información personal, sobre los consumos de luz, pagos, etc. Para esto el servidor web, interactúa con el servidor de base de datos para poder obtener la información.

Servidor de Correo Electrónico

El servidor de Correo Electrónico se encuentra soportado por el sistema operativo AIX 5.1, mediante Lotus Domino y para los clientes Lotus Notes. El servicio del servidor de correo (incluye POP3 e IMAP), aplicaciones, HTTP, NNTP, LDAP y Servicios Web y el repositorio de datos pueden ser bases de datos NSF (nativas de Notes) o DB2 (base de datos relacional de IBM).

Servidor de Correo Blackberry

El servidor de Correo blackberry se encuentra soportado por el sistema operativo Windows 2003 Server, mediante la aplicación Blackberry Enterprise Server.

ARQUITECTURA FISICA DE LA RED

La arquitectura de la empresa se fundamente principalmente en ser cliente/Servidor con tres niveles. Esto significa que la arquitectura generalmente está compartida por:

1. Un cliente, es decir, el equipo que solicita los recursos, equipado con una interfaz de usuario (generalmente un navegador Web) para la presentación.

2. El servidor de aplicaciones (también denominado software intermedio), cuya tarea es proporcionar los recursos solicitados, pero que requiere de otro servidor para hacerlo.
3. El servidor de datos, que proporciona al servidor de aplicaciones los datos que requiere.

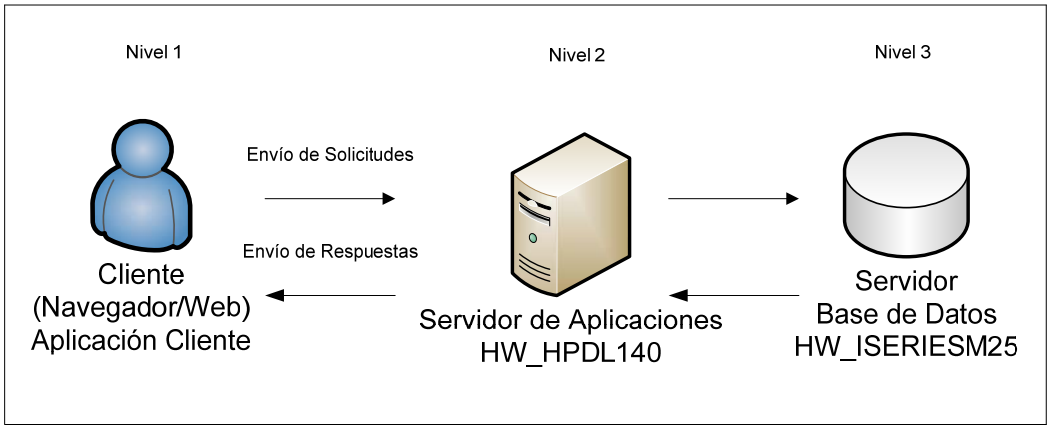


Figura 3.1. Arquitectura Cliente Servidor de tres niveles.

Sin embargo la empresa también dispone de aplicaciones que son cliente servidor con dos niveles como el servidor de RequisitePro y Help Desk

3.2. INTERPRETACION DE LOS RESULTADOS

3.2.1. INTERPRESTACION DE LOS RESULTADOS

OBJETIVOS DE LA ACTIVIDAD

- Interpretar los resultados anteriores de impacto y riesgo
- Establecer relaciones de prioridad por activos o grupos de activos, bien por orden de impacto o por orden de riesgo

Productos de entrada

- Resultados de la actividad A2.1, Caracterización de los activos
- Resultados de la actividad A2.2, Caracterización de las amenazas
- Resultados de la actividad A2.3, Caracterización de las salvaguardas
- Resultados de la tarea T2.4.1, Estimación del impacto
- Resultados de la tarea T2.4.2, Estimación del riesgo

Resultados

Luego de haber realizado todo el proceso de análisis de riesgo, se procederá a realizar el tratamiento de los riesgos sobre los activos críticos para la empresa, estableciendo que riesgos serán evitados, mitigados, trasferidos y aceptados.

PC´s	Avería de Origen físico o lógico de los equipos (I.5)	Medio
	Errores de Mantenimiento y actualización de equipos (E.23)	Medio
Servidores	Incendio o Fuego	Alto
	Desastres Naturales (N.*)	Alto
	Corte del suministro eléctrico (I.6)	Medio
	Avería de Origen físico o lógico de los equipos (I.5)	Alto
	Errores en la configuración y Errores del administrador (E.4, E.2)	Alto
	Robo	Medio
	Acceso no autorizado y Manipulación de la configuración (A.11, A.4)	Medio
	Caída del sistema por agotamiento de recursos infqormáticos (E.24)	Medio
	Errores de Mantenimiento y actualización de equipos (E.23)	Alto
	Ataque destructivo (A.26)	Medio
	Uso no previsto (A.7)	Medio
	Condiciones inadecuadas de temperatura y humedad (I.7)	Medio
Medios de Comunicación	Avería de Origen físico o lógico de los equipos (I.5)	Medio
	Caída del sistema por agotamiento de recursos informáticos (E.24)	Medio
Establecimiento	Incendio o Fuego	Medio
	Acceso no autorizado	Medio
Paquetes de Software	Errores de los usuarios (E.1)	Medio
	Errores del Administrador (E.2)	Alto
	Errores de configuración (E.4)	Alto
	Errores de secuencia (E.10)	Alto
	Vulnerabilidad en los programas de software (E.20)	Medio

	Errores de mantenimiento/actualización de programas de software (E.21)	Medio
	Suplantación de la identidad de usuario (A.5)	Medio
	Manipulación de Programas (A.22)	Medio
	Uso no previsto (A.7)	Medio
Sistemas Operativos	Errores del Administrador (E.2)	Alto
	Errores de configuración (E.4)	Alto
	Errores de secuencia (E.10)	Alto
	Vulnerabilidad en los programas de software (E.20)	Medio
	Errores de mantenimiento/actualización de programas de software (E.21)	Medio
	Manipulación de la configuración (A.4)	Medio
	Suplantación de la identidad de usuario (A.5)	Medio
	Manipulación de Programas (A.22)	Medio
	Falta de Capacidad de Restauración	Medio
	Uso no previsto (A.7)	Medio
Sistema de Comercialización, Sistema Administrativo Financiero, Recursos Humanos, Correo y Documentales, Servicio de Atención al	Errores de los usuarios (E.1)	Bajo
	Errores del Administrador (E.2)	Medio
	Errores de configuración (E.4)	Medio
	Errores de secuencia (E.10)	Alto
	Vulnerabilidad en los programas de software (E.20)	Medio
	Errores de mantenimiento/actualización de programas de software (E.21)	Medio
	Acceso no autorizado (A.11)	Medio
	Manipulación de la configuración (A.4)	Medio
	Suplantación de la identidad de usuario (A.5)	Medio

Cliente	Manipulación de Programas (A.22)	Medio
Servicio de comunicación	Denegación del Servicio (A.24)	Alto
	Manipulación de la configuración (A.4)	Alto
	Uso no previsto [A.7]	Alto
	Caída del sistema por agotamiento de recursos [E.24]	Alto
	Errores del administrador [E.2]	Alto
	Indisponibilidad del Personal (A.28)	Alto
	Errores de configuración [E.4]	Alto
Servicio de Correo Electronico, Help Desk	Repudio (A.13)	Medio
	Denegación del Servicio (A.24)	Alto
	Manipulación de la configuración (A.4)	Medio
	Errores del administrador [E.2]	Medio
	Errores de configuración [E.4]	Medio
Servicio Web	Repudio (A.13	Medio
	Denegación del Servicio (A.24)	Alto
	Manipulación de la configuración (A.4)	Medio
	Uso no previsto [A.7]	Alto
	Caída del sistema por agotamiento de recursos [E.24]	Alto
	Errores del administrador [E.2]	Medio
	Acceso no autorizado (A.11)	Medio
	Indisponibilidad del Personal (A.28)	Medio
	Errores de configuración [E.4]	Medio
Soporte electrónico	Incendio o Fuego (N.1, I.1)	Alto
	Desastres Naturales (N.*)	Alto
	Avería de Origen físico o lógico de los equipos (I.5)	Medio
	Robo (A.25)	Alto
	Ataque destructivo (A.26)	Medio
	Uso no previsto (A.7)	Medio
	Condiciones inadecuadas de temperatura y humedad (I.7)	Medio
Documentos y Registros	Incendio o Fuego (N.1, I.1)	Alto
	Desastres Naturales (N.*)	Alto
	Avería de Origen físico	Alto
	Robo (A.25)	Alto
	Acceso no autorizado	Medio
	Ataque destructivo (A.26)	Alto
	Uso no previsto (A.7)	Alto
	Condiciones inadecuadas de temperatura y humedad (I.7)	Alto
Bases de Datos	Errores de los usuarios (E.1)	Medio

	Alteración de la Información (E.15)	Medio
	Introducción de Información Incorrecta (E.16)	Medio
	Degradación de Información (E.17)	Medio
	Destrucción de Información (E.18)	Medio

Tabla 3.1. Tratamiento del Riesgo de los activos críticos de la empresa.

CAPITULO 4

4. DISEÑO DEL PLAN DE CONTINGENCIAS

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

4.1. MEDIDAS PREVENTIVAS

SEGURIDAD CONTRA INCENDIOS

RIESGO: Incendio o Fuego

RESPONSABLE: Operación y Soporte de Servicios Informáticos

Medidas Técnicas.

- En los centros de computo, y lugares donde se encuentre equipos de computación se contará con extintores de incendio tipo C, que serán recargados cada 12 meses cuando no han sido utilizados, y en un plazo de 72 horas cuando ha sido requerido su uso. Los extintores deberán tener exteriormente un registro de las fechas de la última y la próxima recarga.
- En el centro de datos principal se colocarán sensores de humo conectados aun sistema de alarmas de funcionamiento autónomo.
- Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
- En los centros de datos y lugares donde se cuentan con equipos de computación, deberán utilizar racks y archivadores de material ignifugo para proteger los equipos y documentacion crítica.
- Realizar un mantenimiento periódico a las instalaciones eléctricas, de por lo menos dos veces al año, que permitan prevenir cortoscircuitos.
- Equipos Informáticos de respaldo.

Medidas Organizativas

- Concientizar sobre las políticas establecidas que prohiban fumar cerca de los equipos informáticos

- Disponer de un precontrato de alquiler de equipos informáticos y ubicación alternativa.
- Contar con un procedimiento de copia de respaldo de todos los sistemas críticos de la empresa.
- Contar con un procedimiento de actuación en caso de incendio.
- Tener a la mano los números telefónicos de emergencia.

Medidas Humanas

- Formación para actuar en caso de incendio.
- El personal de la organización debe ser entrenado en el uso de extintores de incendio para equipo electrónico.
- Designación de un responsable de sala.
- Asignación de roles y responsabilidades para la copia de respaldo.

SEGURIDAD CONTROLANDO TEMPERATURA DE LOS EQUIPOS COMPUTACIONALES

RIESGO: Condiciones inadecuadas de Temperatura y Humedad.

RESPONSABLE: Operación y Soporte de Servicios Informáticos

- En el caso de los racks por su mayor masificación y por ser los dispositivos más pequeños y con una mayor integración de componentes la ventilación se convierte en un punto importante a tener en cuenta. Existen racks y armarios ventilados que permiten tener las máquinas en un punto de funcionamiento óptimo.

- Es importante que además de tomar las medidas necesarias para tener la temperatura dentro de unos límites aceptables, se tenga un sistema de monitorización de la temperatura. Este sistema puede ser un simple termómetro electrónico en la sala de computación o en los racks y armarios o un sistema de adquisición de datos conectado a un termómetro que pueda mandar datos de la temperatura a un ordenador que nos permita realizar la monitorización. Un ejemplo de un sistema de este tipo son los diversos aparatos que existen para su integración con el software Nagios y que nos permiten mediante plugins de Nagios la monitorización de la temperatura de cualquier sistema, avisándonos cuando supera los límites preestablecidos.

- Debe configurarse también correctamente la bios de los ordenadores para que monitoricen correctamente la temperatura interna y avisen si

esta supera los límites marcados. Lo mismo para la velocidad de giro de los ventiladores, que redunda al fin y al cabo en la temperatura que el hardware adquirirá.

SEGURIDAD CONTRA INUNDACIONES

RIESGO: Inundaciones

RESPONSABLE: Operación y Soporte de Servicios Informáticos

Medidas Técnicas

- En el centro de datos principal se colocarán sensores de detección de inundaciones a niveles de ras del suelo conectados a un sistema de alarmas de funcionamiento autónomo
- Disponer de cobertores para proteger los equipos.
- Contar con bolsas de plástico para cubrir servidores y documentos importantes que puedan mojarse.
- Colocar los CPUs de todos los usuarios en lugares seguros. No directamente en el suelo.

Medidas Organizativas

- Disponer de medidas preventivas de mantenimiento del edificio, revisión de goteras, filtraciones de agua, ductos de agua y drenaje, por lo menos dos veces al año.
- Disponer de un procedimiento para proteger el equipo contra el agua.

SEGURIDAD CONTRA DESASTRES NATURALES

RIESGO: Desastres Naturales como terremotos.

RESPONSABLE: Planificación de Servicios Informáticos.

Medidas Organizativas

- Crear un plan de evacuación del hardware que permita llevar los equipos críticos a otro edificio o departamento en un mínimo de tiempo y siguiendo un plan predeterminado que tenga en cuenta la importancia de cada sistema. Se deberá tener en cuenta al realizar el estudio y el plan de evacuación, la importancia de los equipos y sobre todo de los datos que albergan estos equipos, de forma que los equipos y datos más importantes sean evacuados primero, y los menos importantes puedan esperar. Se deberá plantear la necesidad de tener personal preparado

para este cometido y la facilidad con que estos datos se pueden mover de un lugar a otro.

- Etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las CPUs con Información importante o estratégica y color verde a las CPUs de contenidos normales.
- Lo principal normalmente en una empresa será evacuar los datos corporativos (datos de la empresa, datos de facturación y contabilidad, del personal que trabaja en la empresa, de los clientes y de los proveedores), que estarán en forma de discos duros, sistemas de almacenamiento NAS o cintas de backups.
    - Para los discos duros se facilita enormemente su evacuación si se dispone de discos duros hotswap (extracción en caliente) que puedan extraerse fácilmente del equipo y tengan una cierta protección física contra golpes o movimientos bruscos
    - Para los sistemas NAS se intentará que estos tengan también discos hotswap o que sean fácilmente desmontables y transportables.
    - Las cintas de backup suelen ser fáciles de transportar, pero deberá tenerse en cuenta que son sensibles a los campos magnéticos y a las temperaturas extremas.
- El plan de evacuación debe continuar con la evacuación de los backups y datos de trabajo de los usuarios para perder el mínimo de horas de trabajo posibles. Se debe tener en cuenta que normalmente es más caro el tiempo de trabajo del personal que trabaja en la empresa que la infraestructura informática de esta, por lo que antes de evacuar otro tipo de equipos deberán evacuarse los datos de trabajo del personal, analizando las prioridades previamente asignadas. Después se podrán evacuar todos los demás equipos que sea posible, teniendo en cuenta las consideraciones que la empresa encuentre más importantes, que pueden ser el valor económico de los equipos, la necesidad de disponibilidad inmediata de una infraestructura mínima para continuar con el trabajo o la necesidad de disponer de un sistema mínimo para la prestación de servicios a clientes y proveedores.

SEGURIDAD FISICA

RIESGO: Acceso no autorizado y Manipulación de la configuración (A.11, A.4) y Robo (A.25)

RESPONSABLE: Operación y Soporte de Servicios Informáticos.

Personal

- Política que el personal autorizado cuente con identificación.

Software

Medidas Organizativas

- Establecer Políticas y Procedimientos de Seguridad para la protección y uso del software de la organización.
- Políticas de control de acceso a las bibliotecas de código fuente de los sistemas operacionales evitando un acceso irrestricto.
- Políticas relacionadas con el ingreso y salida del software de la Unidad de Informática y de la empresa.

Medidas Técnicas

- Mantener un inventario actualizado del software que dispone la empresa con la siguiente información:
    - Listados y cuantificación del software (original y copias)
    - Descripción
    - Distribución (en qué equipos o dispositivos de almacenamiento secundarios se encuentra, en qué lugar físico se localizan: áreas del negocio, bancos, etc.)
    - Registro del software instalado, dado de baja, en proceso de adquisición, etc.)
    - Uso del software (tipo de uso, responsables de su uso, entre otros puntos)
- Politica para mantener por separado los códigos ejecutables de las bibliotecas de códigos fuentes de los sistemas operacionales.
- Crear una política y procedimientos para registrar en una bitácora el ingreso y salida del software que aseguren al menos lo siguiente:
    - Revisada (contenido, cantidad, destino)
    - Justificada (compra, pruebas, reemplazo, devolución, dado de baja, otro)
    - Aprobada por el responsable de informática que va a recibirlo/entregarlo.
    - Registrada (responsables, hora, motivo, etc.)
    - Devuelta (comparar con la fecha estimada de salida)
    - Devuelta en las mismas condiciones de entrada
    - Devolución autorizada por medio de un responsable de informática
    - El personal esté comprometido formalmente a no hacer un mal uso del mismo (copiarlo, dañarlo o modificarlo)

- Crear una política y procedimientos que determinen que la documentación de los sistemas, deben estar almacenadas de una manera segura, en un lugar donde no tengan acceso personal no autorizado.
- Crear una política y procedimientos que determinen los responsables de tener respaldo de los códigos fuentes y ejecutables del software de la empresa, que garanticen su disponibilidad en caso de una contingencia.
- Disponer de una lista de acceso que ayude a restringir al mínimo el acceso a la documentación de los sistemas informáticos, la misma que será administrada por el propietario de la aplicación.
- Utilizar material ignifugo para almacenar los diferentes tipos de documentación, software y medios electrónicos críticos para el funcionamiento de la empresa.

Hardware

Medidas Organizativas

- La empresa debe de contratar un seguro contra robo, incendio, inundaciones, daño o desastres naturales o industriales, para todo el equipamiento electrónico catalogado como bien o activo, cuyo valor actual sea al menos el 30% del valor de la compra, o cuyo valor supere los $1000.
- Establecer una política de control de acceso a la zona de equipos o centro de datos, que restrinja solo al personal autorizado la ejecución de los procesos involucrados en dichos equipos.
- Cuando se requiera que una persona ajena a los procesos informáticos de misión crítica ingrese a la zona de equipos corporativos del centro de datos, deberá hacerlo permanentemente acompañada por una persona autorizada a ingresar a la zona.
- Establecer controles y procedimientos para la clasificación y justificación del personal con acceso a los centros de cómputo del negocio y a las oficinas donde se encuentra papelería o accesorios relacionados con informática.
- Definir una política de aceptación de la entrada a visitantes a la zona del centro de datos. En la cual se especifique claramente las horas de acceso que se puede autorizar.
- Establecer como política, el realizar periódicamente (semestralmente) una verificación física del inventario de activos.
- El personal de limpieza, de mantenimiento del edificio y personal similar debe pasar por los mismos sistemas de control de acceso, que los administradores o usuarios de las máquinas. Lo ideal es que personal de

vigilancia acompañe al personal de limpieza y mantenimiento cuando este deba acceder a los centros de computación o a los sitios donde estén alojados servidores o sistemas de almacenamiento de datos.

Medidas Técnicas

- Los centros de datos deberán contar con un sistema de llaves de seguridad en las puertas para su acceso, y un sistema de alarmas de detección de apertura o rotura de puertas y ventanas cuyo funcionamiento sea autónomo.
- Disponer de personal encargado del control de acceso al hardware del centro de datos, combinado con la utilización de llaves, tarjetas o dispositivos electrónicos.
- Establecer una política y controles para el manejo de bitácoras especiales para los visitantes a los centros de datos.
- Los dispositivos y servidores situados fuera de los centros de datos o de computación o en las zonas departamentales deberán ser protegidos mediante armarios o racks cerrados con llave y deberá imponerse una política en el departamento de acceso a estos sistemas.

Cableado

Medidas Técnicas

- El uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada, en caso de falla de alguna de ellas.
- Políticas y procedimientos que establezcan la iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves.
- Acceso controlado para empalmar los paneles y los cuartos de cableado.

Documentación

- Crear una política y procedimiento en la cual se sugiera contar con vales de salida de documentos y registros del área de TICs, autorizado por el jefe del área.
- Definir un procedimiento y el personal encargado del área de archivo de TICs.
- Establecer dentro de la polítca y del procedimiento el lugar físico donde se encuentran resguardados los archivos impresos y digitales, deberá ser un lugar aislado y seguro.

GESTION DEL CAMBIO DE LOS SISTEMAS DE INFORMACION

RIESGO: Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Desarrollo y Mantenimiento de Sistemas Informáticos.

Medidas Técnicas

Establecer controles de seguridad que permitan cubrir con los siguientes puntos:

- Para realizar cualquier cambio se debe analizar el impacto de la implantación del software en el medio de informática: aplicaciones, hardware, costos. uso del software actualizado como errores, agujeros de seguridad, incompatibilidades.
- Autorización del software por medio de la justificación de la actualización (es decir que los usuarios autorizados acepten el cambio antes de implementarlo).
- Asegurar que el conjunto de documentación del sistema este actualizado al completar cada cambio y que la documentación antigua se archive o se elimine.
- Mantener un control de la versión para todas las actualizaciones del software.
- Mantener un rastro de auditoría de todas las solicitudes de cambio, en lo posible enlazadas con las memorias técnicas o registros de cambio más abajo mencionadas.
- Asegurar que la documentación de operación y procedimientos de usuario sean cambiados según sea necesario para seguir siendo apropiados.
- Las actualizaciones automáticas no deben estar permitidas en los sistemas críticos de la empresa ya que algunas actualizaciones pueden causar que fallen las aplicaciones críticas (ver 12.6)
- Las actualizaciones o reemplazos son realizadas solo por administradores capacitados con la respectiva autorización.
- La implementación de los cambios se deben realizar en el momento adecuado y no interrumpen los procesos comerciales, salvo ciertas excepciones consideradas y autorizadas por la autoridad respectiva.
- Todo el software que dispone la empresa debe de disponer de un registro o memoria técnica respectiva del desarrollo, actualización, mantenimiento, o reemplazo del mismo. Esta memoria técnica deberá de

disponer de al menos fecha, hora, responsable, motivo, autorización, tareas realizadas, errores o fallas que se presentaron durante el proceso de implantación.

OPERABILIDAD DE LOS SISTEMAS DE INFORMACION

RIESGO: Avería de Origen físico o lógico de los equipos (I.5), Caída del sistema por agotamiento de recursos informáticos (E.24), Difusión de software dañino (E.8), Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Operación y Soporte de Servicios Informáticos.

Medidas Organizativas

- Se deben disponer de procedimientos de monitoreo del funcionamiento de los sistemas críticos de la empresa para asegurar su funcionamiento eficiente.
- Disponer de procedimientos documentados de los sistemas críticos de la empresa como: bases de datos, servidor de aplicaciones, servidor de correo, servidor web, copias de seguridad y respaldo de datos e información.
- Tener documentados los contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.
- Tener debidamente identificados y establecidos los responsables y las funciones a desarrollar para cada uno de los sistemas críticos de la empresa.

Medidas Técnicas

- El software operacional crítico deberá tener documentado la información requerida como parámetros, procedimientos, detalles de configuración y software de soporte revisar procedimientos capitulo 6.
- El software operacional critico deberá de disponer de estrategias de regreso a la situación original "roll back" antes de implementar los cambios
- Se deberá mantener las versiones previas del software de aplicación como una medida de contingencia si la nueva versión del software presenta errores o fallos que permitan aplicar la estrategia de “roll back”.
- Se debe tener identificados y establecidos los parámetros o criterios requeridos para determinar el comportamiento eficiente del sistema.

- Disponer de herramientas para el monitoreo y notificación de posibles problemas en los recursos claves de los sistemas.
- Las proyecciones futuras de crecimiento en las capacidades de los recursos de los sistemas se deberían basar en las tendencias actuales del monitoreo de los recursos claves de los sistemas.
- Tener documentados las interdependencias con otros sistemas para al darse un error identificar que procesos y sistemas del core del negocio se verán afectados.
- Establecer los tiempos que les tomaría realizar cada uno de los procedimientos operacionales requeridos para levantar los sistemas y sus respectivos componentes.
- Tener documentadas instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.

Medidas de Personal

- Elaborar un programa de vacaciones que garantice la presencia permanente del personal para vigilar el correcto funcionamiento de los sistemas.

SEPARACION DE AMBIENTES DE DESARROLLO Y PRODUCCION DE LOS SISTEMAS DE INFORMACION.

RIESGO: Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Desarrollo y Mantenimiento de Sistemas Informáticos.

Medidas Organizativas.

- Disponer de políticas y procedimientos de seguridad que verifiquen que el software desarrollado cumple con los requisitos previamente identificados. Este personal puede ser el personal de informática interno de la empresa debidamente calificado y autorizado para realizar la respectiva aceptación de los programas desarrollados.
- Se tiene asignado al personal responsable de definir y verificar los criterios de aceptación para el traspaso del ambiente de desarrollo al ambiente operacional

- Establecer procedimientos y politicas documentadas para la aceptación del traspaso de un nuevo sistema del ambiente de desarrollo y pruebas al ambiente operacional.
- Establecer un procedimiento de control de todos los movimientos o transacciones rechazados por el sistema que ayuden a comprobar que los datos erróneos para el sistema sean registrados, corregidos, alimentados correctamente y actualizados).
- Se deben establecer los responsables que asignan los permisos de acceso al personal de desarrollo, al ambiente operacional o viceversa.
- Crear una política y procedimientos para establecer el respaldo de los códigos fuentes y los ejecutables de los diferentes sistemas de información y aplicativos críticos para la empresa. Los mismos que en caso de una contingencia se encuentren disponibles.

SEGURIDAD EN LOS PROCESOS DE LOS USUARIOS

RIESGO: Avería de Origen físico o lógico de los equipos (I.5), Caída del sistema por agotamiento de recursos informáticos (E.24), Difusión de software dañino (E.8), Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Operación y Soporte de Servicios Informáticos.

Medidas Organizativas.

- Se establezca la política que los usuarios tienen la obligación de respaldar a través de un medio de almacenamiento que la empresa defina así como el período de respaldo de la información que almacenan en sus equipos; el medio utilizado para el almacenamiento deberá ser adecuadamente etiquetado en su exterior.
- Se establezca una política que los usuarios tienen la obligación de resguardar sus claves de acceso a los servicios y equipos que administran.
- Se establezca una política que los usuarios no deberán instalar software ilegal en los equipos que administran.
- Crear una política y procedimientos para asignación de claves a los usuarios para los diferentes sistemas.
- Se debe tener como política de seguridad que los usuarios una vez que han terminado sus actividades deben cerrar las sesiones activas (no solo apagar la pantalla de la PC o terminal). Esto para evitar que los equipos de los usuarios queden desatendidos.

Medidas Técnicas

- Se deberá establecer de algún mecanismo automático de cierre, que después de unos minutos de inactividad el sistema se bloquee y para volver a activar la sesión se debe ingresar la clave de usuario.
- Capacitar a los usuarios en el manejo de las diferentes herramientas, aplicaciones y equipos informáticos que estén bajo su cargo. Entregar manuales de usuario si la complejidad del recurso a utilizar lo amerita.
- Elaborar un Plan de capacitación básica respecto a los aplicativos según el perfil de usuario.

DISPONIBILIDAD DE ACCESO A LA RED DE DATOS

RIESGO: Avería de Origen físico o lógico de los equipos (I.5), Caída del sistema por agotamiento de recursos informáticos (E.24), Difusión de software dañino (E.8), Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Operación y Soporte de Servicios Informáticos.

Medidas Organizativas.

- Establecer procedimientos de autorización para determinar quién está autorizado a tener acceso a cuáles redes o subredes y servicios de red.
- Establecer políticas y procedimientos para el control de accesos de usuarios remotos.

Medidas Técnicas.

- Las conexiones de fibra óptica o de cobre, que forman parte del backbone de red, deberán mantener redundancia para su rápida sustitución en caso de emergencia.
- La Unidad de Informática deberá disponer de un firewall de respaldo redundante que permita garantizar la continuidad de las actividades del negocio. De igual manera, para los switches capa 3 que son parte del backbone de la red de Centrosur.
- Establecer como política que los puertos de los switches que no son ocupados deberán estar desactivados para evitar el acceso no autorizado a la red de datos.
- Si se tiene puntos de red libres, que no estén siendo usados por nadie, deben ser desconectados. Si se va a instalar una nueva máquina o se necesita otro punto de red entonces se conecta el cable que da conectividad al punto de red en cuestión con el respectivo puerto del

concentrador en el rack. Tener todos los puntos de red conectados es tener accesos libres a la red, repartidos por toda la empresa que cualquiera puede usar, incluido un supuesto intruso.

- Establecer como política el que exista dentro de la red de la organización segregación de redes mediante VLANs las cuales se tengan claramente identificados que usuarios pueden compartir recursos y que accesos están autorizados para las diferentes redes y medios. Por ejemplo, sistemas de acceso público, redes internas y activos críticos.
- Monitorear a los usuarios para verificar el acceso a los servicios que tienen, para los cuales hayan sido específicamente autorizados.
- Tener actualizados los diagramas de red que ayuden a tomar decisiones sobre el uso y autorizaciones de las redes y sus servicios.
- Los usuarios tienen acceso a los servicios para los cuales hayan sido específicamente autorizados.
- Los puertos de diagnostico y configuración remotos, deberán estar normalmente desactivados y solo se los activa cuando se requiere realizar alguna tarea de mantenimiento en el equipo, mediante un proceso de autorización entre el responsable y el personal de soporte.
- Disponer de un servidor dhcp redundante, que permita que si el servidor que actualmente está en operación sufre un daño, el redundante entre a funcionar.

DISPONIBILIDAD EN LOS EQUIPOS COMPUTACIONALES

RIESGO: Avería de Origen físico o lógico de los equipos (I.5), Caída del sistema por agotamiento de recursos informáticos (E.24), Difusión de software dañino (E.8), Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Operación y Soporte de Servicios Informáticos.

Medidas Organizativas.

- Establecer como política que sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio de mantenimiento a los equipos
- Políticas orientadas a confirmar que el hardware actualizado/reemplazado cubra los siguientes puntos:
    - Autorización por medio de la justificación de la actualización/reemplazo

- Impacto de la implantación del hardware en el medio de informática: aplicaciones, software y costos
- Procedimientos de emergencia y respaldo ante una falla en la aplicación del cambio.
- Registro de los cambios realizados (fecha, hora, respondable, motivo, autorización, tareas realizadas, errores o fallas detectadas durante el cambio)
- Implicaciones de control en la implantación y uso del hardware actualizado

Medidas Técnicas.

- Disponer de un inventario de activos de los equipos informáticos en los que se detalle:
  - Cuantificación del hardware
  - Descripción del hardware (características básicas)
  - Distribución del hardware (ubicación física mediante planos por capas por tipo de hardware, prioridad)
  - Áreas de informática: departamentos usuarios y áreas locales y remotas.
  - Registro del hardware instalado, dado de baja, en proceso de adquisición
  - Uso del hardware: desarrollo, operación, mantenimiento, monitoreo y toma de decisiones
  - Responsables del funcionamiento y control del hardware
- La Unidad de Informática deberá disponer, en stock de 2 portátiles, 5 PCs, 2 impresoras laser, 1 scanner, para reemplazo emergente de equipamiento crítico de la empresa.
- La unidad de informática deberá disponer de un stock mínimo de componentes informáticos cuyo daño sea más frecuente (discos duros, monitores, unidades de CD/DVD, flash memory, ups).
- Los equipos de informática deben recibir el respectivo proceso de mantenimiento en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor
- Crear una política y procedimiento donde se norme el disponer de registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo realizado.
- Tener presente el cumplir con todos los requerimientos impuestos por las pólizas de seguros.
- Disponer de herramientas de software que permitan monitorear y vigilar la integridad del hardware, mediante redes basados en SNMP como:

  - Netview de HP que permite la monitorización del estado del hardware, de cómo está funcionando y de los parámetros que puedan afectar al tiempo medio entre fallos de este hardware.
  - Otro sistema de este tipo es OpenView de HP, que provee todas estas funcionalidades.
  - Como software libre citaremos a OpenNMS que intenta ser una alternativa libre a los sistemas de gestión de red comerciales.
  - El sistema SMART está implementado en la mayoría de los discos duros, informándonos de todos los parámetros de funcionamiento como el tiempo estimado entre fallos o el tiempo estimado de vida del disco. Esta funcionalidad SMART de los discos duros, ayudan a prever fallos antes de que estos se produzcan

- El control de calidad de las máquinas y los dispositivos de red debe estar basado en dos premisas. La primera es la adquisición de equipos certificados y donde el fabricante nos asegure que se han realizado las pruebas de estrés suficientes sobre ellos para garantizar su calidad. La segunda es la monitorización de estos equipos y la estimación de la vida útil y el tiempo medio de fallos en los mismos.

- Se recomienda disponer para los servidores críticos de la empresa eléctrica así como para los equipos de comunicaciones, la estrategía de replicación. Para garantizar que los daños que estos puedan sufrir no afecten la disponibilidad de las operaciones del negocio. Tanto a nivel de maquinas como a nivel interno de los componentes de hardware (fuentes de poder, tarjetas de red redundantes, varios discos duros montados en RAID).

DISPONIBILIDAD EN LOS SERVICIO DE SOPORTE PÚBLICO

RIESGO: Avería de Origen físico o lógico de los equipos (I.5), Caída del sistema por agotamiento de recursos informáticos (E.24), Difusión de software dañino (E.8), Errores en la configuración, Errores del administrador (E.4, E.2), Acceso no autorizado y Manipulación de la configuración (A.11, A.4), Errores de Mantenimiento y actualización (E.23), Uso no previsto (A.7).

RESPONSABLE: Operación y Soporte de Servicios Informáticos.

Medidas Técnicas

- El equipo de telecomunicaciones de internet se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que

la falla en una conexión afecte el desempeño de los servicios que utilizan internet. Los servicios de internet debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia.

DISPONIBILIDAD DE LOS RESPALDOS DE DATOS/INFORMACION

RIESGO: Alteración de la Información (E.15), Destrucción de Información (E.18), Introducción de Información Incorrecta (E.16), Degradación de Información (E.17)

RESPONSABLE: Desarrollo y Mantenimiento de Sistemas Informáticos.

Medidas Organizativas

- Crear una política y procedimientos que normen el disponer de registros completos de la información de los respaldos como: la fecha, hora, el tipo si es diferencial o completo, a que sistema corresponde, el responsable, si fue probado o no, número de copias, procedimientos documentados de la restauración, si dispone de copias fuera del local)
- Establecer dentro de una política de respaldo de datos que los mismos se almacenen en lugares apartados, a una distancia suficiente, que garantice que si se produce un desastre en el centro de datos principal, estos no se verán afectados.
- Los medios de respaldo deberán ser probados regularmente para asegurar que se pueden confiar en ellos en el momento que se necesite usarlos, en caso de una emergencia
- Los procedimientos de restauración son chequeados y probados regularmente para asegurar que son efectivos y que pueden ser completados en el tiempo asignado en los procedimientos operacionales para la recuperación.
- Establecer el periodo de retención para la información comercial esencial y cualquier otra información o requerimiento para que las copias se mantengan permanentes.

Medidas Técnicas

- Los sistemas de backup y almacenamiento de datos deberán estar en localizaciones seguras dentro del edificio y lejos de canalizaciones de energía o agua, por ser crítico su funcionamiento para la seguridad de los datos
- Los armarios ignífugos son eficaces hasta cierto punto contra los incendios. Si estos son de pequeña magnitud probablemente nuestros backups sobrevivirán, pero si se tiene un incendio de gran intensidad dentro del armario, destruirá los datos de los backups, por lo que son

sólo relativamente eficaces contra este tipo de eventos. Lo mismo es aplicable para los terremotos y otros accidentes naturales.

- El sistema más eficaz para mantener los backups seguros es mantenerlos fuera del edificio, o al menos mantener una copia de estos, ya sea en otro edificio o en un centro de almacenamiento de backups.
    - Estos últimos son centros que proporcionan almacenamiento de las cintas de backup con todas las medidas de seguridad física imaginables y que son una buena alternativa para el mantenimiento de los backups. Puede contratarse uno de estos servicios y mandar los backups o copias de estos a uno de estos servicios, que velará por su seguridad. Normalmente este tipo de servicios se encarga de ir a la empresa en los periodos de tiempo concertados para recoger las cintas de backup.
    - Otra alternativa es mantener backups distribuidos, replicando los backups entre edificios o entre sistemas informáticos, para prevenir la perdida de datos por culpa de un problema de seguridad física en alguno de los sistemas o edificios
    - La frecuencia de los backups también es un factor a tener en cuenta, puesto que no siempre es posible el llevar fuera del edificio o sección los backups en un espacio de tiempo suficientemente corto como para asegurar la mínima perdida de datos y trabajo cuando se produce un desastre de este tipo. Los backups remotos son una opción a tener en cuenta en estos casos, usando sistemas que realizan backups a través de red en máquinas situadas en otros edificios, posiblemente con replicación de los datos, para mantener varias copias de los datos y los backups y preveer así la contingencia de un incendio o un desastre natural en uno de los edificios.

L a forma más común de realizar los respaldos es diariamente en cintas o tapes, y almacenarlas en lugares externos. Sin embargo existen otros medios confiables, que incluyen discos removibles.

4.2. RELACIONES DE COORDINACION

Las relaciones de coordinación son aquellas que se establecen con diferentes entidades ya sean internas o externas a la empresa, con el fin que en caso de presentarse algún evento o suceso donde nuestras operaciones queden fuera de servicio, estas entidades nos ayuden a salir de la crisis y podamos iniciar las operaciones en los tiempos establecidos.

Relaciones de coordinación internas:

- Dirección de Telecomunicaciones
- Departamento de Seguridad Industrial.
- Dirección de Sistemas Informaticos.
- Departamento de Sistemas de Información Geográfico.
- Departamento de Servicios Generales

Relaciones de coordinación externas:

- Bomberos.
- Policia Nacional
- Cruz Roja.
- Proveedor de Servicios de Internet y enlace de datos.
- Empresa de Seguros
- Hospitales
- Empresa donde se dispondrá como sitio alterno de Operaciones
- Empresa de Almacenamiento de Respaldos.
- Empresa Proveedora de hardware.
- Empresas Proveedoras de Software Comercial.

4.3. COORDINADOR DEL PLAN DE CONTINGENCIA (CPC)

El Coordinador del Plan de Contingencia (CPC), es responsable de la supervisión y coordinación de todas las actividades de recuperación establecidas en este plan. Conforme se implante el Plan, será el responsable de acumular y administrar toda la información que esté incluida en el mismo.

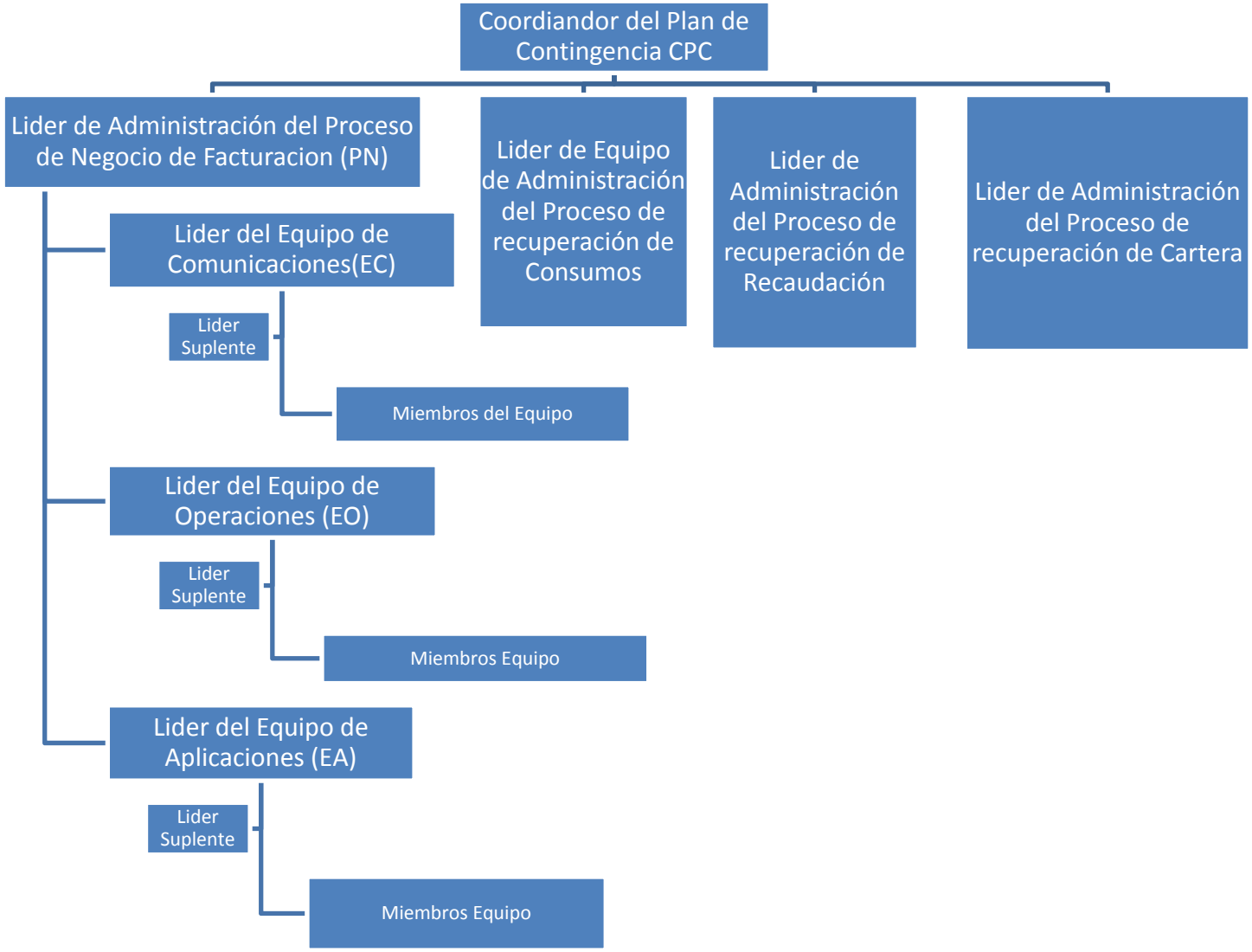
El CPC es responsable de obtener copias de este Plan y distribuirlas a los líderes de los equipos y a sus suplentes. Debe además encargarse de mantener copias de este Plan seguras en los sitios alternos que se determinen.

Todas las actividades de este Plan deben ser ensayadas, tanto para asegurar que los procedimientos funcionarán correctamente, como para brindar entrenamiento a los diferentes equipos. El CPC programará los ensayos y documentará los resultados favorables o negativos. Cuando un ensayo falle, deberá trabajar junto con el líder del equipo correspondiente para resolver los problemas, actualizar el Plan y programar otro ensayo.

4.4. ORGANIGRAMA DEL EQUIPO DEL PLAN DE CONTINGENCIA

Para la adecuada gestión de las diferentes actividades del Plan, es necesario contar con varios equipos de trabajo, los mismos que dependen del tamaño de la organización, de los recursos existentes, (recursos humanos, equipos electrónicos y procesos).

A continuación se presenta el esquema gráfico de cómo se debería establecer el organigrama del Plan de contingencia para la empresa eléctica CentroSur, incluyendo todos los procesos de negocio críticos de la empresa.


Coordiandor del Plan de Contingencia CPC
Lider de Administración del Proceso de Negocio de Facturacion (PN)
Lider de Equipo de Administración del Proceso de recuperación de Consumos
Lider de Administración del Proceso de recuperación de Recaudación
Lider de Administración del Proceso de recuperación de Cartera
Lider del Equipo de Comunicaciones(EC)
Lider Suplente
Miembros del Equipo
Lider del Equipo de Operaciones (EO)
Lider Suplente
Miembros Equipo
Lider del Equipo de Aplicaciones (EA)
Lider Suplente
Miembros Equipo

Equipo de Comunicaciones (EC): Este equipo se encarga de las acciones de recuperación de las comunicaciones y debe informar al CPC de la interrupción en el servicio y el avance en la recuperación.

Algunas de sus responsabilidades son las siguientes:

- Desarrollar y documentar las configuraciones de las comunicaciones de datos.
- Determinar el daño en la red de comunicaciones y asegurar la provisión del equipo de reemplazo.
- Coordinar la instalación del software del sistema operativo que permita la restauración de las comunicaciones.
- Ordenar e instalar el hardware necesario para establecer comunicaciones con las oficinas.
- Coordinar con entes externos por ejemplo con los ISPs para restaurar el servicio y ordenar las comunicaciones.
- Probar que las comunicaciones se hayan establecido adecuadamente.

Equipo de Operaciones (EO): Este equipo de trabajo coordina con el CPC el avance de la restauración de las operaciones de las plataformas críticas. Entre sus responsabilidades están las siguientes:

- Asegurar la disponibilidad de los respaldos necesarios en la recuperación.
- Restaurar archivos y sistema operativo en el sitio de recuperación.
- Elaborar calendarios de operaciones en el sitio de recuperación.
- En caso necesario, coordinar actividades necesarias para restaurar las facilidades en el sitio principal o en la nueva ubicación.
- Ordenar e instalar el hardware necesario para el procesamiento normal en el sitio permanente.

Equipo de Aplicaciones (EA): Este equipo coordina con el CPC y supervisa la restauración de las aplicaciones que residen en el computador principal. Entre sus responsabilidades están las siguientes:

- Coordinar la recuperación de las aplicaciones en el computador alterno y en el computador principal, en caso necesario.
- Reconstruir el ambiente de operación de las aplicaciones que residen en los servidores.
- Soportar el esfuerzo de los usuarios para actualizar los datos de la aplicación.
- En caso necesario, desarrollar un plan de trabajo detallado para moverse del sitio-alterno al sitio principal.

A continuación se tiene una propuetas del organigrama para ejecutar el plan de contingencia de acuerdo al personal que para ese momento dispone la empresa, excepto para el CPC, debido a que es un cargo se solo puede ser sugerido por los directivos de la empresa.

ORGANIGRAMA DEL EQUIPO DEL PLAN DE CONTINGENCIA									
Cordinador del Plan de Contingencias (CPC)	**Procesos y Servicios de Negocio**	**Sistemas Informáticos que los soportan**	**Lider del Equipo de Aplicaciones (EA)**	**Lider de Administración del proceso de Negocio (PN)**	**Lider del Equipo de Operaciones de los Servidores (EO)**				**Lider Equipo Comunicaciones (EC)**
	Servicios	SICO	Susana Ortega Ingeniero de Sistemas	Luis Guillen Jefe Dpto. Servicios al Cliente	Servidor de Aplicaciones (Eduardo Ordoñez) 4	Servidor iSeries Produccion Bases de datos Coorporativa (Fernando Feijo) 3.2	Servidor SAN DATOS corporativos (Eduardo Ordoñez) 3.1	Servidor DNS y Directorio Activo (Eduardo Ordoñez) 2	Servidor DHCP (Eduardo Ordoñez) 1	Firewall Nokia y switches core (Diego Unkuch – Ingeniero de Sistemas DITEL)
	Recaudación		Raúl Romero Ingeniero de Sistemas	Johan Alvarado Jefe Dpto. Recaudación y Gestión de Cartera						
	Cartera									
	Contabilidad	Contabilidad	Sonia Bonilla Ingeniero de Sistemas	Martín Guacho Intendente de Contabilidad						
	Facturacion	SICO	Byron Sánchez Ingeniero de Sistemas	Diego Salamea Jefe Sección Facturación						
	Lecturas	Lecturas75								
	Consumos	ConsumosNuevo								
	Gestión Tributaria	Anexos Transaccionales	Iván Jara Ingeniero de Sistemas	Vicente Ortiz Analista Económico						
	Compras	Compras	Iván Jara Ingeniero de Sistemas	José Montero Intendente de Adquisiciones						

	Nomina	RRHH75FEB	Gabriel Goyo Ingeniero de Sistemas	Freddy Calle Analista de Remuneraciones						
		Sobretiempos								
	Atencion al Cliente	SAR	Dolores Peñafiel Ingeniero de Sistemas	Luis Guillen Jefe Dpto. Servicios al Cliente						
		SICO	Byron Sánchez Ingeniero de Sistemas							
		SRI	Enrique Palacios Ingeniero de Sistemas							
	Inventarios Contabilidad	Inventario Cliente Servidor	Iván Jara Ingeniero de Sistemas	Martín Guacho Intendente de Contabilidad						
	Inventarios Bodega	Inventario Intranet	Iván Jara Ingeniero de Sistemas	José Zuñiga Jefe Dpto. Administrativo (Enc.)						
		Antivirus	Eduardo Ordoñez Ingeniero de Sistemas							
		Correo Electrónico	Geovanny Barrera							

			Ingeniero de Sistemas							
		Sistemas Documentales	Geovanny Barrera Ingeniero de Sistemas							
		Página Web	Enrique Palacios Ingeniero de Sistemas		Servidor Blade Pagina Web (Eduardo Ordoñez) 5					

Líder de Equipo del Proceso de Negocio.

En cada equipo de recuperación debe definirse un Líder, quien debe ser una persona con liderazgo natural, y que tenga la capacidad para tomar decisiones durante el periodo de recuperación. Los líderes de los equipos de recuperación se asignan a cada uno de los procesos de negocios y deberán realizar, sin limitarse a las tareas siguientes:

- Participar en las sesiones de trabajo programadas para la evaluación de los riesgos e impactos del proceso bajo su responsabilidad.
- Aportar su conocimiento del proceso de negocios en el análisis y diseño de los procedimientos de recuperación.
- Liderar la recuperación del proceso de negocios a su cargo en los simulacros y prácticas, y en las situaciones reales.
- Identificar e implantar mejoras al plan de contingencia y a los procedimientos de recuperación bajo su responsabilidad.
- Servir de enlace entre el equipo de recuperación y el líder administrador de recuperación del proceso de negocio.
- Mantenimiento de la información del estado de recuperación
- Coordinar con otros equipos de recuperación.

Líder de Equipo de recuperación de los recursos de TICs.

Los líderes de los equipos de recuperación y sus suplentes deben contar con el perfil siguiente:

- Conocer profundamente el proceso de negocios bajo su responsabilidad.
- Poseer conocimientos de análisis y diseño de procesos de recuperación.
- Poseer un perfil psicológico que lo faculte para liderar grupos en catástrofes o bajo situaciones de alta tensión emocional.
- Tomador rápido y seguro de decisiones y hábil comunicador.
- Dedicar el tiempo que se requiera para a atender y ejecutar eficiente y oportunamente las labores que se le asignen en el proyecto.

Suplente del Líder de Equipo

El suplente sirve como Líder de Equipo, si el líder de equipo designado esta imposibilitado o no disponible para administrar el equipo. Por lo tanto, debe disponer del mismo perfil que el líder y cumplir con las mismas funciones.

Miembros de equipo

Los miembros de equipo son responsables de ejecutar las acciones de recuperación. Debido a que las actividades son usualmente desarrolladas por múltiples personas, quienes pueden variar dependiendo de las circunstancias y recursos disponibles, es mejor evitar la identificación de tareas con individuos específicos. En su lugar, la planeación se limita a experiencias y requerimientos específicos, los cuales son necesarios para realizar tareas particulares.

4.5. ACTIVACION DEL PLAN DE CONTINGENCIA

Se deberá establecer un protocolo de notificación oficial ante la ocurrencia de un desastre, además de establecer el nombre de la persona responsable por la activación de dicho protocolo a nivel de BCP.

Una vez que la notificación se ha hecho, el responsable activará al personal apropiado para realizar las actividades de soporte y recuperación.

Notificación Inicial

Los procedimientos de activación del plan serán realizados después que los planes iniciales de evacuación (BCP) y respuesta de emergencias han sido implantados. Estos procedimientos de activación del plan documentan la evaluación inicial, las decisiones y las actividades de activación de equipo que serán realizadas. Se deberá proveer la coordinación y comunicación centralizada de todas las respuestas al incidente. Específicamente, estos procedimientos incluyen la activación del personal de soporte apropiado, asistencia en el desarrollo de las recomendaciones de recuperación y en la activación de los equipos de recuperación tanto de los procesos de negocio como de los de tecnología.

Para el caso del área de TICs el flujo de notificación será el siguiente.

1. Notifique al departamento de Soporte y Operación de Servicios Informáticos.

1.1. Su nombre
1.2. Una descripción del evento
1.3. Un reporte preliminar de daños
1.4. Información relacionada con cualquier intento de notificación a los contactos
1.5. Un número telefónico y lugar donde puede ser localizado

La persona que recibe la notificación comunicará al CPC de la información antes mencionada.

Si es notificado después de horas o vía un escalamiento del problema, considere la información siguiente:

1. Fecha y hora de la notificación
2. Persona realizando la notificación
3. Descripción de la situación
4. Cualquier instrucción especial.

Verificación del desastre

Para la verificación del desastre deberá seguir las actividades siguientes:

1. Si el acceso a su área de trabajo está disponible, realice una inspección para evaluar el daño de los aspectos siguientes:

1.1. Equipo electrónico (Estado: destruido, fácil de recuperar, disponibilidad de uso).

1.2. Registros vitales: copias de archivos, manuales, documentación, etc. y datos en otros medios (computadoras personales, microfilm, etc.). Esto ayuda en determinar un plan de restauración o salvamento de recursos.

1.3. Equipo de oficina, trabajo en proceso, formulario, misceláneos. Analice el estado de operación en el momento del desastre e identifique la pérdida de datos críticos. Evalúe el impacto en las operaciones si los datos deben ser restaurados desde respaldos.

2. Obtenga una evaluación de daños en relación con lo siguiente:

2.1. Tiempos de recuperación del equipo electrónico (computadoras personales, terminales y equipo de comunicaciones)

2.2. Instalaciones físicas (condiciones ambientales, integridad de la estructura física, etc.)

3. Después de la inspección, el líder del equipo de recuperación debe reportarse al Centro de Operaciones de Emergencia (COE) para participar en una reunión de evaluación. En la evaluación del equipo utilice el formulario “Evaluar Estado de Equipo Crítico” que se incluye en el capitulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs”.

Establecer el COE

Basándose en los resultados de la verificación de daños, el CPC determinará si las circunstancias del incidente justifican la activación de los demás miembros del equipo y la notificación a las direcciones respectivas. Adicionalmente, basados en esas mismas circunstancias, se debe determinar la ubicación más recomendable para el Centro de Operaciones de Emergencias (COE). La determinación de la ubicación se hará con base en la información descrita en el documento “Ubicación del COE” que se incluye en el capitulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs”.

1. Contacte el lugar para el COE seleccionado y coordine el arribo del personal de soporte, así como del equipo de cómputo y los suministros.
2. Coordine la recuperación y entrega del material almacenado fuera de sitio hacia el COE.
3. Verifique que haya suficientes líneas telefónicas y teléfonos en operación.

Escalamiento de Notificaciones

1. Basado en la severidad de la situación, se deberá determinar lo siguiente:
1.1. El evento ha sido manejado apropiadamente y no se requieren notificaciones adicionales. Terminar situación de emergencia.
1.2. Las circunstancias del evento justifican notificaciones adicionales basado en lo siguiente:
1.2.1. El evento involucra daños a la propiedad y / o personas.
1.2.2. El evento involucra una interrupción potencial del negocio que excederá las horas de un día normal de trabajo.
2. Utilice el reporte "Composición de Equipos" que se incluye en el capitulo 6 "Procesos y Procedimientos del Plan de Contingencia de TICs" para notificar de las circunstancias del incidente a personal representativo de la organización. Suministre una breve descripción del incidente a los siguientes:
2.1. Coordinador del Plan de Continuidad
2.2. Encargado de TIC
3. Basándose en las circunstancias del evento se determinarán las acciones de respuesta inicial y el CPC dirigirá las actividades siguientes:
3.1. Si daños a personal han ocurrido, notifique a Recursos Humanos para que dirija los asuntos de notificación a los familiares y establezca las prioridades de la organización durante la crisis.
3.2. Si el acceso al edificio está permitido, inicie una inspección para evaluar los daños. Evaluar Estado de Equipo Crítico (este se utilizará luego de un evento de desastre) (PTC015)

Activación del equipo de recuperación

En cuanto el equipo administrador de la recuperación comunica la decisión de activar el Plan, el Líder debe notificar a todos los miembros del equipo.

1. Determine cuales miembros del equipo deben ser requeridos para realizar los procedimientos siguientes:
   1.1. Cumplir con los objetivos de recuperación
   1.2. Asistir en los esfuerzos de salvamento
   1.3. Asignación temporal para soportar otros departamentos.
   Para ello utilice el formulario Composición de Equipos (PTC006);
2. Elabore una lista del personal que es requerido en las actividades iniciales de la recuperación.
3. Obtenga un lugar para hacer una reunión informativa y preparar el equipo de recuperación. Para ello utilice el formulario Ubicación del Centro de Operaciones de Emergencia (COE) (PTC008);
4. Contacte a todos los miembros de equipo y provea la información siguiente:
   4.1. Identifique la ubicación designada para la reunión COE.
   4.2. Identifique los requerimientos de tiempo para preparar a los miembros de equipo. Utilice el formulario Tiempos Máximos de Interrupción

(PTC004) y Procedimientos de Recuperación para la plataforma de TIC que corresponda utilizar luego de la evaluación de los daños.

Sitio alterno de respaldo de datos

En el momento de la contingencia, el responsable de la recuperación de la información deberá determinar el sitio idóneo para la ubicación de los medios de respaldo de los datos del negocio, sea una localidad en el sitio (en el centro de datos de Centrosur) en caso que ella no se haya visto afectada, o bien una localidad fuera del sitio. Para esto se tiene, la información de localidades externas que se encuentra y deberá documentarse en el formulario "Sitio Alterno de Respaldo de Datos" que se incluye en el capitulo 6 "Procesos y Procedimientos del Plan de Contingencia de TICs".

Evaluación de Daños

El CPC conducirá una inspección en el sitio, con el objetivo de determinar la extensión del daño en las áreas afectadas. Representantes de las áreas afectadas, de seguridad y de tecnología de información deben estar presentes para determinar las condiciones del sitio, y de los equipos de cómputo.

1. En caso de que el edificio haya sido afectado por el evento contingente.

1.1. En caso necesario, obtenga autorización de las autoridades presentes (bomberos, policía, etc.) y envíe personal a las áreas afectadas del edificio.

1.2. Determine el equipo de emergencia que se requiere y adquiera los materiales necesarios para los miembros del equipo, basándose en las circunstancias de incidente. Considere, entre otros, los equipos siguientes:

1.2.1. Cascos y ropa de seguridad
1.2.2. Linternas
1.2.3. Cámara de video / fotografía instantánea o digital
1.2.4. Bloques de notas y lápices
1.2.5. Radios (Walkie-talkies)
1.2.6. Cualquier otro que considere necesario.

2. Brinde una charla resumida, previa a la inspección, al personal de la empresa que visitará las áreas afectadas.

2.1. Discuta la información disponible, tal como la causa, condiciones ambientales, tiempos, consideraciones especiales, etc.

2.2. Haga que el personal revise los procedimientos de seguridad.

3. Discuta los objetivos de inspección y utilice el formulario "Evaluar Estado de Equipo Crítico" (PTC015) que se incluye en el capitulo 6 "Procesos y Procedimientos del Plan de Contingencia de TICs".

4. Asigne objetivos de inspección a cada miembro del equipo de manera que se evalúen cuidadosamente los aspectos siguientes:

4.1. Comunicaciones
4.2. Sistemas
4.3. Equipo de Cómputo
4.4. Edificio (accesos y áreas de trabajo)

4.5. Medios de almacenamiento
5. Viaje al sitio del daño y evalúe la magnitud del mismo. Entre otros, considere el área y su contenido:
5.1. Estructura (interna y externa)
5.2. Accesibilidad dentro del edificio
5.3. Estado de las comunicaciones
5.4. Estado del cableado y conexiones de la red
5.5. Estado del servicio eléctrico
6. En caso necesario, trabaje con el contratista para elaborar un estimado de la reconstrucción de las áreas dañadas.

Elaborar las Recomendaciones de Recuperación

Elabore recomendaciones sobre cuales estrategias deberán ser desarrolladas, considerando para ello los resultados del proceso de evaluación de daños y cualquier otro aspecto especial que podrían incluir, entre otros, el tiempo en que ocurre el evento y regulaciones externas o propias del negocio (por ejemplo, el cierre de fin de mes o año fiscal). El CPC dirigirá a los Líderes de los equipos de recuperación en lo siguiente:

1. Elabore una lista de prioridades de recuperación de la plataforma, basándose en las Tiempos Máximos de Interrupción (TMI) establecidos según tabla incluida en el capitulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs”. Actualice esta lista con cualquier cambio necesario, considerando los recursos disponibles y requerimientos inmediatos de TI.

Revisar y Finalizar las Recomendaciones de Recuperación

1. El CPC evaluará el evento suscitado y determinará de inmediato la necesidad de actualizar el COE.
2. Si el COE no está disponible inmediatamente, entonces:
2.1. Coordine para determinar el tiempo estimado en el cual estará disponible.
2.2. Obtenga la identificación y el tiempo estimado de la duración de la interrupción de los servicios de Tecnología de Información.

Seguimiento del Evento de Contingencia.

El estado del evento y el reporte de las acciones de recuperación deben ser mantenidos por el CPC. Para realizar eso, algunas sugerencias se ofrecen a continuación:

1. Controle el estado del evento brindando seguimiento a las actividades de respuesta y recuperación del personal involucrado en las mismas. Considere, al menos, lo siguiente:
1.1. Tipo de evento

1.2. Áreas funcionales afectadas
1.3. Actividades planeadas
2. Documente la bitácora del avance de las tareas en secuencia cronológica. Utilice para ello el formulario "Resumen del Estado del Evento" (PTC014), en el capitulo 6 "Procesos y Procedimientos del Plan de Contingencia de TICs". El propósito de este reporte de estado es asistir el control y las comunicaciones. Es conveniente considerar la utilización de múltiples formularios para documentar actividades concurrentes.
2.1. Actividades de soporte y recuperación de Tecnología de Información
2.2. Actividades de restauración de las instalaciones (edificio) y/o del COE.
3. Brinde seguimiento apropiado para la pronta solución de asuntos que podrían obstaculizar la ejecución oportuna de tareas.
3.1. Asuntos de seguridad
3.2. Adquisición de recursos
3.3. Disponibilidad de los proveedores
3.4. Asuntos del personal

4.6. PLATAFORMA DE TIC CRÍTICA PARA LA CONTINUIDAD DEL NEGOCIO DE LA EMPRESA.

Orden de Recuperación	Recurso	Equipo Recuperación	TMI
1.1	Firewall Nokia	Equipo Comunicaciones	
1.2	Switches Core capa 3	Equipo Comunicaciones	
1.3	Servidor DHCP	Equipo Operaciones	
2.1	Servidor DNS y Directorio Activo	Equipo de Operaciones	
2.2	Servidor SAN DATOS corporativos	Equipo de Operaciones	
2.3	Servidor iSeries Produccion Bases de datos Coorporativa	Equipo de Operacioes	
3	Servidor de Aplicaciones	Equipo de Operacioes	

	Tiempos Máximos de Interrupción (PTC004)					CÓDIGO: PTC004 FECHA: EDICION:			
Área, Unidad de Proceso	**Funciones afectadas**	**Sist. Informac. de apoyo**	**Factor Riesgo**	**TMI Tiempo máximo de interrupción**	**TR Tiempo de recuperación**	**RPO Tiempo de actualidad de los datos**	**Criticidad (5 máxima - 1 mínima)**	**Fecha de Operabilidad Critica**	**Se puede crear un proceso alternativo en caso de contingencia?**
Comercialización	Facturación	SICO	O	72 h	5 h	8 h	5	Fin de mes	
	Lecturas	SICO	O	72 h	5 h	8 h	5		
	Consumos	SICO	O	72 h	5 h	8 h	5		
	Recaudación	SICO	F	72 h	5 h	8 h	5	Diaria	
	Cartera	SICO	F	72 h	5 h	8 h	5	Fin de mes	
Administrativo Financiero	Contabilidad	Contabilidad	L,O,F	120 h	8 h	8 h	4	Fin de mes	
	Gestión Tributaria	Anexos Transaccionales	L, F	120 h	8 h	8 h	4	Inicio de mes	
	Compras	Compras	O, F	120 h	8 h	8 h	3	Diaria	
	Inventario	Inventario	O	120 h	8 h	8 h	3	Diaria	Registro manual de egreso de materiales
Recursos Humanos	Nomina	RRHH75FEB	O, L	72 h	5 h	8 h	3	Inicio de mes	
	Sobretiempos		O, L	72 h	5 h	8 h	3	Inicio de mes	

Atención al Cliente	Atención al Cliente	SRI SAR SICO	I,O	72 h	5 h	8 h	4	Diaria	Registro de reclamos de forma manual
Toda la empresa	Correo Eléctrónico	LotusDominio	O	120 h	8 h	8 h	3		
	Sistemas Documentales	LotusDominio	O	120 h	8 h	8 h	3		Correspondencia: trámite con documentos impresos.
	Página Web	Servidor Web SICO	I	120 h	8 h	8 h	3		

4.7. MEDIDAS DE MITIGACION O RECUPERACION

CONTINGENCIA: INCENDIO.

CONTINGENCIA	Incendio o Fuego
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software Otros Equipamientos Instalaciones	Alto
RESPONSABLES DEL PLAN	
PLAN DE ACCION ASOCIADO	
1. Verificar que el sistema contra incendio esté operando. 2. Si se conoce sobre el manejo de extintores, intentar sofocar el fuego. Si este es considerable, no tratar de extinguirlo con los propios medios, solicitar ayuda. 3. Llamar a los números de emergencia. 4. Activar el sistema de alarmas. 5. Respetar los señalamientos de rutas de evacuación. 6. Si es necesario, utilizar lámparas emergentes con batería. 7. Asegurar que se tengan los respaldos externos 8. Cualquiera que sean los procesos que se estén ejecutando en los servidores, se deberá (si el tiempo lo permite) "Salir de Red y Apagarlos": Down en los servidores, apagar la caja principal de corriente. 9. Comunicar al Coordinador del Plan de Contingencia el evento ocurrido y proceder a activar el plan de Contingencia y los procedimientos de recuperación documentados.	

CONTINGENCIA: HUMEDAD O INUNDACION

CONTINGENCIA	Humedad o inundación
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software Otros Equipamientos Instalaciones	Alto
RESPONSABLES DEL PLAN	

PLAN DE ACCION ASOCIADO	
1. Apagar equipos de cómputo prioritarios. 2. Cubrir con bolsas de plástico servidores y documentos importantes que puedan mojarse. 3. Colocar los no-breaks sobre mesas 4. Colocar en lugares seguros el hardware, software y documentos importantes. 5. Determinar la causa del problema: Hardware, Software, conectividad. 6. Cuando se presenten problemas de hardware, se debe comprobar la disponibilidad del fluido eléctrico, se deben monitorear los indicadores de funcionamiento, se debe ejecutar un autosetup, etc. En caso de daño en los componentes, se debe coordinar con el proveedor para cambio, reemplazo o reparación de los mismos, y proceder de acuerdo al procedimiento de recuperación para la plataforma de TICs Hardware (PTC011), del capítulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs. 7. Cuando se presenten problemas de software, se deben revisar el Sistema Operativo, más aplicaciones, los procesos en las bases de datos, y otros procesos que intervengan en el funcionamiento de los sistemas corporativos. Para ello se deben de ayudar del mapa de dependencias de los sistemas corporativos que debe disponer la empresa y del procedimiento de recuperación para la plataforma de TICs Software (PTC012) de la aplicación que se necesita realizar la recuperación, incluida en el capítulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs. 8. Cuando se presentan problemas de conectividad, se debe comprobar la disponibilidad de los enlaces y accesos de red, de acuerdo a los parámetros de configuración del sistema corporativo que se esté analizando para ello se debe utilizar los formularios de recuperación para la plataforma de TICs Software (PTC012) de la aplicación que se necesita realizar la recuperación, incluida en el capítulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs.	

9. Cuando los procesos no pueden suspenderse, y la solución al daño de hardware o software requiere de un tiempo superior a 1 día se restituirá el servicio mediante un servidor alterno con software adecuado para ese servidor o se pondrá en ejecución un procedimiento manual para el proceso de negocio que soporte este sistema corporativo si el caso lo amerita (para esto se debe tener descrito con anterioridad el procedimiento manual utilizando el formulario Procedimiento Alterno de Trabajo PTC017).

CONTINGENCIA: SISTEMAS CORPORATIVOS FUERA DE SERVICIO

CONTINGENCIA	SISTEMAS CORPORATIVOS FUERA DE SERVICIO
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software Otros Equipamientos Instalaciones	Alto
RESPONSABLES DEL PLAN	
PLAN DE ACCION ASOCIADO	

1. Determinar la causa del problema: Hardware, Software, conectividad.
2. Cuando se presenten problemas de hardware, se debe comprobar la disponibilidad del fluido eléctrico, se deben monitorear los indicadores de funcionamiento, se debe ejecutar un autosetup, etc. En caso de daño en los componentes, se debe coordinar con el proveedor para cambio, reemplazo o reparación de los mismos, y proceder de acuerdo al procedimiento de recuperación para la plataforma de TICs Hardware (PTC011), del capítulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs.
3. Cuando se presenten problemas de software, se deben revisar el Sistema Operativo, más aplicaciones, los procesos en las bases de datos, y otros procesos que intervengan en el funcionamiento de los sistemas corporativos. Para ello se deben de ayudar del mapa de dependencias de los sistemas corporativos que debe disponer la empresa y del procedimiento de recuperación para la plataforma de TICs Software (PTC012) de la aplicación que se necesita realizar la recuperación, incluida

en el capítulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs. 4. Cuando se presentan problemas de conectividad, se debe comprobar la disponibilidad de los enlaces y accesos de red, de acuerdo a los parámetros de configuración del sistema corporativo que se esté analizando para ello se debe utilizar los formularios de recuperación para la plataforma de TICs Software (PTC012) de la aplicación que se necesita realizar la recuperación, incluida en el capítulo 6 “Procesos y Procedimientos del Plan de Contingencia de TICs. 5. Cuando los procesos no pueden suspenderse, y la solución al daño de hardware o software requiere de un tiempo superior a 1 día se restituirá el servicio mediante un servidor alterno con software adecuado para ese servidor o se pondrá en ejecución un procedimiento manual para el proceso de negocio que soporte este sistema corporativo si el caso lo amerita (para esto se debe tener descrito con anterioridad el procedimiento manual utilizando el formulario Procedimiento Alterno de Trabajo PTC017).

CONTINGENCIA: SUSPENSIÓN DEL SERVICIO DE INTERNET.

CONTINGENCIA	SUSPENSIÓN DEL SERVICIO DE INTERNET.
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software Otros Equipamientos Instalaciones	Alto
RESPONSABLES DEL PLAN	
PLAN DE ACCION ASOCIADO	
1. Determinar la causa del problema: conectividad, hardware, problema de configuración. 2. Cuando se presentan problemas de conectividad, se debe monitorear y comprobar que los enlaces con los proveedores estén funcionando. Si se ha producido la suspensión del servicio llamar al respectivo contacto para	

consultar el motivo de la falla del servicio.

3. Cuando los procesos no pueden suspenderse, y la solución al daño de conectividad requiere de un tiempo superior a 1 día se restituirá el servicio mediante un enlace alterno con otro proveedor.
4. Si el problema es hardware, se debe comprobar la funcionalidad del equipo, revisar sus respectivos indicadores para determinar la falla. Una vez identificado el componente afectado, coordinar con el proveedor el cambio, reemplazo o reparación del mismo. Se debe determinar si este servicio no se puede suspender por ningún motivo, se procederá a poner en funcionamiento un equipo alterno al dañado, para no afectar la disponibilidad del servico.
5. Si el problema es de configuración, revisar en el manual de configuración del servicio de internet y el diagrama actualizado de redes, y las memorias técnicas de las ultimas modificaciones realizadas, para identificar cuales han sido los cambios realizados para corregir la falla.

CONTINGENCIA: DAÑO EN UNA LINEA DE FIBRA OPTICA DEL BACKBONE DE LA INSTITUCION.

CONTINGENCIA	DAÑO EN UNA LINEA DE FIBRA OPTICA DEL BACKBONE DE LA INSTITUCION.
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Instalaciones	Alto
RESPONSABLES DEL PLAN	
PLAN DE ACCION ASOCIADO	

1. Determinar la causa del problema: Identificar en que parte se ha producido el daño.
2. Cuando se presentan problemas de conectividad, se debe monitorear y comprobar qué enlaces y áreas de trabajo han sido afectados, para ello se debe revisar el diagrama de red actualizado y revisar que tan grave es el daño.
3. Cuando los procesos no pueden suspenderse, y la solución al daño de conectividad requiere de un tiempo superior a 1 día se restituirá el servicio

mediante un enlace alterno. 4. Proceder a contactarse con el personal técnico o empresa especializada que repare el daño.

CONTINGENCIA: DAÑO EN UN EQUIPO DE COMUNICACION DEL BACKBONE DE LA INSTITUCION

CONTINGENCIA	DAÑO EN UN EQUIPO DE COMUNICACION DEL BACKBONE DE LA INSTITUCION**.**
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software Otros Equipamientos Instalaciones	Alto
RESPONSABLES DEL PLAN	
PLAN DE ACCION ASOCIADO	
1. Determinar si el daño es producto de deficiencias en la red eléctrica o un problema de hardware. 2. Si el problema es eléctrico se procede de acuerdo a la contingencia correspondiente. 3. Si el daño es de hardware y se cataloga como menor, se procede a reparar el equipo. 4. Si el daño es mayor se envía el equipo a reparación a una empresa especializada, y se lo reemplaza por un equipo temporal. Se procede a aplicar el procedimiento documentado de recuperación de infraestructura de TICs para comunicaciones y hardware respectivo.	

CONTINGENCIA: DAÑO EN EQUIPOS DE PCS DE USUARIO.

CONTINGENCIA	DAÑO EN EQUIPOS DE PCS DE USUARIO
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software Otros Equipamientos Instalaciones	Medio
RESPONSABLES DEL PLAN	

PLAN DE ACCION ASOCIADO
1. Usuario reporta a la Unida de Informática el problema, mediante el sistema de incidentes o help desk. 2. La Unida de Informática verifica si el daño es producido por hardware, software o conectividad. 3. Si el problema es por hardware se notifica a la empresa que alquila los equipos para que lo reemplace o haga la respectiva reparación. 4. Si es una falla de un componente del equipo y sus aplicaciones siguen funcionando normalmente entonces se procede a dar por terminada la contingencia. 5. En caso de no poder tener acceso directo al disco se procede a respaldar la información, se formatea el disco duro y se resinstala el software y los archivos de los usuarios. Para ello se utiliza los perfiles de configuraciones que corresponde al usuario afectado.

CONTINGENCIA: DAÑOS EN LAS BASES DE DATOS CORPORATIVAS

CONTINGENCIA	DAÑO EN LAS BASES DE DATOS CORPORATIVAS
FUENTES DE RIESGO	**ESTIMACION RIESGO**
Hardware Software	Medio
RESPONSABLES DEL PLAN	
PLAN DE ACCION ASOCIADO	
1. Determinar la causa del problema: hardware, configuración, instalación y datos. 2. Si el problema es hardware, se debe de revisar que los discos RAïD que se utilicen entren en funcionamiento para mitigar la contingencia. 3. Si el problema es de configuración, se deben verificar los parámetros de configuración y ajustar el motor de bases de datos de acuerdo al procedimiento documentado de recuperación y registrar una memoria técnica de los errores y problemas corregidos, durante el evento. 4. Si el problema es de instalación, se debe realizar la reinstalación del motor	

de bases de datos, y la recuperación de últimos respaldos de acuerdo al proceso de recuperación de la base de datos respectiva que se encuentra documentado. De igual manera generar una memoria técnica donde se registre las acciones y problemas que se presentaron durante la reinstalación que sirva para posibles soluciones en el futuro si se presenta algún evento.

5. Ante un problema de datos, se debe corregirlos directamente o mediante una modificación de los datos con procedimientos parametrizables. Para ello se debe actuar de acuerdo a la política de modificación o actualización de datos en las bases de datos que dispone la empresa.

CAPITULO 5:

5. ANALISIS COSTO-BENEFICIO

En este capítulo se pretende demostrar que la solución y los costos generados por su implementación, son justificables en función de las pérdidas económicas que se pueden generar por las fallas de seguridad corregidas en el presente proyecto.

5.1. COSTOS DE IMPLEMENTACION

Una vez que el sistema deja de funcionar la empresa puede tolerar como máximo un día sin que la información perdida se vuelva imposible de recuperar y la empresa empiece a asumir pérdidas por la falta de información. Aun cuando la información pueda ser recuperada esto también implica costos en cuanto a tiempo de trabajo de los empleados que deben cumplir horas extras para poder actualizar el sistema.

Al costo de pérdida de información también se debe agregar las horas laborales que el personal que depende íntegramente de la aplicación para realizar su trabajo, permanece inactivo pero que finalmente se pagan. Esto sucede especialmente en la parte administrativa donde la mayoría de procesos

se desencadenan de acuerdo al flujo de información de departamento a departamento.

Como costos de implementación se consideran los listados en la Tabla 5.1 donde se detallan los valores totales de un año de implementación tanto en equipos como en trabajo.

A estos costos hay que agregarles valores de mantenimiento de seguridad en los cuales hay que invertir durante toda la duración del proyecto, que actualmente se prevé será de mínimo dos años. Estos costos se detallan en la Tabla 5.1

RECURSO	Cantidad	Precio Unitario	COSTO
Pagos de sueldos de personas que asistan en la implementelación del plan	2	1100	26400
Extintores de incendio tipo C y colocación en puntos estratégicos cercano al centro de datos y area de informática	4	295	1180
Software para gestión del Sistema de detección de incendios para el centro de datos.	1	3000	3000
Archivadores de material ignifugo para documentación impresa, digital y respaldos local y en el centro de datos alterno	2	3500	7000
Comprar un firewall para redundancia del principal	1	5000	5000
Switches capa 3 para el bachbone 48 puertos que sirva como equipo alterno	1	2000	2000
La unidad de informática deberá disponer de un stock mínimo de componentes informáticos cuyo daño sea más frecuente (discos duros, monitores, unidades de CD/DVD, flash memory, ups).			2000
Local alternativo	1	73000	73000

Capacitación en Seguridad contra Incendios	20	50	1000
Sistema de Monitorización de Temperatura.	1	1500	1500
Sistema de detección de inundaciones autónomo	1	1600	1600
Cobertores para protección de equipos	15	20	300
Bolsas de Plástico para proteger documentos			
Desarrollar un plan de evacuación contra desastres naturales	1	5000	5000
Iluminación de emergencia en caso de una falla en la fuente de energía principal.	5	40	200
Sistema de Alarmas de seguridad de detección de apertura o rotura de puertas y ventanas para el Centro de Datos	1	2000	2000
Sistemas de control de acceso mediante dispositivos electrónicos al Centro de Datos	1	3000	3000
Los dispositivos y servidores situados fuera de los centros de datos o de computación o en las zonas departamentales deberán ser protegidos mediante armarios o racks cerrados con llave	1	3000	3000
Habilitar la ruta alternativa para la fibra Optica que se utiliza para la Red LAN.	1	5000	5000
Capacitación en Seguridad de Planes de Contingencia de TICs, al personal que se encuentra dentro del organigrama propuesto del Plan de contingencias diseñado.	12	1000	12000
		TOTAL	154180

Tabla 5.1. Tabla de Costos de Implementación

En la siguiente tabla se listan los costos de implementación del sitio alterno que se sugiere como una estrategia del plan de contingencias.

Recursos	Cantidad	Precio Unitario	Costo
Servidores	6	5000	30000
Firewall	1	5000	5000
Switches	2	2000	4000
Arriendo Local	12	1000	12000
Racks	1	10000	10000
Varios	1	12000	12000
		Total	73000

Tabla 5.2. Tabla de Costos de Sitio Alterno

5.2. JUSTIFICACION DE COSTOS

Como se puede demostrar a simple vista la pérdida de las bases de datos de toda la empresa causaría una pérdida económica mayor a la suma total del costo de implementación y mantenimiento de seguridad de los diferentes sistemas informáticos criticos. Ahora este es el peor escenario así que una relación más realista debe ir en función de si el centro de datos sufre un daño total, antes de la implementación de este proyecto, que son errores o pérdida de información esporádica en la base de datos y retrasos en el procesamiento de información por denegación de servicio de los servidores. La Tabla 5.3 muestra el costo anual de estos problemas en función también su frecuencia.

Problema	Costo		Frecuencia Anual	Costo Anual
Daños de Servidores total	15000	Los servidores críticos son 5	1	15000
Perdida de Datos	12000	Por un dia de trabajo de 8 horas de 300 personas, estimando la hora a $5.	1	12000
Daño del Firewall	5000	Unico firewall que se encuentra en el centro de datos	1	5000
Daño de	2000	Se tienen	1	2000

Switches backbone		actualmente 2 switches de 48 puertos que conectan a toda la red del edificio		
Swithes areas de trabajo	3500	Son siete switches para los 300 puntos.	1	3500
Rack y path panel centro de datos	5000		1	5000
Rack y patch panel areas de trabajo	10500	Cada piso tiene su rack y patch panel donde se conectan los puntos del area de trabajo en los 7 pisos y cada uno cuesta 1500	1	10500
Cableado al centro de datos	175	De cada piso se cablea al centro de datos son 7 pisos por $25 cada punto.	1	175
Cableado para las areas de trabajo	7500	Son 300 puntos a $25.	1	7500
Documentos, Manuales, Estudios, licencias de Software, Documentos de Consultorias.	20000		1	20000
Perdida de los códigos fuentes y ejecutalbes de los sistemas de información	60000		1	60000
Perdida de los Respaldos de datos	1728000	Si un dia de trabajo se pierde la información que equivale a $12000 si se	1	4320000

		perdiera la información de un año comercial 360 dias equivaldría a este costo.		
Perdida de ingresos por no disponer del Sistema de Recaudación	200000	Si un día se va el sistema para recaudación, dejarían de percibir la empresa en promedio $200.000	1	200.000
			TOTAL	2035275

Tabla 5.3. Tabla de Costos de Pérdidas por daños en activos críticos.

Una vez que se tiene identificados los costos de implementación y mantenimiento del proyecto de ejecución de este plan de contingencia, se aplica el método de Analisis costo beneficio, aplicando la respectiva relación de estos valores estimados.

Beneficios/costos= 2035275/154180=13.20

Al ser la relación Costo-beneficios positiva, permite con mayor convicción justificar que la implementación de este plan diseñado, como un proyecto a ejecutar, es beneficiosa para la empresa.

CAPITULO 6:

6. DEFINICIÓN DE PROCESOS Y PROCEDIMIENTOS

6.1. FORMATO DE LOS PRINCIPALES PROCESOS IDENTIFICADOS

El plan de continuidad a desarrollar, incluye en esta sección documentos que deberá preparar previo a la manifestación de un evento de interrupción,

mientras que otros documentos incorporados en esta Guía, serían utilizados después de la contingencia o evento de desastre o interrupción.

La información o documentos que deberá tener preparados previos a la manifestación de cualquier desastre y/o como parte del plan de continuidad son los siguientes:

- Carátula de Plan de Continuidad de la Gestión de TIC.
- Control de revisión y aprobación del documento (PTC000).
- Información de la Unidad (PTC001, PTC002);
- Inventario de hardware y software (PTC003);
- Tiempos Máximos de Interrupción (PTC004);
- Organización para la Continuidad (PTC005);
- Composición de Equipos (PTC006);
- Información de Contactos Externos (PTC007);
- Ubicación del Centro de Operaciones de Emergencia (COE) (PTC008);
- Sitio alterno de respaldo de datos (PTC009);
- Memoria Tecnica (PTC010)
- Procedimientos de Recuperación para la plataforma de TIC Hardware (PTC011);
- Procedimientos de Recuperación para la plataforma de TIC Software (PTC012);
- Procedimientos de Recuperación para la plataforma de TIC Comunicaciones (PTC013);
- Resumen del Estado del Evento (este se utilizará luego de un evento de desastre) (PTC014);
- Evaluar Estado de Equipo Crítico (este se utilizará luego de un evento de desastre) (PTC015).
- Perfil de Configuración de Usuarios (PTC016).
- Procedimiento Alterno de Trabajo (PTC017).

	CONTROL DE LLENADO DE MATRICES	FECHA LLENADO
Control de revisión y aprobación del documento (PTC000).		
Información de la Unidad (PTC001, PTC002);		
Inventario de hardware y software (PTC003);		
Tiempos Máximos de Interrupción (PTC004);		
Organización para la Continuidad (PTC005);		
Composición de Equipos (PTC006);		
Información de Contactos Externos (PTC007);		
Ubicación del Centro de Operaciones de Emergencia (COE) (PTC008);		
Sitio alterno de respaldo de datos (PTC009);		
Memoria Técnica (PTC010)		
Procedimientos de Recuperación para la plataforma de TIC Hardware (PTC011);		
Procedimientos de Recuperación para la plataforma de TIC Software (PTC012);		
Procedimientos de Recuperación para la plataforma de TIC Comunicaciones (PTC013);		
Resumen del Estado del Evento (este se utilizará luego de un evento de desastre) (PTC014);		
Evaluar Estado de Equipo Crítico (PTC015).		
Perfil de Configuración de Usuarios (PTC016).		
Procedimiento alterno de trabajo. (PTC017).		

Este es el formulario que servirá como registro de control para el procedimiento de revisión del Plan de Contingencia.

La versión del documento, el autor del Plan de Contingencia, la fecha de la revisión y el número de la revisión, el responsable de la revisión la firma y la fecha de la revisión. En la siguiente parte del formulario se encuentra el control de los ensayos realizados sobre el plan de contingencia vigente.

	Control de revisión y aprobación del documento		**CÓDIGO: PTC000**
			FECHA:
			EDICION:

HISTORIAL DE REVISIONES			
Versión	**Autor**	**Fecha**	**Revisión**

CONTROL DE REVISIONES			
	Responsable	**Firma**	**Fecha de Aprobación**
1			
2			
3			
4			
5			

CONTROL DE ENSAYOS			
	Responsable	**Fecha**	**Resultados**
1			
2			
3			
4			
5			

El siguiente formulario sirve para registrar los datos de las diferentes Unidades Organizativas de la empresa. Que servirán para en el caso de una contingencia documentar quien es el líder de la Unidad Organizativa, que ayudará al equipo de TI a apoyar en el proceso de recuperación. Estas personas tanto el líder como el suplente son quienes deben ayudar a coordinar el proceso de

recuperación. Para mostrar como se registra este formulario se muestra el siguiente ejemplo.

	Información de la Unidad (PTC001, PTC002)	CÓDIGO: PTC001
		FECHA:
		EDICION:

Nombre de la Unidad	DICO
Dirección	Max Uhle
Ciudad	Cuenca
Número de teléfono	Ext 2190
Unidad programática	Dpto. Recaudación y Gestión de Cartera

LIDER: persona a cargo de gestionar la crisis y será el portavoz de la unidad en caso de emergencia.(PTC002)

Nombre Contacto Primario de Emergencia	Johan Alvarado Jefe Dpto. Recaudación y Gestión de Cartera
Numero de Telefono	
Numero Alternativo	
Correo Electrónico	
Unidad programática	

SUPLENTE: En caso que el funcionario anterior no esté disponible, será relevado por:

Nombre Contacto Secundario de Emergencia	
Numero de Telefono	
Numero Alternativo	
Correo Electrónico	
Unidad programática	

En el siguiente formulario se tiene lo referente al inventario de los activos, es decir, se debe ingresar los datos de todos los activos críticos para la continuidad del negocio.

	INVENTARIO DE ACTIVOS DE TICS	CÓDIGO: PTC003
		FECHA:
		EDICION:

Codigo del Activo	Tipo	Descripcion	Fecha ingreso	Ubicación Fisica	Documento de Especificaciones Técnicas	Prioridad	Area/Departamento	Estado del activo (Operativo, mantenimiento, dado de baja)	Uso del Activo (desarrollo,pruebas, produccion,monitoreo)	Responsable del funcionamiento del Activo	Proveedor	Fecha Ultimo Mantenimiento	Procedimiento de Configuración	Parámetros/Criterios de Funcionamiento	Memoria Tecnica ultimo Mantenimiento	Fecha de Operabilidad Critica
Ser001	HW	Servidor de Directorio Activo	15-06-2001	Centro de Datos Principal	DocEsp010	5	DISI	Operativo	Producción	Eduardo Ordoñez	IBM		Conf015	Conf015 192.168.100.17	Mem057	Diaria

Prioridad

5= Muy Alto: La ausencia de dicho hardware o software para interrumpe toda la operación de la Empresa
4= Alto. La ausencia de dicho hardware o software para interrumpe algunos procesos de la Empresa
3= Medio: La ausencia de dicho hardware o software para interrumpe varios usuario con un TMI con una ventana de tiempo corto.

2= Bajo: La ausencia de dicho hardware o software para interrumpe un usuario con un TMI con una ventana de tiempo amplio.

Este formulario sirve para registrar los datos de los tiempos máximos de interrupción que cada uno de los procesos de negocio, pueden aceptar antes que esto se convierta en un problema grave para la empresa, en los cuales los recursos de TICs son los que afecten la continuidad de estos procesos.

Los factores de riesgos se pueden clasificar en aspectos Operativos (O), Imagen (I), Legales (L) y Regulatorios (R).

La definición del TMI y del RPO se puede hacer en minutos, horas, días, etc. Esta definición es la que permitirá priorizar el orden de ejecución de los procesos de recuperación.

	Tiempos Máximos de Interrupción (PTC004)					CÓDIGO: PTC004		
						FECHA:		
						EDICION:		
Área, U.P.	**Funciones afectadas**	**Sist. Informac. de apoyo**	**Factor Riesgo**	**TMI**	**TR**	**RPO**	**Criticidad**	**Fecha de Operabilidad Critica**
Comercialización	Facturación	SICO	O	72 h	5 h	24 h	5	Fin de mes
Comercialización	Lecturas	SICO	O	24 h	5 h	24 h	5	
Comercialización	Consumos	SICO	O	72 h	5 h	24 h	5	
Comercialización	Recaudación	SICO	F	4 h	5 h	24 h	5	diaria
Comercialización	Cartera	SICO	F	24 h	5 h	24 h	5	Fin de mes
Administrativo Financiero	Contabilidad	Contabilidad	L,O, F	24 h	3 h	24 h	3	
Administrativo Financiero	Gestión Tributaria	SRI_IVA	L	72 h	2 h	24 h	2	Inicio de mes
Administrativo Financiero	Compras	Compras	F	24 h	150 min		3	
Recursos Humanos	Nomina	RRHH75 FEB	O	72 h	150 min	24 h	3	Inicio de mes
Atención al Cliente	Atención al Cliente	Reclamos 75 SICO	I,O	48 h	150 min	24 h	3	
Toda la empresa	Correo Eléctrónico	LotusDominio	O	24 h	4 h	24 h	4	
Toda la empresa	Sistemas Documentales	LotusDominio	O	24 h	4 h	24 h	4	
Toda la empresa	Página Web	Servidor Web	I	24 h	2 h	24 h	3	

		SICO						

En el siguiente formulario, se tienen establecidas las diferentes funciones que se realizan en el Area de TICs en la empresa, y qué unidades organizativas son responsables de llevarlas a cabo. Con el fin de poder realizar un seguimiento de las estrategias de prevención que se han seleccionado para implementar en este plan.

	Organización para la continuidad del Negocio	CÓDIGO: PTC005
		FECHA:
		EDICION:
UNIDAD	**FUNCION GENEREAL**	
Dirección de Telecomunicaciones DITEL	Mantener y monitorear los servicios de red	
Departamento de Soporte y Operación de Servicios Informáticos	Mantenimiento y reparación de computadores y equipo tecnológico (hardware).	
Departamento de Soporte y Operación de Servicios Informáticos	Vigilar por el buen funcionamiento de los servidores	
Departamento de Desarrollo y Mantenimiento de Sistemas de Información	Desarrollar e implementar las necesidades de los usuarios en los sistemas de Información. Esto incluye la responsabilidad de asignar los permisos de acceso al personal de desarrollo, al ambiente operacional o viceversa.	
Departamento de Operación y Soporte de Servicios Informáticos	Verificar y garantizar el correcto funcionamiento de los sistemas implementados. Esto incluye, asegurar que la documentación de operación y procedimientos de usuario sean cambiados según sea necesario para seguir siendo apropiados	
Departamento de Desarrollo y Mantenimiento de Sistemas de Información	Responsable de copias de seguridad de la información critica de la empresa.	
Departamento de Operación y Soporte de Servicios	Autorizar y Verificar los permisos de acceso de los usuarios a las diferentes redes, servicios y sistemas de información.	

Informáticos	
Departamento de Desarrollo y Mantenimiento de Sistemas de Información	Responsable de la documentación crítica del sistema (impresa y medios digitales).
Departamento de Servicios Generales	Responsable de verificar que se realice el mantenimiento de las redes eléctricas y equipos de suministro eléctrico (placas de pared, supresoras de picos, estabilizadoras de voltaje, ups, extensiones eléctricas).
Departamento de Desarrollo y Mantenimiento de Sistemas de Información	Responsable del software de la organización, incluyendo la biblioteca de fuentes y los códigos ejecutables de los sistemas informáticos.

Tabla 6.1 Estructura Orgánica del DISI propuesta.

Este formulario se deberá llenar con los datos de las personas que formarán el equipo para recuperar el área de negocio afectada como por ejemplo el proceso de comercialización y que se encuentren disponibles durante el momento de la contingencia.

	Composición de Equipos				CÓDIGO: PTC006
					FECHA:
					EDICION:
Equipo de UP.	**Nombre del Empleado**	**Rol**	**Dirección**	**Celular**	**Teléfono**
Recuperación de Facturación	Eduardo Ordoñez	Equipo de Operaciones de los Servidores (EO)			
	Byron Sánchez	Lider del Equipo de Aplicaciones (EA)			
	Jaime Campos	Lider Equipo Comunicaciones (EC)			

Cuando ocurre un desastre de grandes proporciones se necesitará registrar información de entidades externas que ayuden a solucionar o recuperar las operaciones de la empresa. Como son: Policia, Bomberos, Cruz Roja, Hospitales, Proveedores de Equipos, Proveedores de Servicios Públicos, Proveedores de Sotware de Aplicaciones, Proveedores de sitios alternos, Proveedores donde se guardan los respaldos y documentación crítica del negocio, Proveedores de Cableado, Contratistas que evalúen el estado estructural del edificio. El siguiente formulario sirve para este propósito y se muestra un ejemplo.

FORMATO DE INFORMACION DE LOS PRINCIPALES PROVEEDORES DE HARDWARE/SOFTWARE/SERVICIOS DE TICs

	Información de Contactos Externos		CÓDIGO: PTC007
			FECHA:
			EDICION:
Compañía	Autelcom		
Tipo (Servicio,Hardware,Software)	Hardware		
Tel. Cía.	2841595		
Fax Cía.	2837118		
Dirección Cía.	Gran Colombia 21-51 y Unidad Nacional		
E-mail Cía.	ventas@autelcom.net		
Activo al que provee	Equipos de redes y cableado.		
Contactos	**E-mail**	**Teléfono**	**Celular**
Mauricio Tello	mauricio_tello@autelcom.net		099851981

Cuando ocurre un desastre se debe tener definido el lugar en donde el equipo de recuperación se reunirá para poder implementar el centro de emergencia de operaciones, desde donde podemos gestionar y realizar los procesos de recuperación, sea dentro del mismo edificio de la empresa o si no se tiene acceso, se tendrán registrados otras alternativas. Para ello se utilizará el siguiente formulario.

	Ubicación del Centro de Operaciones de Emergencia	CÓDIGO: PTC008
		FECHA:
		EDICION:
SITIO No. 1		
Ubicación:		
Dirección:		
Teléfonos:		
Contactos:		
#1	Nombre:	
	Puesto:	
	Rol:	
	Tel. Hab.:	
	Tel. Celular:	
	Beeper:	
	Dirección:	
#2	Nombre:	
	Puesto:	
	Rol:	
	Tel. Hab.:	
	Tel. Celular:	
	Beeper:	
	Dirección:	

En el siguiente formulario, documente los datos de los lugares donde se almacenan los respaldos de datos y cualquier otra información sea digital o

impresa crítica, en los sitios de respaldo. Se muestra un ejemplo de cómo se debe registrar este documento. (PTC009)

	REGISTRO DE COPIAS DE RESPALDO DE LOS SISTEMAS DE INFORMACION	CÓDIGO: PTC009
		FECHA:
		EDICION:

Sitio Alterno de Respaldo de Datos										
SITIO No. 1										
Ubicación:										
Direcciòn:										
Telefono:										
Contacto:						Telefono:				
Sistema de Información	Código de Identificación	Tipo de Respaldo	Periodicidad del Respaldo	Medio de almacenamiento	Persona que lo genera	Fecha de Realización	Fecha de Prueba del respaldo	Tipo Ubicación	Nro de Copias	Proceso de restauración
SICO	Sico-01012011	Diferencial, Incremental, Completo	Diario, Semanal	Cinta, DVDs				Local, distribuidad, Entidad Externa	2	
OBSERVACIONES:										

En este formulario se registra los datos de la memoria técnica de los procesos de mantenimiento y actualización de los equipos y sistemas de información.

	Memoria Técnica	**CODIGO: PTC010**
		FECHA:
		EDICION:

Nro Documento	Men-075	**Fecha**	29/03/2011	**Hora**	18:00 pm	
Nombre del Software						
Tipo de Software						
Estudio de Impacto del cambio						
Responsable ejecución del cambio						
Responsable Autorización						
Documento de Autorización						
Motivo/Justificación						

Tareas Realizadas	**Errores /Fallos presentes durante la aplicación del Cambio**
1. Bajar base de datos	
2. Sacar respaldo	

Este formulario, sirve para documentar el procedimiento de recuperación de equipos servidores críticos para el negocio. A continuación se presenta un ejemplo de cómo se debe registrar la información.

	Procedimiento de Recuperación Equipos	CÓDIGO: PTC011
		FECHA:
		EDICION:

Nombre del Hardware	Servidor de Correo
Objetivos:	Documentar la información requerida para recuperar el funcionamiento del equipo que soporta el servicio de correo de la empresa CentroSur
Distribución	Ing. Fabiola Mora (Lider del Equipo de Aplicaciones), Eduardo Ordoñez (Lider del Equipo de Operaciones).
TMI (RTO)	40 min
Integrantes del Equipos de Recuperación	
Lider del Equipo	

Principal	Eduardo Ordoñez (Lider del Equipo de Operaciones).	
Suplente		
Miembros del Equipo		
	Principal	**Suplente**
Miembro Nº1	Ing. Fabiola Mora (Lider del Equipo de Aplicaciones)	
Miembro Nº2	Ing. Eduardo Ordoñez (Lider del Equipo de Operaciones).	
Miembro Nº3	Ing. Jaime Campos (Lider del Equipo de Comunicaciones)	
Miembro Nº4		
Miembro Nº5		
Miembro Nº6		
Información general del hardware		
Marca y modelo	pSeries	
Dirección IP	192.168.10.18	
Procesadores		
Sistema Operativo: Aix		
Versión	5.3	
Parches		
Base de datos		
Versión	Lotus Dominio	
Parches		
Discos Duros		
Especificación técnica	SCSI 500 GB, SAS (Serial Attached SCSI; SCSI: Small Computer SystemInterface), con la capacidad de expansión de dos discos duros hot swap.	
Área de SWAP		
Tarjetas controladoras	SAS	
Tarjeta de red		
Especificación técnica	3com Gigabit Ethernet, conectores RJ45	
Redundancia	Si. Dos tarjetas de red	
Memoria		
Cantidad	4 GB	
Tolerancia a fallos (ECC memory)	No soporta esta tecnologia	
Fuente de poder		
Especificación técnica	ATX	
Redundancia	Si	

Unidad de respaldo	
Marca y modelo	
Tipo de cinta	
Software usado	
Garantía de fábrica	
Proveedor y contacto	
Fecha de Vencimiento	
Contrato de mantenimiento	
Proveedor y contacto	
Fecha de vencimiento	
Otros	

Recuperación del hardware		
Acciones requeridas previo o durante el proceso de recuperación		
Accion	**Parámetros de Configuración**	**Tiempo**
Instalar Sistema Öperativo AIX	Instalación por defecto	15 min
Configurar Interfaces de Red	Eth0 IP=192.168.10.18 Mascara=255.255.255.0 Gateway=192.168.10.10 Eth1 IP= 192.168.10.23 Mascara=255.255.255.0 Gateway=192.168.10.10 DNS= 192.168.10. 222	5 min
Asignar un nombre al equipo	[BASH]# Hostname=mail	
Procedimientos de validación y sincronización con otros equipos		
Accion	**Parámetros de configuración**	**Tiempo**
Verificar que se encuentra conectado a la red	Ping 192.168.10.10	20 s
Verificar que se encuentra conectado correctamente con el firewall de la empresa	Ping 192.168.10.10	20 s
Verificar que el servidor DNS se encuentra operando y que resuelve el nombre del servidor	Ping 192.168.10.222	20 s
Verificar que el firewall tiene correctamente configurado el acceso al servidor de correo		5 min

desde el exterior		
Procedimientos para regreso al sitio principal		
Accion	**Completado S/N**	**Tiempo**
Otros procedimientos posteriores al evento		
Accion	**Completado S/N**	**Tiempo**

Contactos requeridos (empleados involucrados con el equipo, proveedores, etc.)

Empresa	**Nombre de Referencia**	**Teléfono**	**Celular**
Autelcom	Ing. Tello	2837118	099851981

Observaciones

Luego que el hardware ha sido recuperado, se procede a aplicar la recuperación del Software de aplicaciones. Para ello se utilizará el formulario de recuperación de software que se presenta a continuación. Con un ejemplo de cómo se debe ingresar la información.

	Procedimiento de Recuperación Sistemas de Información o Aplicación.	CÓDIGO: PTC012
		FECHA:
		EDICION:

Nombre del Software	Sendmail	**TMI (RTO)=** 120 min
Objetivos:	Documentar la información requerida para recuperar el funcionamiento del servicio de correo de la empresa CentroSur	
Distribución	Ing. Fabiola Mora (Lider del Equipo de Aplicaciones), CPC (Coordinador de Plan de contingencia).	
Integrantes del Equipo de Recuperación		

Lider del Equipo		
Principal	Ing. Fabiola Mora (Lider del Equipo de Aplicaciones)	
Suplente		
Miembros del Equipo		
	Principal	**Suplente**
Miembro Nº1		
Miembro Nº2		
Miembro Nº3		
Miembro Nº4		
Miembro Nº5		
Miembro Nº6		
Información general de la aplicación		
Versión en Producción	5.0	
Sistema Operativo		
Versión	AIX 5.1	
Parches		
Plataforma Base		
Servidores	Servidor de Correo	
Equipos de Comunicación	Firewall	
Enlaces	Gigabit Ehernet	
Otros		
Garantía de fábrica		
Proveedor y contacto		
Fecha de Vencimiento		
Contrato de mantenimiento		
Proveedor y contacto		
Fecha de vencimiento		

Recuperación de la aplicación				
Recursos requeridos previo o durante el proceso de recuperación				
Id	**Recurso**	**Responsable**	**Ubicación**	**Tiempo**
1	Cinta con respaldo de datos	Ing. Fabiola Mora	Entidad Externa	40 min

Instalación de la aplicación		
Accion	**Parámetros de configuración**	**Tiempo**
Instalar el paquete de sendmail	[BASH]# yum install -y sendmail sendmail.cf dovecot cyrus-sasl cyrus-sasl-plain cyrus-sasl-md5 make m4	20 min
Instalar el paquete squirrelmail		20 min

Procedimientos y parámetros para configurar la aplicación		
Accion	**Parámetros de Configuración**	**Tiempo**
Configuracion del fichero --> /etc/mail/access#	#IP Publica de su Servidor de correo Connect: 207.249.24.30 RELAY #Nombre de su Dominio Connect: midominio.com.mx RELAY #Nombre de su Equipo Connect: correo.midominio.com.mx RELAY #IP Local de su Servidor de correo Connect: 192.168.1.10 RELAY	15 min
Configuracion del fichero --> /etc/mail/local-host-names#	correo.centrosur.com.ec centrosur.com.ec	1 min
Configuracion del fichero --> /etc/mail/relay-domains#	correo.centrosur.com.ec centrosur.com.ec	1 min
Configuracion del fichero --> /etc/mail/sendmail.mc#	DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl	2 mim

Otros procedimientos posteriores al evento	
Accion	**Tiempo**
Crear cuentas de los usuarios	60 min
Proceder a restaurar los datos del servidor de correo	60 min

Contactos requeridos (empleados involucrados con el equipo, proveedores, etc.)

Empresa	**Nombre de Referencia**	**Teléfono**	**Celular**

Observaciones

En este formulario, sirve para documentar el procedimiento de recuperación de equipos de comunicaciones.

	Procedimiento de Recuperación Comunicación	CÓDIGO: PTC013
		FECHA:
		EDICION:

Nombre del Hardware	
Objetivos:	
Distribución	

Integrantes del Equipos de Recuperación		
Lider del Equipo		
Principal		
Suplente		
Miembros del Equipo		
	Principal	**Suplente**
Miembro Nº1		
Miembro Nº2		
Miembro Nº3		
Miembro Nº4		
Miembro Nº5		
Miembro Nº6		
Información general del hardware		

Marca y modelo				
Dirección IP				
Sistema Operativo				
Versión				
Parches				
Puertos				
Tipo	Cantidad			
Memoria				
Cantidad				
Tolerancia a fallos (ECC memory)				
Fuente de poder				
Especificación técnica				
Redundancia				
Garantía de fábrica				
Proveedor y contacto				
Fecha de Vencimiento				
Contrato de mantenimiento				
Proveedor y contacto				
Fecha de vencimiento				
Otros				
Recuperación del hardware				
Recursos requeridos previo o durante el proceso de recuperación				
ID	**Recurso**	**Ubicación**	**Responsable**	
Parámetros de Configuración de Interfaces				
Interfaz	**Equipo con el que se conecta**	**Interfaz de conexión**	**Descripción**	**Parámetros de Configuración de la Interfaz**

Procedimientos para instalar y configurar el equipo de comunicación. Cuando aplique, incluya versiones de sistema operativo y parches	
Accion	**Tiempo**

Procedimientos de validación y sincronización con otros equipos	
Accion	**Tiempo**

Procedimientos para regreso al sitio principal	
Accion	**Tiempo**

Otros procedimientos posteriores al evento	
Accion	**Tiempo**

Contactos requeridos (empleados involucrados con el equipo, proveedores, etc.)

Empresa	**Nombre de Referencia**	**Teléfono**	**Celular**

Observaciones

Este formulario es utilizado para realizar el seguimiento del estado del evento o contingencia a la que se está enfrentando para poder en base a esto el CPC,

puede dar información respecto a la situación del mismo, y como se desarrolla el procesos de recuperación.

	Resumen del Estado del Evento			CÓDIGO: CODIGO:PTC0014
				FECHA:
				EDICION:
Nombre del Incidente		**Lugar**		
Nombre de la persona que reporta				
Actividad	**Procedimiento Aplicado**	**Resultado/Estado**	**Fecha preparado (fecha y hora)**	

Este formulario es utilizado cuando se realiza la evaluación de los daños causados por una contingencia, para envase a esto activar el Plan de mitigación o recuperación.

	Evaluar el Estado del Equipo de TIC		CÓDIGO: PTC0015
			FECHA:
			EDICION:
Lugar:		Nombre del Evento	
Equipo	**Condición**	**Tiempo de Rescate**	**Comentarios**

Leyenda		
Condición:	ND	No dañado
	DPU	Dañado pero Utilizable
	DRU	Dañado requiere rescate antes de utilizar
	DRC	Dañado requiere reconstrucción

Este formulario permite registrar los datos de configuración de los equipos de los usuarios que son críticos para la continuidad del negocio. A continuación el formulario con un ejemplo de cómo llenarlo.

	Ficha De Perfiles De Usuario	Código: PTC016
		Edición:
		Fecha:

DENOMINACIÓN DEL PUESTO:

OPERADORES

USUARIO:

DEPARTAMENTO/AREA:

☐	Compras	■	Contabilidad / Finanzas
☐	Comercial / Atención al cliente	☐	RR.HH. / Administración
☐	Calidad	☐	Mantenimiento & Almacén
☐	Logística externa	☐	Logística interna
☐	Producción	☐	Cambio de utillajes, ajuste de máquinas
☐	Diseño del proceso	☐	

APLICACIONES:

- Microsoft Office 2003
- Antivirus F-Security
- Internet Explorer
- Navegador Mozilla FireFox.
- Adobe Reader
- Winzip.

.

APLICACIONES CORPORATIVAS:

- Sistema Administrativo Financiero
- Sistema Documentales y Correo Electrónico

APLICACIONES ESPECIALES:

- Anexos Transaccionales del SRI
- JInitiator de JAVA

CONFIGURACIONES DE RED

- Direccionamiento IP:
  - Estático
    - Dirección IP:
    - Mascara:
    - Puerta de enlace:
    - DNS 1:
    - DNS 2:
  - DHCP
- **Nombre del Host:**
- **Dominio:**
- **Grupo de Trabajo:**

PERMISOS DE ACCESO A LOS SERVICIOS DE RED

PERMISOS DE ACCESO A LOS SISTEMAS CORPORATIVOS

No requerida
IMPRESORAS INSTALADAS
• **Impresoras tipo local:** o HP Color LaserJet 2600n • **Impresoras de red:** o HP Color LaserJet 5500n

OBSERVACIONES:	Firma: Fecha: __/__/__

Cuando una contingencia se presenta algunos procesos de negocio pueden seguir operando manualmente, sin recursos de TICs. Dando una ventana de tiempo hasta que el equipo de recuperación lo restaure.

	Procedimiento Alterno de Trabajo	CÓDIGO: PTC0017
		FECHA:
		EDICION:

Unidad de Negocio				
Nombre del Procedimiento				
Fecha de Aprobación				
Procedimientos relacionados				
Objetivos				
Responsable				
Recursos Criticos	Personal			
	Nombre	Rol	Telefono	
	Equipo de Comunicaciones			
	Equipo de Oficina			
	Formularios y documentos			

	Otros recursos		
Detalle del Procedimiento	Acciones en orden secuencial	Responsable	Recursos
Actividades a desarrollar luego de la restauración de TIC	Acciones en orden secuencial	Responsable	Recursos
Notas			

CAPITULO 7:

7. CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

En esta sección, se listan a continuación, las conclusiones a las cuales se ha llegado, luego de desarrollar este tema de tesis sobre el plan de contingencias de TICs.

- Debe entenderse que los riesgos identificados en este análisis, únicamente deberán ser considerados para preparar una estrategia de mitigación de riesgos previo a cualquier interrupción o desastre. No serán utilizados para estrategias o acciones durante o después de un evento que provoque la interrupción de los servicios.

- La elaboración de un plan detallado para la recuperación de los sistemas y procesos críticos del negocio, debe ser una guía de implementación, es decir, responder el “que hacer”, no el “como hacerlo”.

- Los cambios de las tecnologías disponibles, hacen que un proceso de planeación de contingencia sea extenso e intenso, al mismo tiempo que este dinamismo, complica su realización, dada la necesidad de incluir una ingente y siempre creciente cantidad de detalles que hay que tener en cuenta para cada configuración y arquitectura de aplicaciones particular.

- En nuestro país el area de seguridad, específicamente planes de contingencia y análisis de riesgos es un tema que todavía es nuevo y que muchas empresas no le dan el valor que realmente tienen en el funcionamiento de sus operaciones.

- El objetivo del plan no es evitar los riesgos en su totalidad, sino minimizar el impacto que las incidencias podrían producir en la organización.

- Los recursos o activos críticos de una organización sin duda son establecidos en base al RTO o tiempo máximos de interrupción TMI que una organización puede aceptar en base a sus requerimientos de negocio y requerimientos de recuperación.

- Actualmente existen algunas aplicaciones de misión crítica que permiten monitorear la infraestructura de una organización mediante la agregación de modulos de los diferentes subsistemas, gracias a sus

diseños modulares, ayudando a monitorear y tomar decisiones que ayuden a prevenir las amenazas sobre los activos críticos de TICs de la empresa.

- Los Planes de Contingencia establecen la respuesta qué se debe hacer en situaciones de emergencia. Su implementación se realiza mediante documentos genéricos (definición de los escenarios y gestión de las contingencias, desarrollo de simulacros) y se materializa en procedimientos individuales que se adaptan a cada instalación.

- El análisis de riesgos realizada para el diseño de este plan de contingencia es una base importante para la planificación e implementación del SGSI para la empresa, en donde se analiza el negocio para determinar los activos más importantes, las amenazas y vulnerabilidades que pueden generar, los cuales serán gestionados con controles apropiadamente implementados y criterios establecidos.

- Dentro de la estructura orgánica del área de TICs, se debe de reflejar los cargos y roles minimos necesarios para mantener el SGSI vigente, de lo contrario, los controles y estrategias de prevención y mitigación quedarán obsoletas.

- Es primordial que el tema de seguridad esté incluido dentro de las políticas y normativas de la empresa para que generen la obligatoriedad de aplicar los controles y estrategias sugeridas, de lo contrario, la seguridad quedará a criterio y voluntad del personal que en ese momento labore en la empresa.

7.2. RECOMENDACIONES

- Es esencial que dentro de las políticas de seguridad de la empresa, se establezca una política que incluya el riesgo y su tratamiento, como la base para la elaboración de un BCP y el plan de contingencias.

- Un aspecto importante es que el personal de TICs y la alta gerencia, tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad este plan, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional. Llegando a largo plazo a contar con un BCP-Plan de Continuidad del negocio para toda la empresa.

- El éxito de este proyecto dependerá de que todas las areas de la empresa sean incluidas en la aplicación de las estrategias de prevención.

- Que los procesos de recuperación documentados sean realmente probados como si el riesgo se hubiera presentado usando el peor escenario, que es recuperar desde cero todo el activo.

- Es necesario un programa de entrenamiento tanto para los directivos, así como para el personal adscrito al plan de contingencia, que entregue la información y la capacitación necesaria para que se pueda realizar la implementación del mismo. De lo contrario, se quedará solo en un documento más que perderá su vigencia y valor.

- El éxito para que el diseño del plan y la implementación sean vigentes y eficaces en el momento de la contingencia dependerá de la realización de pruebas, a pesar del coste que implican. De esta manera, la cantidad de pequeños detalles a tener en cuenta, unos aparentemente excesivos (como en qué lugar se guardan las llaves de acceso al armario, donde están las copias de seguridad, cambio de contraseñas en la máquina de producción real al finalizar las pruebas) y otros no tan sencillos (como la, designación de las personas autorizadas para dar la orden de activación del Plan o las pruebas del mismo), nos lleva a concluir que es imprescindible la realización de pruebas.

- Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

- La empresa eléctrica de acuerdo al análisis de riesgos realizado cuenta con la mayor cantidad de herramientas y recursos tecnológicos, para minimizar el riesgo sobre sus activos críticos, lo que necesita es establecer políticas y procedimientos documentados que garanticen la eficacia de la aplicación de los controles.

- Dentro de la estructura orgánica de la empresa, específicamente en el área de TICs, se debería tener un equipo de personas encargadas del SGSI, las mismas que monitoreen y verifiquen la seguridad de los diferentes activos, ayudando a mantener vigente los controles de seguridad aplicados e identificar los nuevos requerimientos, dado el dinamismo que las plataformas tecnológicas sufren, para asegurar que el riesgo sea el minimo, aceptado por la empresa.

- El análisis de riesgos y la elaboración de este plan de contingencias pueden servir como base para aplicarlo en otras áreas de la empresa, en donde también se manejan TICs, con los debidos ajustes que se alinien a las configuraciones particulares de las plataformas de esas áreas de la empresa.

- La empresa eléctrica debería dentro de sus políticas del SGSI, incluir a corto plazo, una política y normas que determinen los criterios para la clasificación de la información, dentro de la dimensión de la confidencialidad.

- Una copia del plan debería mantenerse almacenado fuera de la empresa eléctrica, junto con los respaldos

REFERENCIA BIBLIOGRAFICA

[1] 2008*, DAVID DE DOMPABLO FANTOVA, Plan General de Seguridad de una Empresa, Escuela Técnica Superior de Ingeniería, Universidad Pontificia Comillas.*

[2] 2008, *Plan de Contingencia del DCV Fundamentos y Metodología Aplicada,* http://www.dcv.cl/images/stories/DOC/empresa/procedimientos/download/PlandeContingenciade0DCV2008.pdf

[3] 2003, LIOTINE Matthew, *Mission-Critical Network Planning*

[4] 2009, SILBERFICH Pablo A., Análisis y Gestión de riesgos en TI ISO 27005 – Aplicación Práctica, http://www.segurinfo.org.ar/SITIO2009/Programa09/presentaciones/1610_ESET.pdf

[5] Del Monte Paulo, Implantacion del SGSI de SONDA Uruguay, www.cert.uy/historico/pdf/**SondaSGSI**.pdf

BIBLIOGRAFIA

[6] 2006, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Catálogo de Elementos, MINISTERIO DE ADMINISTRACIONES PÚBLICAS

[7] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Guia de Procedimientos, versión 1

[8] 2011, ORTEGA David, Plan de Contingencia. Aspectos a tener en cuenta, http://calidadtic.blogspot.com/2011/02/plan-de-contingencia-aspectos-tener-en.html

[9] 2011, ORTEGA David, Plan de Contingencia y Catálogo de Servicios de TI, http://calidadtic.blogspot.com/2011/03/plan-de-contingencia-y-catalogo-de.html

[10] 2011, ORTEGA David, http://calidadtic.blogspot.com/2011/01/como-hacer-un-plan-de-contingencia.html

[11] 2009, Plan de Contingencia de TIC, Empresa Portuaria Antofagasta, http://web.puertoantofagasta.cl/intranet/INFORMATICA/2002/pdc/PlanContingencia_20031127.htm#_Toc20985549

[12] 2003, Planes de Contingencia TIC: más que tecnología, novática / upgrade nº 166 noviembre-diciembre 2003 - Edición digital, http://www.ati.es/novatica/2003/166/166-3.pdf

[13] 2007, DISEÑO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD, http://dspace.epn.edu.ec/bitstream/15000/8682/4/T10528CAP3.pdf

[14] 2008, GONZALEZ BREÑA Julio, Análisis de Riesgos en la Agencia Estatal de Meteorología mediante el empleo de Magerit y Pilar, http://administracionelectronica.gob.es/recursos/pae_000005940.pdf

[15] 2008, GONZALEZ BREÑA Julio, http://www.revista-ays.com/DocsNum23/PersAAPP/Gonzalez.pdf

[16] 2007, Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones TIC-ASC-CGN-0001, Seguro Social Costa Rica, http://www.ccss.sa.cr/html/organizacion/gestion/gerencias/g_infraestructura/proyectos/Inicio/TIC-GCN-0001-guia_para%20Elaboracion_de_Planes_de_Continuidad_en_TIC.pdf

8. ANEXOS.

8.1. A-1: TERMINOS USADOS

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Gestión de riesgos: selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Activos: se refiere como activos a los recursos del sistema de información o que se encuentran estrechamente relacionados con este, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección, que aportan valor a la Organización.

Amenazas: son las cosas que les pueden pasar a los activos causando un perjuicio a la Organización

Salvaguardas: o contra medidas, son elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño.

Proceso de Negocio: es un conjunto de tareas relacionadas lógicamente llevadas a cabo para lograr un resultado de negocio definido. es un conjunto de tareas relacionadas lógicamente llevadas a cabo para lograr un resultado de negocio definido.

Recursos de front-end: Son los recursos que interactúa directamente con el usuario final (clientes).

Recursos de back-end: Son los recursos que se encuentran detrás de los procesos que interactúan con el usuario final.

Back Office: (trastienda de la oficina) es la parte de las empresas donde tienen lugar las tareas destinadas a gestionar la propia empresa y con las cuales el cliente no necesita contacto directo. Por ejemplo: el departamento de informática y comunicaciones que hace que funcionen los ordenadores, redes y teléfonos, el departamento de recursos humanos, el de contabilidad, etc.

8.2. A-2: ESCALA DE VALORACION DETALLADA.

CRITERIO	VALOR
10	[olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística [iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información [si] Seguridad: probablemente sea causa de un incidente excepcionalmente serior de seguridad o dificulte la investigación de incidentes excepcionalmente serios [ps] Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas [po] Orden público: alteración sería del orden constitucional [ir] Probablemente cause un impacto excepcionalmente grave en llas relaciones internacionales [lbl] Datos clasificados como secretos
9	[da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones [adm] Administración y gestión: probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre [lg] Probablemente causaría causaría una publicidad negativa generalizada por por afectar de forma excepcionalmente grave a las relaciones ... [lg.a] a las relaciones con otras organizaciones [lg.b] a las relaciones con el público en general [lg.c] a las relaciones con otros paises [olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística [iio] Probablemente cause serios daños a misiones muy importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de enorme interés para la competencia [cei.b] de muy elevado valor comercial [cei.c] causa de pérdidas económicas excepcionalmente elevadas [cei.d] causa de muy significativas ganancias o ventajas para individuos u organizaciones [cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros [lro] Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación

	[si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios [ps] Seguridad de las personas: probablemente suponga la muerte de uno o más individuos [po] Orden público: alteración seria del orden público [ir] Probablemente cause un serio impacto en las relaciones internacionales [lbl] Datos clasificados como reservados
8	[ps] Seguridad de las personas: probablemente cause daño a la seguridad o libertad individual (por ejemplo, es probable que llegue a amenazar la vida de uno o más individuos) [crm] Impida la investigación de delitos graves o facilite su comisión [lbl] Datos clasificados como confidenciales
7	[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones [adm] Administración y gestión: probablemente impediría la operación efectiva de la organización [lg] Probablemente causaría una publicidad negativa generalizada [lg.a] por afectar gravemente a las relaciones con otras organizaciones [lg.b] por afectar gravemente a las relaciones con el público en general [lg.c] por afectar gravemente a las relaciones con otros paises [olm] Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística [iio] Probablemente cause serios daños a misiones importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de alto interés para la competencia [cei.b] de elevado valor comercial [cei.c] causa de graves pérdidas económicas [cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones [cei.e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros [lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación [si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos [ir] Probablemente cause un impacto significativo en las relaciones Internacionales

	[lbl] Datos clasificados como confidenciales
6	[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos [pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal [ps] Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo [po] Orden público: probablemente cause manifestaciones, o presiones significativas [lbl] Datos clasificados como de difusión limitada
5	[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones [adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización [lg] Probablemente sea causa una cierta publicidad negativa [lg.a] por afectar negativamente a las relaciones con otras organizaciones [lg.b] por afectar negativamente a las relaciones con el público [olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local [iio] Probablemente dañe a misiones importantes de inteligencia o información [pi1] Información personal: probablemente afecte gravemente a un individuo [pi2] Información personal: probablemente quebrante seriamente leyes o regulaciones [lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación [ir] Probablemente tenga impacto en las relaciones internacionales [lbl] Datos clasificados como de difusión limitada
4	[pi1] Información personal: probablemente afecte a un grupo de individuos [pi2] Información personal: probablemente quebrante leyes o regulaciones [ps] Seguridad de las personas: probablemente cause daños menores a varios individuos [crm] Dificulte la investigación o facilite la comisión de delitos [lbl] Datos clasificados como de difusión limitada
3	[da] Probablemente cause la interrupción de actividades propias de la Organización [adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la organización [lg] Probablemente afecte negativamente a las relaciones internas de la Organización [olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local) [iio] Probablemente cause algún daño menor a misiones

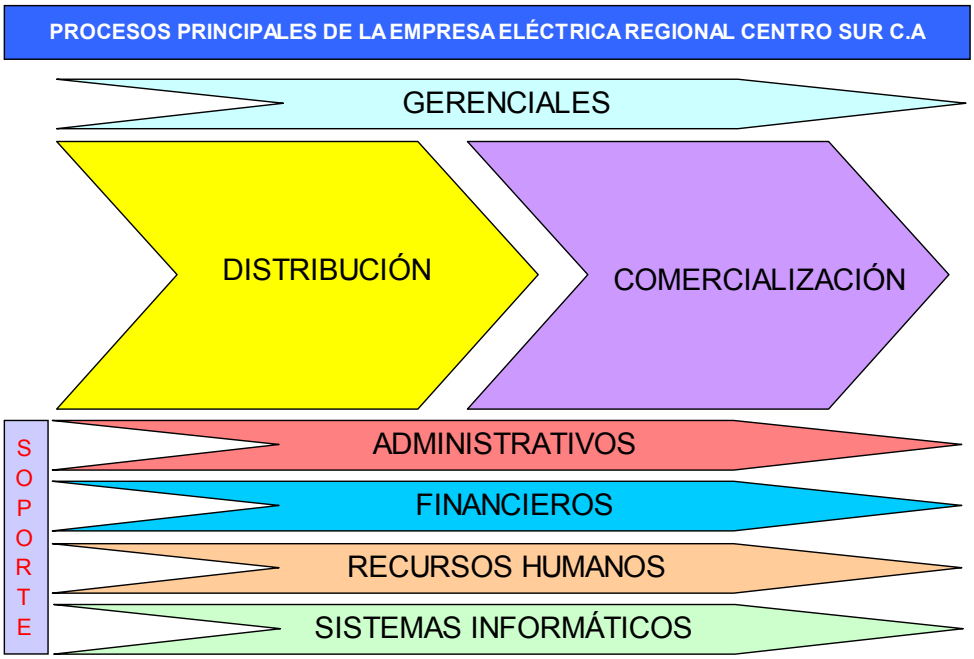
	importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de cierto interés para la competencia [cei.b] de cierto valor comercial [cei.c] causa de pérdidas financieras o merma de ingresos [cei.d] facilita ventajas desproporcionadas a individuos u organizaciones [cei.e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros [pi1] Información personal: probablemente afecte a un individuo [pi2] Información personal: probablemente suponga el incumplimiento de una ley o regulación [lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación [si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente [ps] Seguridad de las personas: probablemente cause daños menores a un individuo [po] Orden público: causa de protestas puntuales [ir] Probablemente cause un impacto leve en las relaciones internacionales [lbl] Datos clasificados como de difusión limitada
2	[lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización [cei] Intereses comerciales o económicos: [cei.a] de bajo interés para la competencia [cei.b] de bajo valor comercial [pi1] Información personal: pudiera causar molestias a un individuo [pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones [ps] Seguridad de las personas: pudiera causar daño menor a varios individuos [lbl] Datos clasificados como sin clasificar
1	[da] Pudiera causar la interrupción de actividades propias de la Organización [adm] Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización [lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización [olm] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local) [iio] Pudiera causar algún daño menor a misiones importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de pequeño interés para la competencia [cei.b] de pequeño valor comercial [pi1] Información personal: pudiera causar molestias a un individuo

	[lro] Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación [si] Seguridad: pudiera causar una merma en la seguridad o dificular la investigación de un incidente [ps] Seguridad de las personas: pudiera causar daños menores a un individuo [po] Orden público: pudiera causar protestas puntuales [ir] Pudiera tener un impacto leve en las relaciones internacionales [lbl] Datos clasificados como sin clasificar
0	[1] no afectaría a la seguridad de las personas [2] sería causa de inconveniencias mínimas a las partes afectadas [3] supondría pérdidas económicas mínimas [4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

8.3. A-3: PROCESOS DE NEGOCIO DE LA EMPRESA ELECTRICA CENTRO SUR

A-3.1 Procesos de negocio.

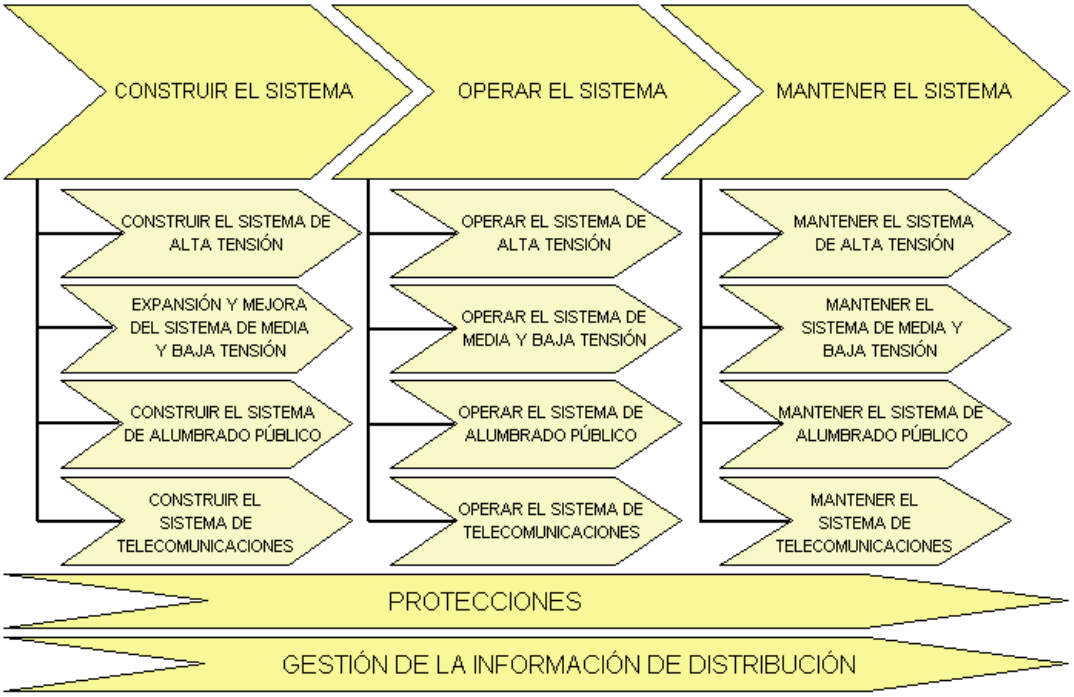
A continuación se presenta los procesos de negocio principales de la empresa eléctrica Centro Sur, agrupados según la cadena de valor, en procesos primarios y procesos secundarios.



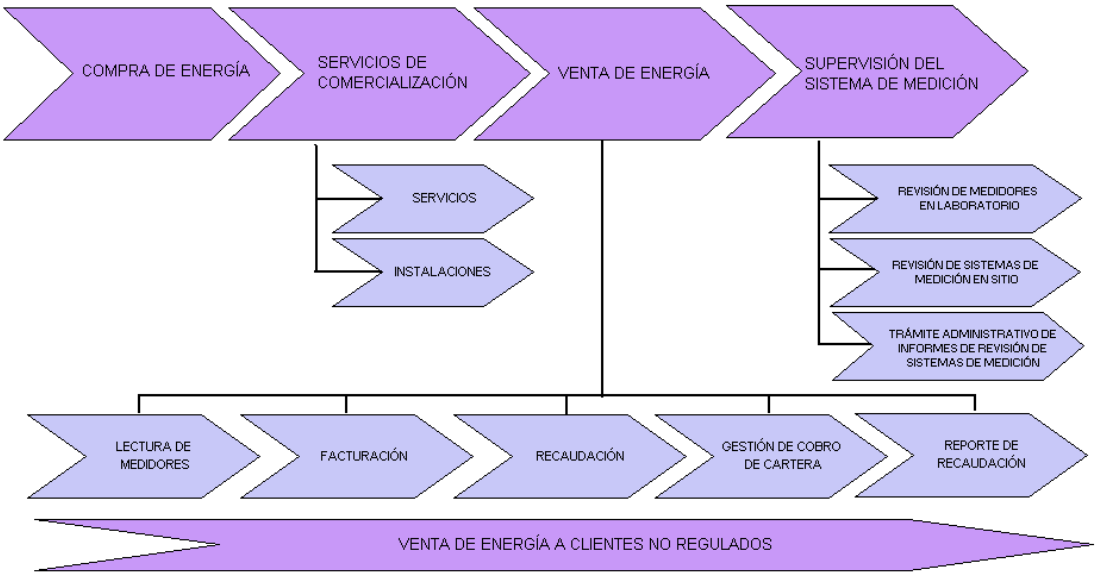
PROCESOS PRIMARIOS

Dentro de los procesos primarios en la cadena de valor se identificaron los procesos de distribución y de comercialización.

A-3.2 Distribución



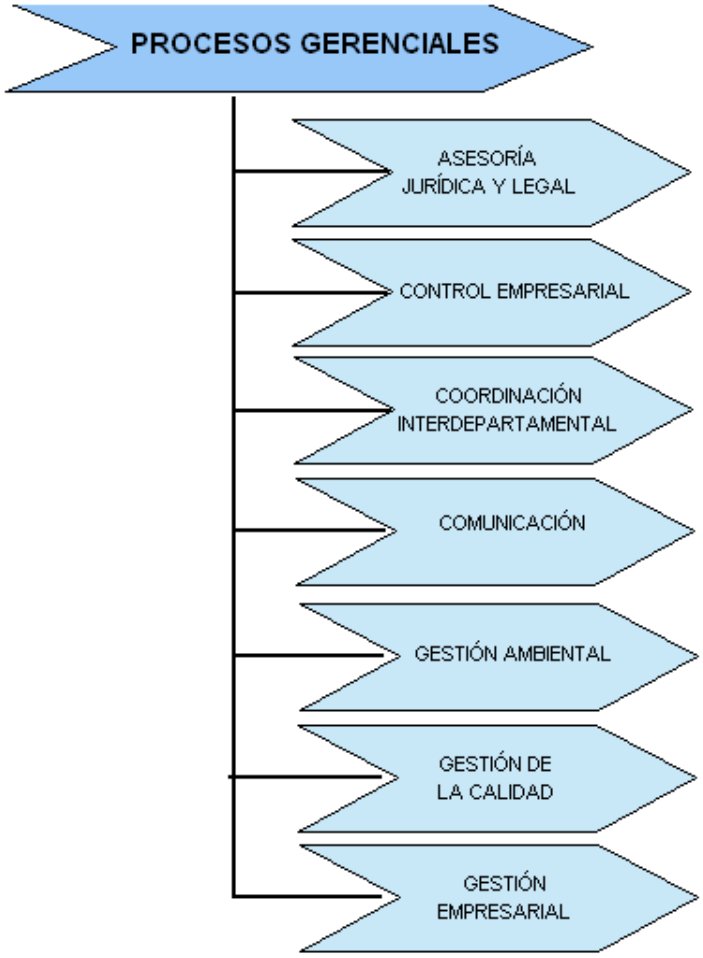
A-3.3 Comercialización



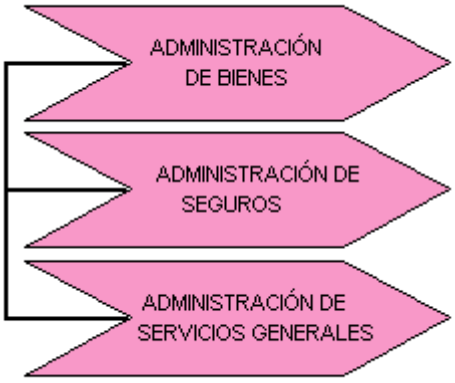
PROCESOS SECUNDARIOS

Los procesos secundarios son aquellos que sirven de apoyo a los primarios y garantizan su funcionamiento. Se identificaron dentro de este grupo a los siguientes procesos.

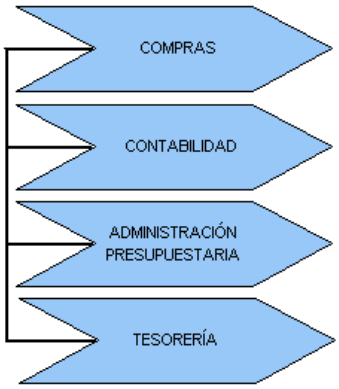
A-3.4 Gerenciales



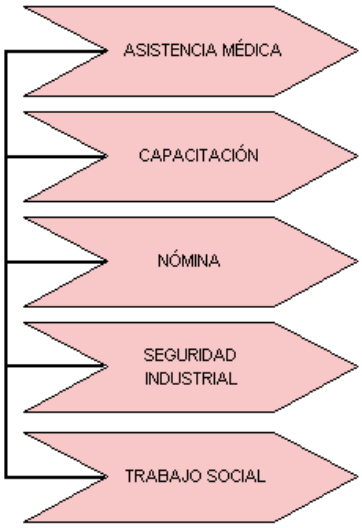
A-3.5 Administrativos



A-3.6 Financieros



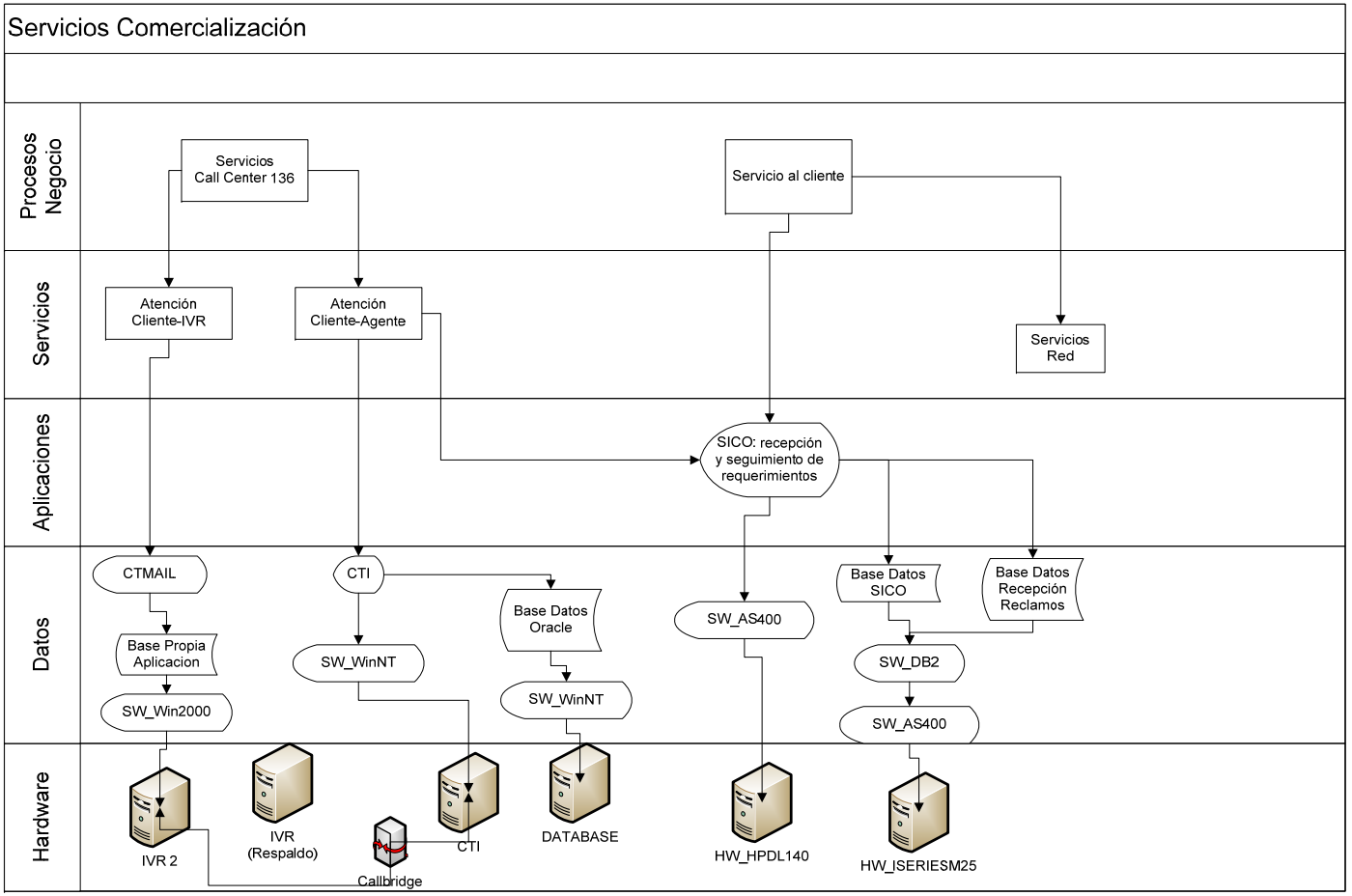
A-3.7 Recursos Humanos

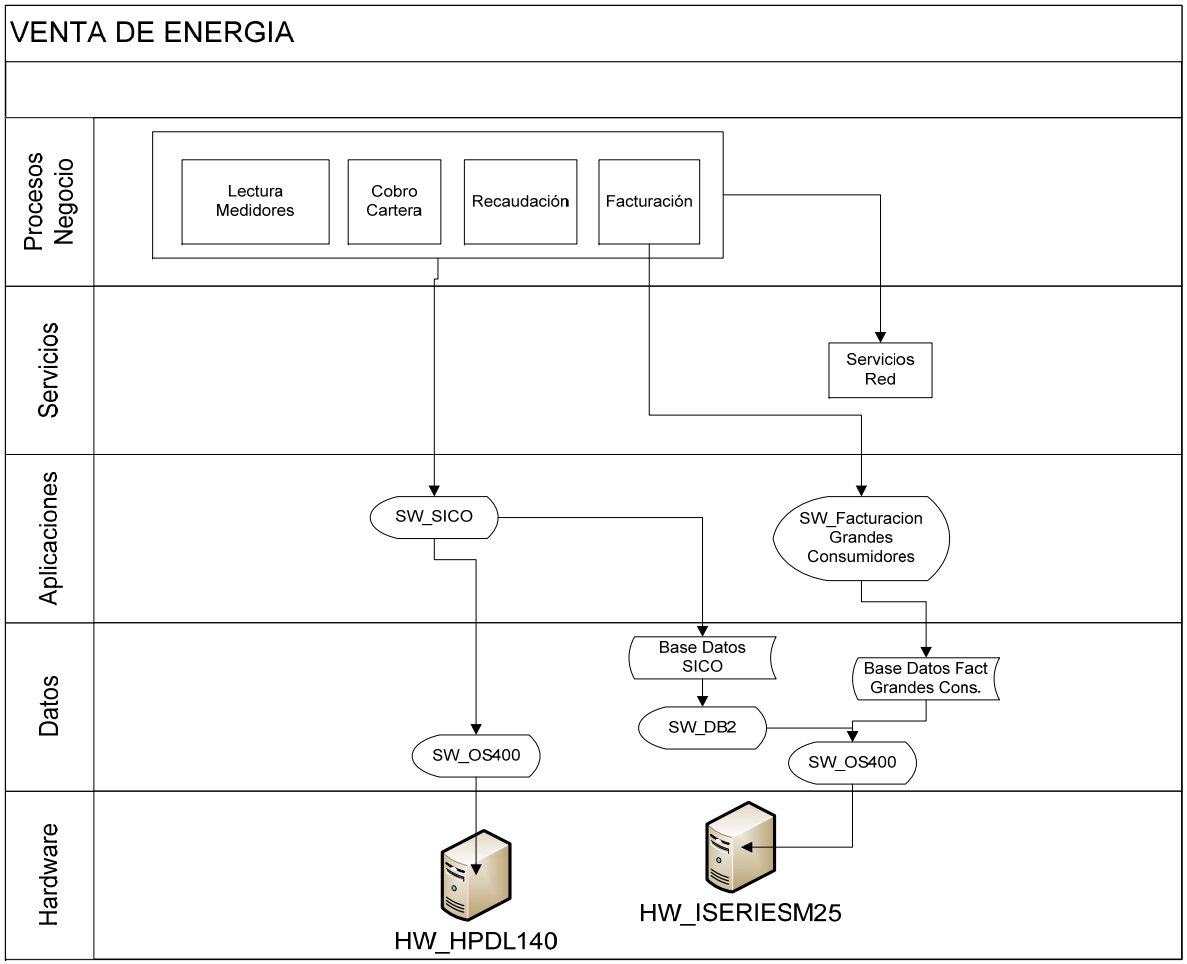


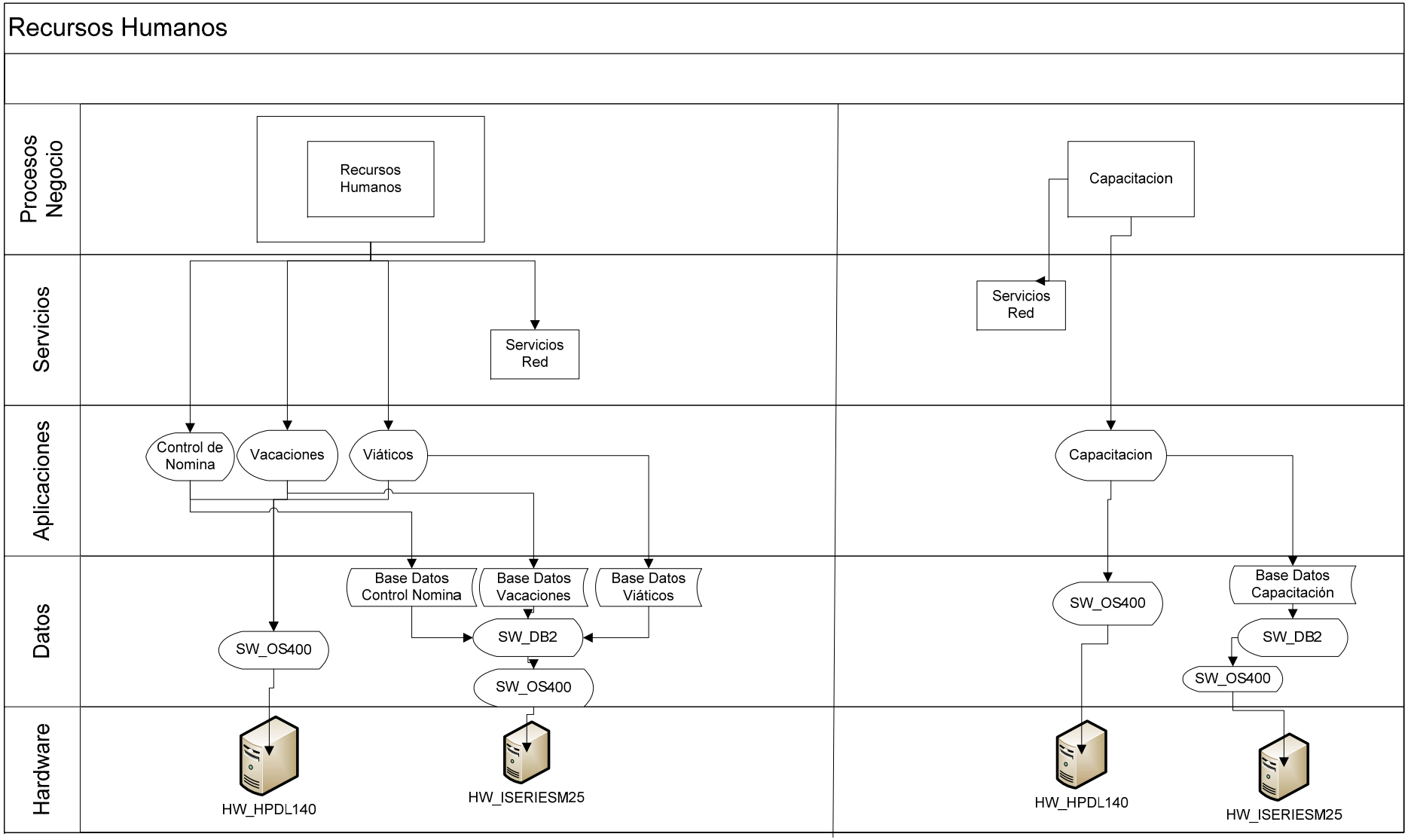
A-3.8 Sistemas Informáticos

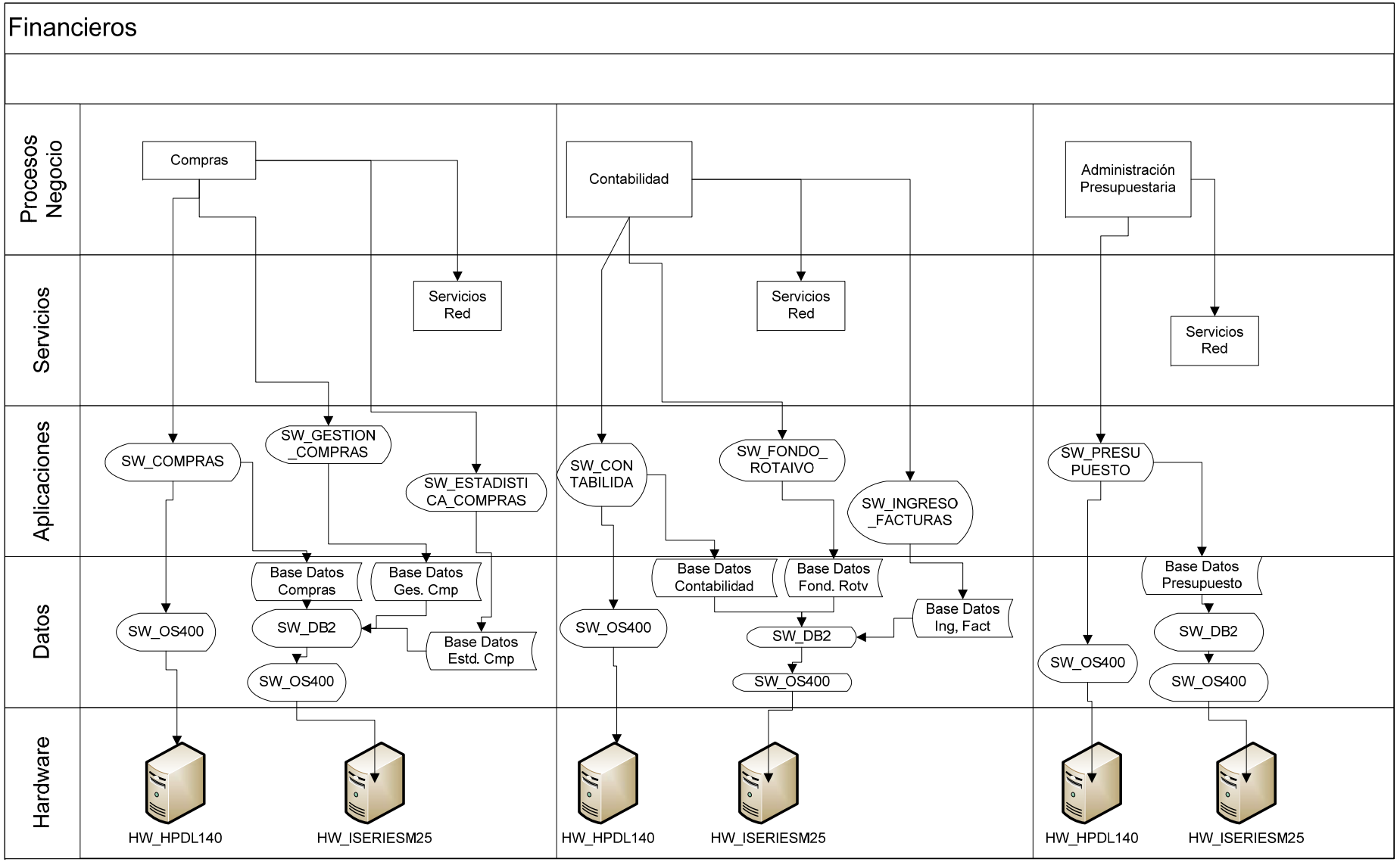

SISTEMAS INFORMÁTICOS
PLANIFICACIÓN DE SERVICIOS INFORMÁTICOS
DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS
OPERACIÓN Y SOPORTE DE SERVICIOS INFORMÁTICOS

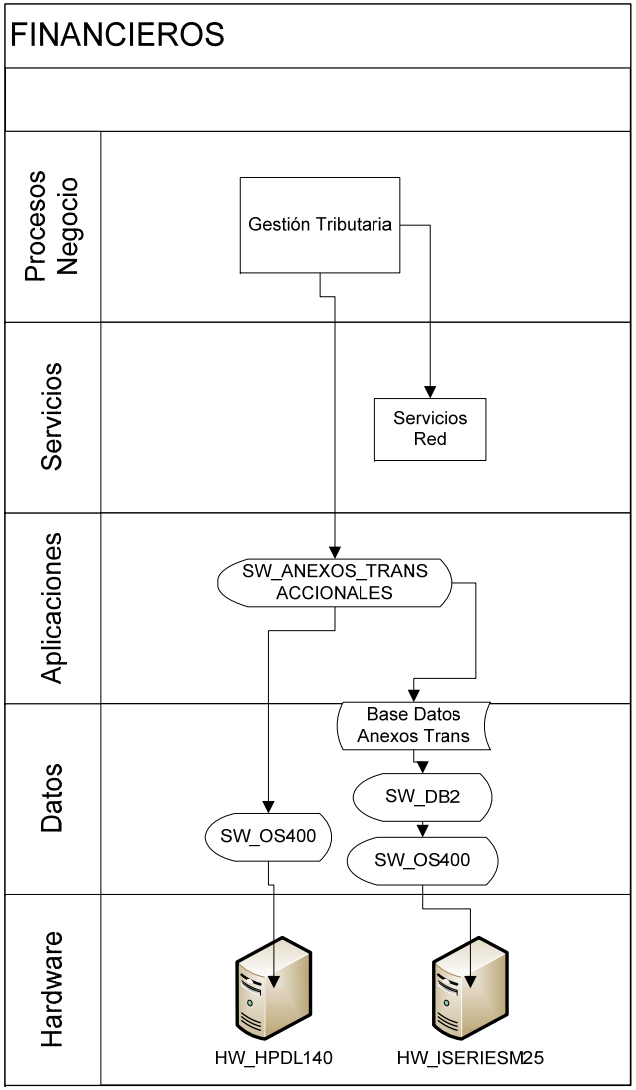
8.4. A-4: DIAGRAMAS DE DEPENDENCIA ENTRE ACTIVOS.

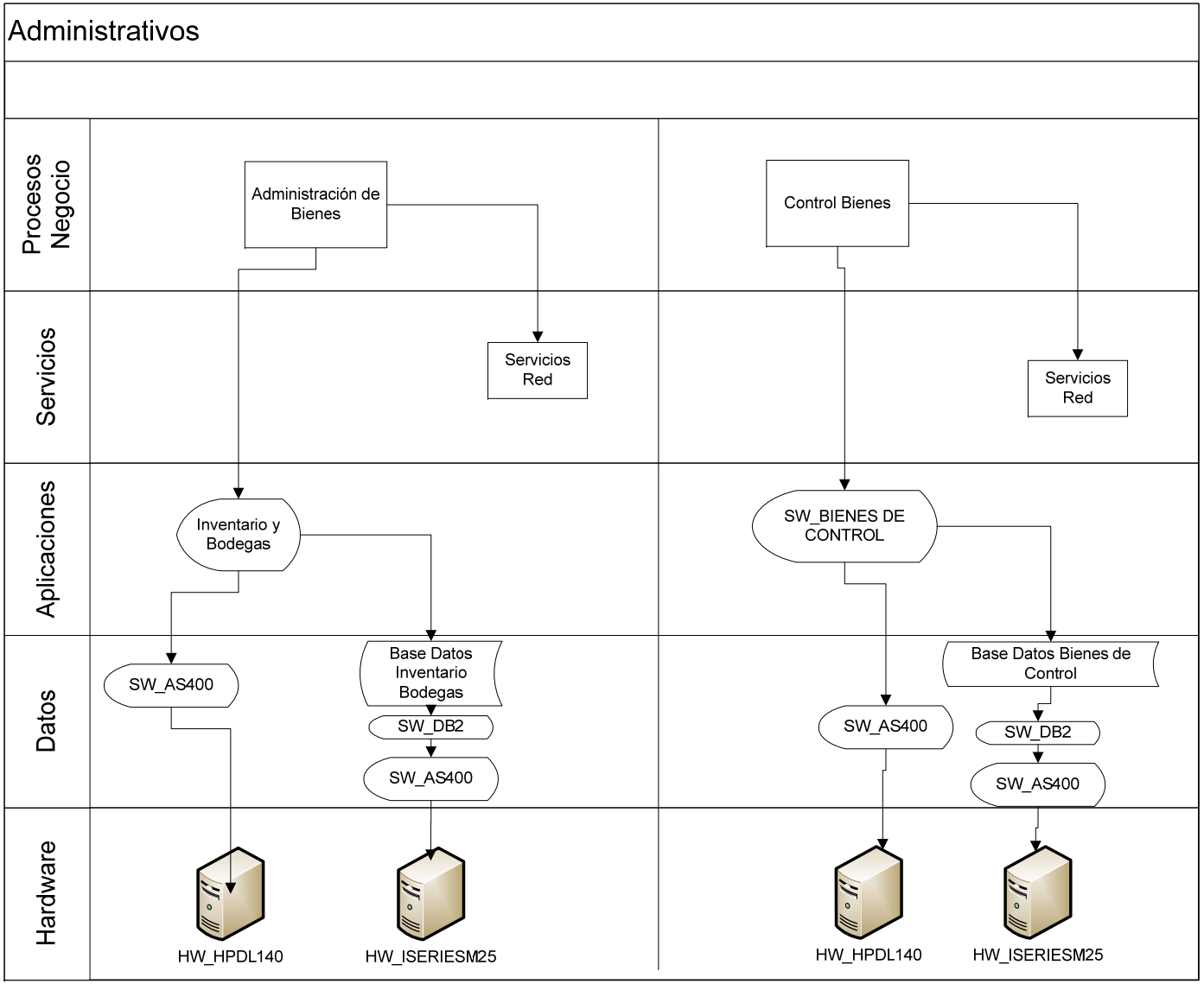


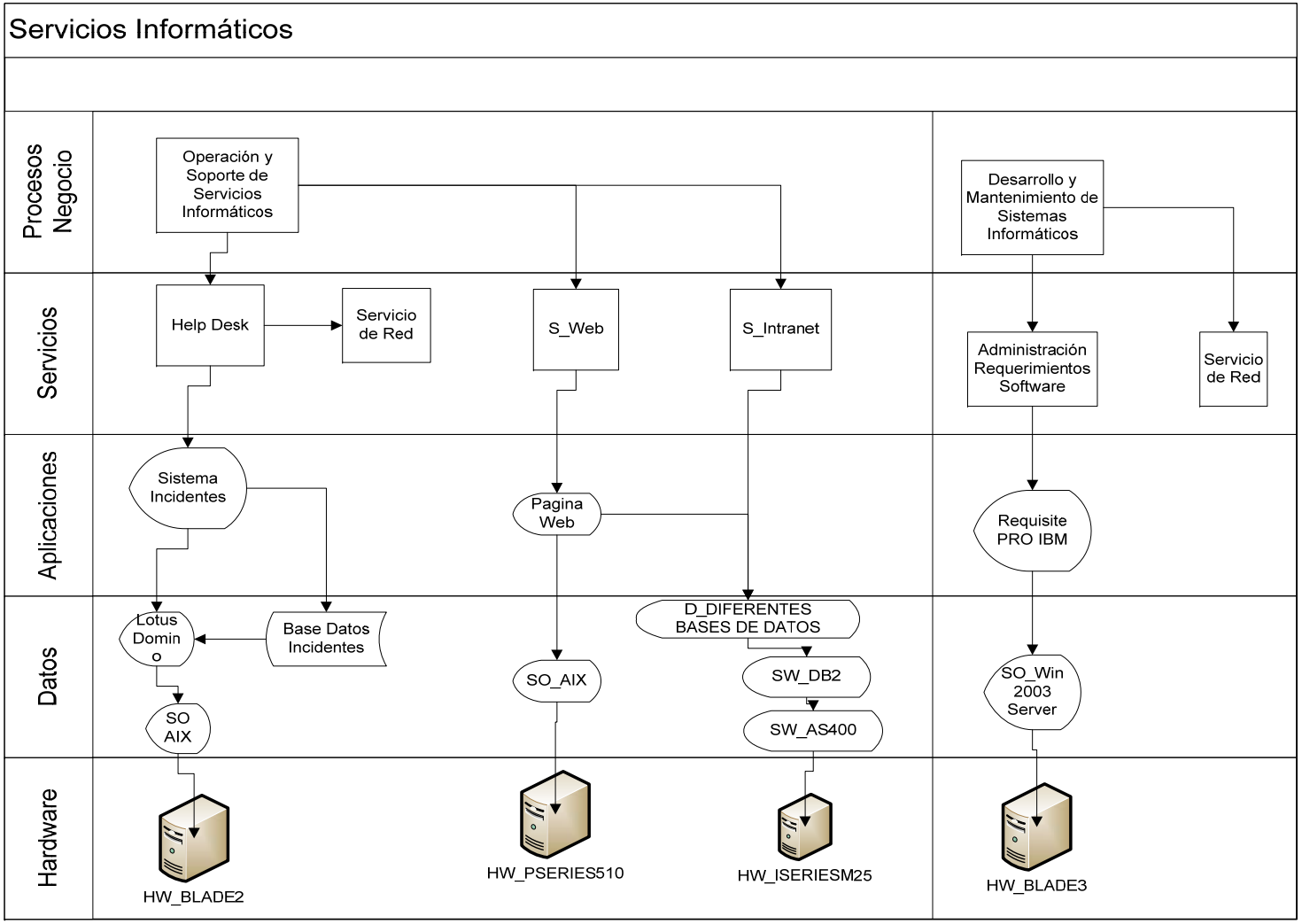

VENTA DE ENERGIA
Procesos Negocio
Lectura Medidores
Cobro Cartera
Recaudación
Facturación
Servicios
Servicios Red
Aplicaciones
SW_SICO
SW_Facturacion Grandes Consumidores
Datos
Base Datos SICO
Base Datos Fact Grandes Cons.
SW_DB2
SW_OS400
SW_OS400
Hardware
HW_HPDL140
HW_ISERIESM25

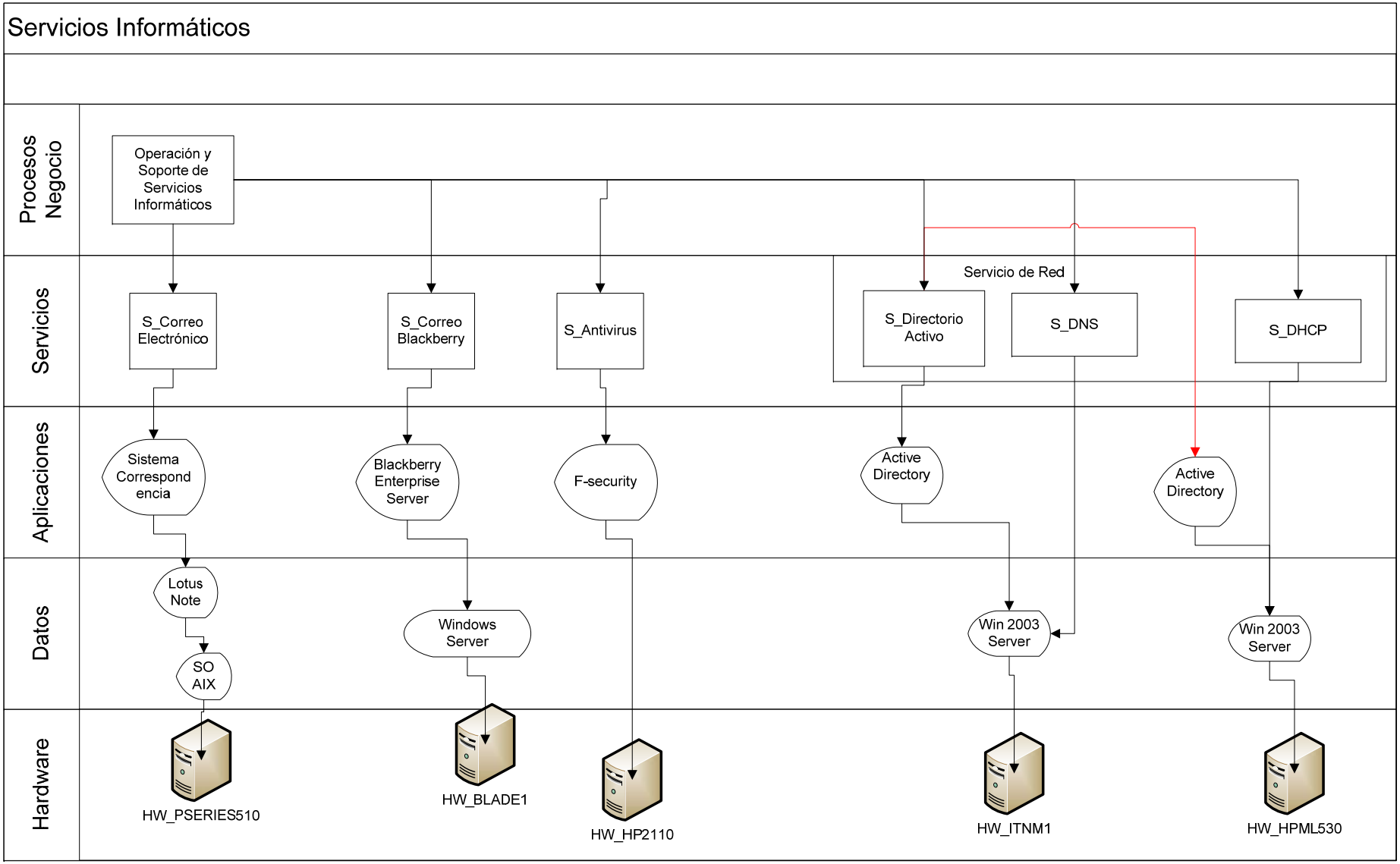

Recursos Humanos
Procesos Negocio
Servicios
Aplicaciones
Datos
Hardware
Recursos Humanos
Servicios Red
Control de Nomina
Vacaciones
Viáticos
Base Datos Control Nomina
Base Datos Vacaciones
Base Datos Viáticos
SW_OS400
SW_DB2
SW_OS400
HW_HPDL140
HW_ISERIESM25
Capacitacion
Servicios Red
Capacitacion
SW_OS400
Base Datos Capacitación
SW_DB2
SW_OS400
HW_HPDL140
HW_ISERIESM25


Financieros
Procesos Negocio
Servicios
Aplicaciones
Datos
Hardware
Compras
Contabilidad
Administración Presupuestaria
Servicios Red
Servicios Red
Servicios Red
SW_COMPRAS
SW_GESTION _COMPRAS
SW_ESTADISTI CA_COMPRAS
SW_CON TABILIDA
SW_FONDO_ ROTAIVO
SW_INGRESO _FACTURAS
SW_PRESU PUESTO
Base Datos Compras
Base Datos Ges. Cmp
Base Datos Estd. Cmp
Base Datos Contabilidad
Base Datos Fond. Rotv
Base Datos Ing, Fact
Base Datos Presupuesto
SW_OS400
SW_DB2
SW_OS400
SW_OS400
SW_DB2
SW_OS400
SW_OS400
SW_DB2
SW_OS400
HW_HPDL140
HW_ISERIESM25
HW_HPDL140
HW_ISERIESM25
HW_HPDL140
HW_ISERIESM25


FINANCIEROS
Procesos Negocio
Gestión Tributaria
Servicios
Servicios Red
Aplicaciones
SW_ANEXOS_TRANS ACCIONALES
Datos
Base Datos Anexos Trans
SW_DB2
SW_OS400
SW_OS400
Hardware
HW_HPDL140
HW_ISERIESM25


Administrativos
Procesos Negocio
Servicios
Aplicaciones
Datos
Hardware
Administración de Bienes
Control Bienes
Servicios Red
Servicios Red
Inventario y Bodegas
SW_BIENES DE CONTROL
SW_AS400
Base Datos Inventario Bodegas
SW_DB2
SW_AS400
SW_AS400
Base Datos Bienes de Control
SW_DB2
SW_AS400
HW_HPDL140
HW_ISERIESM25
HW_HPDL140
HW_ISERIESM25


Servicios Informáticos
Procesos Negocio
Servicios
Aplicaciones
Datos
Hardware
Operación y Soporte de Servicios Informáticos
Desarrollo y Mantenimiento de Sistemas Informáticos
Help Desk
Servicio de Red
S_Web
S_Intranet
Administración Requerimientos Software
Servicio de Red
Sistema Incidentes
Pagina Web
Requisite PRO IBM
Lotus Domino
Base Datos Incidentes
D_DIFERENTES BASES DE DATOS
SW_DB2
SW_AS400
SO_AIX
SO_Win 2003 Server
SO AIX
HW_BLADE2
HW_PSERIES510
HW_ISERIESM25
HW_BLADE3


Servicios Informáticos
Procesos Negocio
Servicios
Aplicaciones
Datos
Hardware
Operación y Soporte de Servicios Informáticos
S_Correo Electrónico
S_Correo Blackberry
S_Antivirus
Servicio de Red
S_Directorio Activo
S_DNS
S_DHCP
Sistema Correspond encia
Blackberry Enterprise Server
F-security
Active Directory
Active Directory
Lotus Note
SO AIX
Windows Server
Win 2003 Server
Win 2003 Server
HW_PSERIES510
HW_BLADE1
HW_HP2110
HW_ITNM1
HW_HPML530